ETNO-GSMA feedback on draft implementing act under the NIS2 Directive

The telecommunications perspective

ETNO and the GSMA welcome the opportunity to share their views on the draft implementing regulation regarding cybersecurity risk management and reporting obligations for various digital infrastructure and service providers. Our members, who represent the leading telecommunication network and service providers in Europe, are thoroughly preparing to comply with the NIS 2 Directive and have been actively engaging with decision-makers and regulators on the national implementation of the law.

Member States are currently implementing and applying a plethora of security legislation, including the national transposition of NIS 2, which now also encompasses security rules for the telecom sector previously under the European Electronic Communications Code (EECC); the new Critical Entities Resilience Directive (CER); the Digital Operational Resilience Act (DORA); and national measures stemming from the 5G Security Toolbox. Additionally, data privacy legislation such as the General Data Protection Regulation (GDPR) and the ePrivacy Directive demands further incident notifications in case of a data breach. These regulations affect the telecoms industry all at once. Therefore, consistent, and harmonized application of this layered security rulebook is paramount.

As stated in NIS2, to avoid unnecessary disruption, existing national guidelines adopted for the transposition of the rules related to security measures laid down in Articles 40 and 41 of the EECC should be considered. If the Commission were to adopt further implementing acts in the future, we would encourage the Commission to perform a thorough gap analysis and to build on its established corpus of legal requirements and practices, including the ENISA Guidelines on Security Measures and Incident Reporting under the EECC, which we understand are being updated considering the draft implementing acts.

Regarding the draft implementing regulation, we understand that it is strictly addressed to categories of digital infrastructure, digital and ICT service management providers whose operations have a cross-border dimension. However, telecommunications operators typically also serve as cloud computing providers and often include CDN, DNS, and managed services as part of their portfolios. If telcos were to be subject to differing principles regarding the applicability of rules, thresholds, and requirements for incident reporting and risk management depending on which asset or service is affected, this could result in overlapping and incoherent rules, causing both additional legal and operational uncertainty and costs.

The implementing regulation should therefore clearly specify how it applies to those entities whose core business is different from the provision of the services encompassed in the act, but which also provide these services as part of their portfolio. The act should help avoid duplication, support coherence, and prevent fragmentation through differing national cybersecurity policies.

Below, we present some general remarks on the draft implementing act, along with specific comments on the text of the draft regulation and its annex. However, due to the short timeframe and the highly detailed and technical nature of the document, it cannot be considered a comprehensive assessment.

General comments on the draft implementing act

- The Better Regulation agenda aims to ensure that EU legislation is evidence-based, transparent, and considers the views of those affected, creating sustainable policies and efficient, non-burdensome regulations. The Commission is also committed to streamlining reporting requirements with a goal of reducing them by 25%. To this end, an effective multi-stakeholder approach, increased use of international standards, and a cost analysis of the higher number of incident notifications should be pursued.

- The timing of this call for feedback leaves stakeholders with little time for analysis or review, and almost no prior interaction to assess the proposed requirements. This makes it challenging to ensure the efficiency, effectiveness, or proportionality of the detailed and technical measures outlined in the draft. In contrast, work on the implementation of DORA has been ongoing for months. Proper interaction with the private sector, which will ultimately implement the adopted measures, is essential.

- The timescale for the implementing regulation, which aims to be "binding in its entirety and directly applicable in all Member States" from 18 October 2024, appears too short. Not only is the act still in a draft stage with the target date for enactment being only three months away, but dependencies on potential delays in national legislation or the introduction of a unified notification portal must also be considered. We call for the introduction of a grace period of one to two years, which may need to be extended depending on the final outcome, especially if stakeholders' comments and interplay with other legislations are not sufficiently addressed. This will allow companies to review and prepare their network and information systems, supply chains, and operational procedures before the implementing act becomes binding.

- There are outstanding questions regarding the overlap with national regulations. For instance, what will take precedence between this implementing regulation and potential national-level implementing regulations on the same matters? What is the impact of the absence of national systems for reporting and registration? How will differing reporting criteria and incident taxonomy across Member States affect implementation? Addressing these ambiguities is crucial for ensuring coherent implementation.

- The draft implementing act does not specify how to determine the perimeter of concerned entities within a group of companies, nor the methodology for determining the networks and IT systems to which the security measures should apply.

- We welcome that the technical and methodological requirements described in the Annex generally align with ISO 27001, other common standards, and industry best practices, or offer these standards as an alternative to the proposed measures. However, we have noted some misalignment between the definitions and obligations provided by ISO certifications and the DORA delegated regulation, leading to complexity and legal uncertainty.

- The principle of proportionality is inconsistently applied across the different requirements of the regulation and its annex. Furthermore, several provisions may significantly diverge from existing practices in Member States or extend beyond the scope of current legislation, particularly concerning the risk taxonomy for incident reporting, audits, or supply chain management.

- The descriptions of a significant incident are overly extensive and detailed, with highly granular criteria that vary for different entities or parts of them. This complexity makes them unsuitable for all relevant situations and often lacks a causal relationship with the incident. Additionally, the definition may not accurately reflect the seriousness of an incident, as some criteria are too low and may lead to overreporting. Furthermore, if the criteria are alternative rather than cumulative, as is the usual practice, they may be too easily met, resulting in almost all incidents being considered significant. We recommend establishing a clear set of technology-agnostic requirements.

