Brussels, 25 July 2024

Orgalim's response to the European Commission's consultation on the NIS2 Directive draft implementing regulation

Executive summary

Orgalim is supportive of the main objectives stipulated in the revised Network and Information Systems (NIS2) Directive which aim to enhance cybersecurity requirements across Europe, including in its technology industries, and to address the growing threat of cyberattacks. The NIS2 Directive is expanding its scope to cover a broader range of sectors compared to its predecessor, the current Network and Information Security (NIS) Directive.

Therefore, it is crucial to address several shortcomings in the draft implementing act on cybersecurity risk management and reporting obligations, as these can significantly impact Europe's industries. We recommend to:

- Clarify and narrow down the criteria for classifying an incident as significant (feedback on reporting obligations).
- Assess the interplay between the draft implementing regulation and other existing standards, schemes and the national transposition of the NIS2 Directive (feedback on cybersecurity risk management measures).

1. Introduction

Orgalim represents Europe's technology industries, comprised of 770,000 innovative companies spanning the mechanical engineering, electrical engineering and electronics, ICT and metal technology branches. Together they represent the EU's largest manufacturing sector, generating annual turnover of €2,835 billion, manufacturing one third of all European exports and providing 11.7 million direct jobs.

The European manufacturing industry plays a pivotal role in producing a wide range of digital products which represent a significant part of the supply chain. With the increasing prevalence of cyber threats, it is imperative to strengthen cybersecurity measures, safeguard our critical infrastructures and ensure the continuity and security of operations.

We welcome the NIS2 Directive as a piece of legislation with the objective of increasing the cyber resilience of businesses and society and reducing inconsistencies in cybersecurity levels across the internal market. The corresponding draft implementing act should lay down the conditions of implementation for the NIS2 Directive in a proportionate and clear manner for organisations, creating a harmonised framework across Member States.

Please find below the Orgalim response to the European Commission`s consultation on the NIS2 Directive draft implementing regulation.

2. Clarify and narrow down the criteria for classifying an incident as significant

2.1 Significant incident criteria

The draft implementing regulation lays down criteria which will be used to determine if an incident is to be classified as *significant*. The criteria presented in Article 3 are, however, ambiguous and can potentially create confusion in terms of reporting obligations which can ultimately lead to "reporting fatigue" for in-scope entities.

Article 3(1)(a) introduces a criterion for determining a significant incident as "an incident which has caused or is capable of causing financial loss for the relevant entity that exceeds €100,000 or 5% of the relevant entity`s annual turnover, whichever is lower." We find the criteria unclear as there is no specification on how to determine the *capability* of an incident to cause financial loss. In addition, the €100,000 or 5% of the relevant entity`s annual turnover threshold can differ greatly across the sector, based on the size of the entity. We suggest that the criterion in Article 3(1)(a) should be applied only to incidents which are proved to cause financial loss for the entity. We also recommend that only relative thresholds (e.g. percentage of the turnover) are used to categorise an incident as significant.

Article 3(1)(b) introduces a criterion for determining a significant incident as an "incident which has caused or is capable of causing considerable reputational damage". Article 3(2)(a) further specifies the parameters for determining the existence of considerable reputational damage. We find the criteria unclear as there is no specification on how to determine the *capability* of an incident to cause considerable reputational damage. In addition, the parameters describing "considerable reputational damage" are vague. Point (a) specifies that the incident must be "reported in the media". This does not clarify if the media includes local, national or international channels. We consider the expectation of entities to monitor the full extent of media coverage as unrealistic. Point (b) refers to an incident which results in "complaints from different users": however, it does not specify a quantitative threshold of how many complaints (relative to the size of the entity) must be recorded to count towards "considerable reputational damage". We suggest the addition of further clarifications and quantifiable thresholds for points (a) and (b) to clarify the extent of the entity`s efforts to monitor and report significant incidents.

Article (3)(1)(f) refers to "suspected malicious action" and mandates that entities must report incidences that occur as a result of suspected malicious action. Until an investigation is complete, the entity will not have the appropriate level of information to ascertain whether an incident was malicious or not. This can lead to confusing reports of incidents and potential over-reporting. We suggest only "malicious action" remains part of the scope.

