bitkom

Position Paper

Implementing act under Articles 21 and 23 of the NIS2 Directive

Bitkom's response to the public consultation

Content

1 Summary

The Cybersecurity Committee of the European Commission has issued a draft implementing act on the NIS2 directive (EU) 2022/2555. It serves the purpose of aligning the risk management requirements for some operators from the digital sectors with cross-border activities at the EU level. Furthermore, it is specified in which cases an incident must be considered significant.

Bitkom welcomes the Commission's initiative to seek a clear and harmonized understanding of the NIS2 directive (EU) 2022/2555 for affected companies. It is in the interest of the industry to have an equal ground with a European framework across all member states. We therefore appreciate this opportunity to participate in this consultation and to contribute to the public consultation on behalf of our members. This position paper examines the individual articles of the implementing act, explores their effects on businesses and offers improvements, if needed.

Before looking at the individual articles themselves, we would like to highlight the manner in which this regulation was developed. Despite the Commission's advocacy for a multi-stakeholder approach, the process was largely conducted behind closed doors without adequate industry involvement from the outset. For true collaborative policymaking, the Commission should incorporate input from industry stakeholders from the beginning stages to ensure that the regulation is both practical and effective.

We observe that some criteria for determining significant incidents across the regulation are subjective and lack clear, measurable standards. While some criteria focus appropriately on the impact of an incident, others do not align with this focus. It is essential that the regulation remains centred on the end impacts of incidents. For instance, if malicious access results in surpassing other thresholds, it will naturally be reportable under those terms. Hence, maintaining a clear focus on the actual impacts will prevent unnecessary ambiguities and ensure that reporting requirements are straightforward and actionable.

The definition of users and customers remains ambiguous throughout various sections of the implementing act. While the recitals and Annex provide a definition, this is conspicuously absent in the sections pertaining to incident reporting. The NIS2 directive (EU) 2022/2555 itself lacks a general definition of "user." The term "users" could encompass either end-users or enterprise customers, each category bearing distinct implications and necessitating separate thresholds to reflect their unique characteristics. To enhance legal certainty and streamline compliance and reporting processes for companies, we advocate for a precise definition and clear distinction between "customers" and "users."

The present implementing act regulates measures relating to service operators from the digital sector, and all services, except for the "Trust Service Providers," fall under Article 26(1)(b) of the NIS2 directive (EU) 2022/2555, making them subject to the jurisdiction of the member state where the company or group is headquartered. This includes central registration. However, Trust Services are subject to the jurisdiction of the EU member state where they have their local registered office (Article 26(1)). This distinction could pose challenges for the implementation of the implementing act throughout the EU and potentially conflict with the eIDAS regulation. We note that

Article 21(5) of the NIS2 directive (EU) 2022/2555 suggests that trust service providers should already be included in the scope of the implementing acts.

The Annex imposes stringent security requirements on affected companies, mirroring established standards but lacking explicit references and being overly prescriptive. This independent definition of "state of the art" deviates from the New Legislative Framework (NLF), creating significant burdens for companies trying to align with industry norms. Any modifications to the implementing act would necessitate a bureaucratic amendment process. To achieve high security levels and ensure harmonization, the Commission should align with existing standards. This alignment would mitigate extensive efforts for companies already adhering to these standards. Early availability of these mappings is critical for regulated entities to conduct gap analyses in preparation for NIS2 compliance.

There are also general questions that remain unanswered, particularly regarding the overlap with national regulations. For instance, what applies to companies that fall under both this regulation and the German NIS2 implementation law? Furthermore, what happens if the implementing act comes into force before the German implementation law? There is a lack of clarity about what applies to companies that fall under the implementing act but do not yet have national systems for reporting and registration. Addressing these general ambiguities is crucial for ensuring coherent implementation across member states.

To answer the mentioned questions and hurdles, we suggest a targeted approach in line with recital (21) of NIS2 Directive (EU) 2022/2555. This recital acknowledges the complexity that businesses face, particularly those with multifaceted operational structures that may straddle the definitions of both essential and important entities or engage in activities that are variably covered by the Directive. We urge the Commission to actively follow up on the suggested guidance from recital (21), providing Member States with clear, detailed instructions on how to apply the Directive's scope and assess the proportionality of measures. This guidance should specifically address the needs of entities with complex business models, ensuring they receive adequate support to navigate regulatory obligations and maintain compliance.

2 Article 3 - Significant incidents

Overall, we appreciate the Commission’s intention to define clear, explicit reporting thresholds. However, we are concerned that some of these thresholds are so low or so broadly defined that they will be difficult or impossible for companies to implement in practice. In addition, they would bind significant internal resources, which could hinder companies to focus on critical incident response and mitigation activities.