Detailed comments on the text

Proportionality

- The elaboration of 'proportionality' given in recital (5) is too limited for two reasons:
    - It is limited to situations where relevant authorities cannot implement the requirement. This should also be broadened to include situations where there is a better option to achieve the same goal.
    - the elaboration is limited to situations related to the size of the entity. This should be broadened to include situations where it is not available, less. efficient, etc.
- The risk-based approach should be embedded, among others, in the following items of the Annex: 3.2.3, 3.2.6, 6.2, 6.3, 6.7, 6.9, 9, 10, 11, and 13.

Significant incident

- Overall, the criteria for identifying a 'significant' incident are too detailed, and there is not always a causal relationship with such incidents. They do not apply to a broad range of situations. This could lead to a sharp increase in the number of incident notifications, overwhelming already overstretched Member State authorities. As a result, minor incidents may be reported at the expense of adequately addressing major incidents. Adhering to the risk-based approach, the scope of reportable incidents should be limited to core, high-volume, and high-impact services. Therefore, it is advisable to maintain broader thresholds aligned with the reporting practices established under implementing regulation (EU) 2018/151 under NIS 1.
- Examples of criteria in the draft act that will not necessarily lead to a 'significant' incident:
    - Article 3.1.a: A financial loss exceeding EUR 100,000 or 5% of annual turnover is too easily attainable and could lead to overreporting. For instance, IBM estimates the average cost of an incident at $4 million1. Even a minor incident affecting a small number of customers or requiring forensic analysis could surpass the proposed EUR 100,000 threshold for a large multinational. We suggest either maintaining the EUR 1 million financial loss threshold under the NIS1 Directive or increasing it to a higher percentage of turnover that more accurately captures incidents significantly impacting operations. Additionally, there

[1] IBM, Cost of a Data Breach Report 2023

needs to be clarity on how financial loss should be calculated and proven, as many incident-related costs are influenced expertise and resources rather than solely reflecting the incident's true significance.

- Article 3.1.f: The criterion related to successful, suspected malicious, and unauthorized access is relevant but overly broad in scope. Criteria should remain focused on the end impacts.
- Article 3.2: The criteria for assessing reputational damage are overly broad and extensive. (a) Mere media coverage does not necessarily indicate high reputational damage; other factors such as the extent of media coverage, volume of customer inquiries/complaints, etc., should also be considered. (b) Having to report an incident because two or three different users have made complaints is too strict. What if these users are consumers without critical business relationships, significant influence, or if their complaints do not concern significant issues? (d) Predicting customer loss is subjective and difficult to measure until it happens. Calculating the number of affected customers may not be appropriate as it represents the maximum potential impact rather than the actual number affected.
- Article 4: This requirement is too strict for entities that experience minor incidents repeatedly due to the nature of their operations, such as damage to cables/fibre or digital subscriber line access multiplexers (DSLAMs) from excavation or unforeseen power outages. There are no criteria indicating the potential risk to or the real impact on the entity's operations. We recommend raising the threshold proposed in Article 4 and to avoid overreporting of incidents, especially when they do not result from a malicious activity. Moreover, a materiality qualifier based on impact and relevance to critical services should be included.
- Article 5.a and b: One cannot determine if it is a significant incident solely based on the outage period mentioned. The issue may also lie within the customer's domain in the given situation. The thresholds of 10 minutes and 10 seconds response time are excessively low and, if enforced, could result in incidents being deemed significant when they are not. For instance, in the case of DDoS attacks, adjusting countermeasures may require more time than these thresholds allow.
- Article 7(a): The 10-minute reference for cloud service unavailability is overly short and significantly deviates from market standards of what is considered a critical incident.
- Articles 7, 8, and 10: Service level agreements are commercial agreements with business customers, and it is undesirable for these agreements to become part of compliance rules. This is a commercial matter for which fines can be imposed by the regulator. As previously indicated, these thresholds are excessively low and do not accommodate the varying SLAs required for different types of services. Regarding the impact on data, the mere fact that data is affected should not be the sole criterion; the quantity and sensitivity of the information involved should also be considered to determine the significance of an incident.
- Articles 7, 8, 10, 11, 12, 13: Several articles suggest a threshold based on "a suspectedly malicious action". We recommend removing the word "suspectedly" as it makes the threshold too vague as any incident may be suspected to occur as a result of a malicious

action. We recommend that incidents are reported once an entity establishes evidence of malicious activity.

- Article 10a: Mentioning a specific duration of 10 minutes is not logical; it adds unnecessary detail and may not fit every situation.
- Article 10.c: A notification must always be made when the availability of a service is affected. This means that an operator can no longer provide best-effort services and cannot offer experimental services without having to report interruptions.
- Article 14.b: Entities are required to maintain an uptime of 99.99%, regardless of what is agreed upon with their customers.