Article 3(4) introduces a proposal for calculating the number of users impacted by an incident for the purpose of classifying the incident as significant. Due to the nature of services provided (e.g. in the case of cloud services), it is not always feasible to assess the exact number of impacted users or individuals. In this case, the service provider may not have a clear and direct relationship with all the end-users or may not be able to ascertain the exact number of users accessing the service at any given time. Rather than monitoring individual users, we suggest the tracking of error rates, and setting the thresholds at API endpoints.

Article 4 introduces the concept of "recurring incidents", which categorises an incident as significant based on two parameters. The first parameter establishes the frequency with which incidents must occur in order for it to be classified as significant, which is "twice within six months". We find the threshold too low, especially in the case of

recurrent phishing attacks which can occur often but do not pose a significant risk. We suggest increasing the frequency threshold to a realistic level. The second parameter requires that incidents must have the same "apparent root cause". This description is vague and difficult to determine, therefore we suggest replacing "apparent root cause" with "unquestionable root cause".

2.2 Service outage criteria

Articles 7-10 mention that one of the criteria for an incident to be determined as significant is the services or security services of some providers being unavailable for more than ten minutes. We consider the timeline to be challenging, especially for smaller-sized service providers which can not ensure 24/7 staff availability. The duration of an incident does not directly indicate how significant an incident can be. In addition, it is unclear if this would apply to unavailability of services in non-EU countries which affect European users. Depending on whether the unavailability of the services is global, limited to the EU, or only affecting European users, the implications and necessary actions may differ. We suggest limiting the scope to services hosted within the EU, where a certain number/percentage of direct users have been affected, instead of a time-based threshold. Alternatively, Service Level Agreements can be used to determine availability commitments and the corresponding risk associated with the incident when a service is unavailable.

3. Interplay with the draft implementing regulation

The Annex of the draft implementing regulation does not clarify the overlap between the draft implementing regulation and existing standards. It does not mention EU certification schemes under development or compliance programmes addressing cybersecurity risk management and incident-handling mechanisms. We call for clarity on how companies can leverage existing standards and certifications to demonstrate compliance.

In addition, the Annex does not clarify the interplay with the national transposition of the NIS2 directive. The implementing regulation will directly apply to entities without the need for transposition and will override national provision. In this case, it is unclear how differences will be resolved between the two pieces of legislation. Under the NIS2 Directive, Member States are allowed to adopt additional national provisions to complement the cybersecurity risk management measures. Despite this, Member States are unlikely to take the official implementing regulation into account in a timely manner since the deadlines for application and national transposition are the same. For example, Recital 13 of the Annex mentions that relevant entities should regularly carry out security tests to verify the implementation of cybersecurity risk-management measures. Entities with a wide range of services across multiple Member States need a unified understanding of "regular security tests". It is important that the dates for security tests, to be carried out across subsidiaries, are precise. Therefore, we suggest that the frequency of security tests is specified in the Annex to avoid a fragmented interpretation of "regular testing" across Member States.

To avoid the confusion of applying two potentially overlapping sets of provisions, we suggest clarifying that any national transposition measures in conflict with the measures of the implementing regulation should be disregarded. This will lead to less fragmentation among Member States in accordance with Recital 84 of the NIS2 Directive.

We encourage the implementing regulation of the NIS2 Directive to take into account the New Legislative Framework (NLF) which provides a broad outline of what must be achieved, leaving the specific technical details to

be filled in by industry experts through standards. In this case, we require more clarity on how compliance with recognised standards such as ISO 27001 and IEC 62443 (comprehensive frameworks for managing cybersecurity risks) can be used to prove conformity with the cybersecurity requirements laid down in the Annex of the implementing regulation.

Finally, we suggest that the Annex of the draft implementing regulation takes into account the principle of proportionality of the cybersecurity risk management measures. The Annex describes actions from entities by using "shall", leaving little space for entities to assess the appropriate, risk-based measures suitable for their risk profile. We recommend that, in some cases, the word "shall" could be replaced by the word "should".

Orgalim aisbl
BluePoint Brussels
Boulevard A Reyers 80
B1030 | Brussels | Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438