We would generally advise against overreliance on quantitative metrics to define thresholds for incident reporting, especially if thresholds are imposed through formal

legislation. As an alternative to these proposed thresholds, we would recommend that the Commission's implementing act is restricted to qualitative criteria and accompanied by separate qualitative and quantitative non-legislative guidance, complete with explanations and examples of how entities should assess an incident and when it should be reported. We recognize that the proposed metrics can be useful benchmarks for comparing incidents and facilitating the response process. However, these metrics should only be helping organizations to assess whether an incident is "significant" and should be reported, rather than a strict requirement. Each essential or important entity is different, and defining incident thresholds using strictly quantitative metrics is likely to skew reporting to specific types of incidents for specific types of services.

Article 3(1)(a) determines that incidents with regard to relevant entities that have caused or are capable of causing losses over €100.000 or 5 % of the relevant entity's annual turnover are to be considered as significant. It is decisive whichever of the two possible options is lower. An entity shall report these significant incidents without delay and at the latest within 24 hours, however it may be impossible to assess this impact within the given time. The information on financial losses caused by the incident may be more suited for the final report one month after the incident, but not as a triggering point to identify whether the incident is or is not significant, as the calculation of costs would take longer than the reporting deadlines (24 hours respectively 72 hours).

For a large multinational organization, even a small incident affecting one or two customers or requiring forensic analysis can easily exceed the threshold of €100,000. In many cases, the costs associated with the incident would not necessarily connote significance but would instead represent the expertise and the resources used to address any incident, even small ones. This issue would be resolved by maintaining the current financial loss threshold under NIS1 directive (EU) 2016/1148, which required reporting if the damage caused by an incident exceeds EUR 1,000,000. In our experience, the high damage threshold better reflects the impact of an incident that would be considered "significant" and would minimize the risk of overreporting non-significant incidents.

We further suggest for Article 3(1)(a) to remove the "whichever is lower" qualifier or include thresholds relating to different organizational sizes. Including the "whichever lower" caveat for the monetary threshold of impact as it could have the unintended side effect of inundating cybersecurity regulators with notifications, and it may be difficult to identify incidents which are more significant for smaller organizations. Furthermore, we consider the choice of "capable of" to be in the same category as "suspects." It's overbroad and difficult to assess during an incident. Arguably, any incident is "capable of" inflicting €100,000 if it catches on at the wrong time. With the very large scope in Recital 34, it would be reached too quickly, especially for larger companies.

According to Article 3(1)(b), incidents are considered to be significant if they have caused or are capable of causing considerable reputational damage. However, this is highly subjective and cannot be measured objectively.

The mention of "death" and "health of individuals" in Article 3(1)(d) and Article 3(1)(e) introduces the potential for associating incidents with events beyond the control of

affected companies. To ensure relevance to cybersecurity, these criteria should specify that incidents must be IT-related, thereby preventing an overly broad scope. Mechanisms for assessing causality and attributing actions should be clearly defined to establish uniform, harmonized, and precise reporting obligations for the obligated parties.

For the criteria of “a successful, suspectedly malicious and unauthorized access to network and information systems occurred” in Article 3(1)(f), we note that it does not focus on the impact of an incident like the other criteria in this implementing act. We think this regulation should remain focused on the end impacts. Malicious access that results in one of the other thresholds being surpassed, would be reportable anyway. Article 3(1)(f) should therefore be deleted as well as the provisions in Articles 7 and 8.

To determine the existence of a considerable reputational damage of an incident the draft requires relevant entities to take into account whether “the incident has been reported in the media” and “has resulted in complaints from different users or critical business relationships” according to Article 3(2)(a) and 3(2)(b). These two seem excessively broad/likely to result in a lot of incident reports. There is no clarification provided as to the scope of “media” (e.g. this could also include blogs with negligible reach). We consider the perfect tense used here to be problematic, as it covers both past and current events. This would suggest extensive monitoring measures and reporting obligations without sufficient time to assess the facts. We therefore suggest the use of the past tense. Also, having more than one customer complaining about a service issue is a very low standard. The phrasing "different users or critical business relationships" is furthermore unclear. How many users have to complain for it to meet the standard of “complaints from different users”? How large or important does a business relationship need to be for it to be considered “critical”? In our experience, even the most trivial of outages can result in a handful of customer complaints.

Article 3(2)(c) should contain a time-specification, such as “exceeding 72hours”, which would be the time to report in more detail on the incident. Since any incident may cause temporary inability to meet obligations.

The criterion of likely losing customers with a material impact on the business in Article 3(2)(d) is another point that may be very difficult for the company to judge. We therefore ask for a more objectively based approach.

