RIPE NCC feedback on the draft NIS2 Implementing Act on cybersecurity risk-management measures and significant incident criteria

The RIPE NCC is a not-for-profit membership organisation and a Regional Internet Registry (RIR) that allocates Internet number resources in Europe, the Middle East and part of Central Asia. It also operates one of the world's 13 global DNS root servers (K-root) and acts as the secretariat for the RIPE community, which is an inclusive forum open to all parties interested in wide area IP networks. The RIPE NCC actively participated in discussions on the proposed revision of the NIS2 Directive[1] and welcomes the opportunity to provide feedback on the draft implementing act on the technical and methodological requirements of cybersecurity risk-management measures and specifications for significant incidents.

Alignment with international standards

The RIPE NCC fully supports the main goal of the NIS2 Directive, which is to improve cybersecurity levels across the EU. This involves ensuring a consistent level of readiness, response and resilience, as well as promoting cooperation and information sharing among EU member states and relevant stakeholders. To achieve this, it is crucial for relevant entities to be able to leverage well-established international standards. The RIPE NCC advises national and EU authorities to align national guidelines and frameworks with globally recognised standards and conformance schemes for information risk management, such as ISO/IEC 27001. This approach will provide assurance and facilitate compliance for many organisations, while also promoting greater harmonisation across the EU and globally.

Incident reporting and information sharing

Organisations must be able to prioritise resource allocation in resolving incidents and restoring operations. Defining significant incident criteria using a risk-based approach and ensuring that the exchanged information provides valuable insights are essential steps. Simplifying and streamlining the reporting process itself is equally important. Instead of reporting to both the CSIRT and the national competent authority, there should be a single point of entry to avoid double reporting. Additionally, harmonising and streamlining obligations across the various EU regulatory frameworks would further reduce administrative burden and costs. This would enable affected entities to dedicate their resources and attention to risk mitigation and incident response. The RIPE NCC also encourages CSIRTs to actively share threat information with relevant entities in order to create a two-way operational collaboration to better prevent and resolve incidents.

Proportionality and compensatory measures

The draft implementing act allows for compensatory measures where full compliance is not feasible for specific reasons, particularly for smaller companies as explained in recital 5, but it lacks detailed guidance and specification. We recommend that these operators must be able to make their own decision on the appropriate compensatory measures and demonstrate these are adequate and proportionate in order to mitigate risks and achieve the desired outcome. Special consideration should be given to non-commercial entities with complex business models and operating environments. A more gradual approach to the requirements based on the size and risk profile would help ensure a more effective and proportionate application of the NIS2 framework.

[1] See RIPE NCC Response to the European Commission's Proposed NIS2 Directive

Supply chain security and FOSS components

We would also like to highlight concerns expressed by RIPE community members[2] and other related stakeholders on the draft provisions on supply chain security requirements in Annex and the uncertainty expressed regarding Free and Open Source Software (FOSS). Since the term 'supplier' is not explicitly defined, and noting the reference to unspecified "software editors" in recital 85 of the NIS2 Directive, a broad interpretation could potentially encompass any natural or legal person developing and publishing software. It is important to underline that FOSS components can be incorporated in any software products and services even with no formal contractual relationship being established between the provider and relevant entities. It is therefore important to provide legal certainty with regard to FOSS components. Finally, clearly referencing the Cyber Resilience Act would ensure a higher level of coherence and consistency across the two regulatory regimes.

[2] As aligned with responses provided by the Free Software Foundation Europe, NLnet Labs and the Open Source Security Foundation, as well as CENTR