Technical and methodological requirements (Annex)

- To achieve the desired high security levels, alignment with existing standards is crucial to ensure harmonization. This alignment will be particularly beneficial for companies already adhering to these standards, reducing the extensive efforts required by the detailed requirements of the implementing regulation. It would be beneficial to provide an official mapping to internationally recognized industry standards such as ISO 27001, IS0 2230, ETSI EN 319 401, C5, SOC2, or EUCS.
- The use of international standards such as ISO 27001 and alternatively or additionally, CSA STAR Level 2 for cloud services or a SOC 2 Type 2 report for managed services, should be considered as the primary tools for risk assessment and security management, or at least as possible alternatives to the requirements outlined in the current draft implementing act. NIS2 encourages the use of "relevant European and international standards", and its preamble suggests utilizing the ISO/IEC 27000 series for cybersecurity measures. ISO 27001 is endorsed by ENISA and is widely accepted internationally. Many companies already use these certifications as a standard practice with other entities. This makes ISO 27001 a logical choice for NIS 2 compliance, facilitating harmonization, rapid market deployment, efficiency, and alignment with existing certification tools and mechanisms. Mapping NIS 2 obligations to ISO 27001 and ISO 27002 procedures demonstrates its broad applicability as a reference for risk management, rather than creating a new cybersecurity management approach from scratch, which could diverge from current standards and national practices, potentially hindering interoperability.
- Item 1.1.1: The list is too prescriptive and includes items of questionable value. E.g., if the policy clearly states the mandatory requirements for the entity that must be met – why would it be necessary to include a commitment to allocate appropriate resources for its implementation?
- Item 2.1.2 (a): For the avoidance of doubt, we recommend including a precise reference to the European and international standards that are expected to form the basis for the entity's risk management methodology instead of leaving room for interpretation. In case there are different methodologies that could be followed, the implementation guidance should not limit the entity's flexibility to choose an appropriate one.

- Item 3.2.3: This is an overly extensive list of logs to implement, maintain, and review. For many entities, this is likely to be complex to achieve within the required timelines. It could be interpreted that all traffic must be logged, which would require specific and costly infrastructure (e.g., to store the information). Entities should have the flexibility to define events of interest in a flexible way per event source following a risk and threat model-based approach. Overlap with 11.2.2 (f) and 11.5.2 (d) which should be avoided.
- Item 3.2.5: There may be technical, cost or legal reasons for not storing all logs in one central location – the guidance shouldn't dictate how controls are being implemented.
- Item 3.2.6: Requiring redundancy for logging and monitoring (detective) seems to be unbalanced – what about redundancy for preventative controls? Again, the guidance shouldn't dictate how controls are being implemented.
- Item 3.4.2 (b): The requirements for quarterly reviews of recurring incidents seem to be quite prescriptive. Entities should have more flexibility to organize their incident review process.
- Item 4.2: Currently, low-cost services are available on the market that do not include backups. It is essential to inform customers properly to avoid any issues in case of incidents. The question is whether, due to security standards, these offers should be discontinued despite their low price. Cloud providers are increasingly asked to offer backup services systematically, even when the service does not request it. This concern also relates to the environmental footprint requirements of cloud services.
- Items 4.2.4 and 4.2.5: The intention of these requirements and the specific scenarios where they apply are not clear. Requesting 'at least partial redundancy' is not clear and does not provide helpful guidance.
- Items 5 and 6: Many of the supply chain requirements are novel and may diverge from existing regulations or ongoing efforts for other legislation (e.g., DORA). They could also prove excessively burdensome for SMEs, potentially leading ICT companies to exclude certain suppliers altogether to comply with the proposed implementing legislation. Enhancing supply chain cybersecurity necessitates careful consideration, including a risk-based approach for each supplier, assessing associated costs, and analyzing the broader impact on the ecosystem.
- Item 5.1.2. (d): This provision may not be proportionate as it could increase costs and create management difficulties, potentially counteracting its intended security benefits. The diversification of supply chain security should be assessed considering both the risks involved and the feasibility of implementation.
- Items 6.7 and 6.8: Network security implementation plans should be evaluated as the network evolves, and many of the proposals may be disproportionate. Among others, the term 'latest generation network layer protocol' should be defined.
- Item 10.2: Due to applicable laws, particularly labor and privacy regulations, employers will be able to conduct only very limited background checks. In some Member States, background checks may even be prohibited.
- Item 11.3.2 (d): The restriction of administrator accounts to connect to system administration systems does not align with basic IT operation's needs.

- Item 11.4: The term 'system administration system' should be defined.
- Item 12.1.3: While processes need to support the reclassification of assets, the performance of periodic reviews which would come at a high cost due to the high number of assets to be considered and doesn't seem to be proportionate to the potential risk that the classification of an asset isn't being upgraded as required resulting in an insufficient protection and handling of the asset.
- Item 12.3.2: The regulation should not prescribe the way data is being protected. There are secure ways to manage removable media.
- Item 13.2.2(b): The term "control thresholds" should be defined as it is unclear what this means in the context.

Policy contacts:

Paolo Grassia
Senior Director of Public Policy, ETNO
grassia@etno.eu

Pierantonio Rizzo
Director EU Affairs, GSMA
prizzo@gsma.com