The term "user" in Article 3(4)(a) and (b), along with other Articles, creates ambiguity regarding whether it refers to corporate customers (B2B) or end users. It is imperative to distinguish between these groups, as different threshold values should apply to corporate customers and end users. In the context of B2B transactions, the number of end users is typically unknown, necessitating clear differentiation to ensure appropriate application and compliance.

In general, undefined legal terms such as "considerable", "media" or "material" are often used. We suggest the creation of legal definitions of undefined terms that are used within the implementing act in order to create uniform, harmonized and clearer reporting obligations for obliged entities.

3 Article 4 - Recurring incidents

Incidents not deemed significant individually will be considered collectively as one significant incident if they occur at least twice within six months and share the same apparent root cause. This shall ensure repeated issues with a common origin are treated as a major concern. However, these two criteria are too broad. As currently drafted, several types of incidents, such as those resulting from human error, would require notification if they recur within six months, even if they are not significant. We recommend including a materiality qualifier based on the impact and relevance to the critical service to minimize the notification requirements for incidents that would otherwise create an administrative burden for NIS2 cybersecurity regulators. Without this qualifier, legal ambiguities may arise. For instance, if a typing error by different employees from different departments affects various trust services, does this constitute the "same apparent root cause"?

One possible solution to the problem could be to clarify that the recurring incidents are significant only if, collectively, they meet the threshold for significant incidents as described above. Otherwise, it can be inferred that any (even “insignificant”) recurring incidents are to be considered as significant. Another proposal would be to replace the wording “shall” with “may”. Thereby, the businesses are given the possibility to appreciate if the incident is problematic, as well as the incident’s real impact.

Generally, Article 4 should be reviewed to oblige organizations to have a holistic and long-term vision on their incidents, giving them the capacity to detect incidents having the same cause, while having the possibility to better assess their impact.

4 Article 7 - Significant incidents with regard to cloud computing service providers

We consider the general specification of when an incident shall be considered as significant as far too detailed. This assessment as also applies to the specific provisions for cloud computing service providers. In addition, the indicated thresholds are too low and seem to be arbitrary. Consequently, the problem arises that the specification does no longer do justice to the individual case. This will lead to a disproportionate number of notifications overloading the supervisory authorities and overburden companies. In the spirit of a risk-based approach, the scope of reportable incidents should therefore

be restricted to core, high-volume and high impact services, excluding microservices and sub-products. Larger cloud providers typically offer thousands of microservices and sub-products, which individually do not impact critical services.

As currently drafted, maintenance operations leading to service unavailability should not be classified as significant incidents. We support this decision, as it prevents operators from having to report anticipated outages to NIS2 regulators. However, the clarification for this exemption is only found in Recital 31 and not in Article 7 itself. This issue applies to other clarifications as well (e.g. Recital 4 on the "risk-based approach"). We request that these clarifications be explicitly included in the articles to avoid any ambiguity.

The threshold for reporting based on service unavailability for more than 10 minutes according to Article 7(a) is too short. In some cases, 10 minutes might be a significant incident. However, there are cases in which such a technological failure is at least harmless, if not unimportant. For example, certain kinds of business software are in most of the cases used during certain hours of working days. If those are not available for 10 minutes on a weekend or at nighttime, this cannot be considered a significant incident. Criteria should put a stronger focus on impact criticality instead of fixed time frames.

The issue with the reference to "customer service level agreement" in Article 7(b), is that service level agreements are drafted to ensure that customers are receiving the full value of their services, not necessarily to identify and remediate incidents that have a significant impact. Accordingly, to the extent that the Commission wants to include a consideration of latency or degraded service when assessing an incident, they should tie it directly to the impact on customers and end users in the EU, not on contractual service levels or other commercial arrangements with customers that may be unrelated to an incident's actual impact. We further ask to clarify whether the term of "cloud computing service users" in Article 7(b) refers to end-users or business customers and adjusting the criteria to reflect B2B/B2C practicalities. This can provide more clarity and avoid ambiguity in the context of SLA breaches.

Article 7(c) appears to impose identical requirements regardless of the presence of an SLA. This approach lacks logical consistency, as lower SLAs can be negotiated for reduced service levels based on customer demand. Mandating them to have the same high level of service as agreements without SLAs would place a significant burden on operators and represents an undue intervention in B2B contracts, potentially exceeding acceptable regulatory limits.

Article 7(d) provides that an incident shall be considered significant when the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the cloud computing service is compromised with an "impact" on more than 5 % of the cloud computing service users. However, it is not clearly defined what an impact, in that context, actually is. We propose an "impact" to be defined according to a more risk-based approach, by referring instead to a significant impact.

In addition, "related to the provision" is very broad. Applying a risk-based approach, we propose a rephrasing into "required for the provision".

The comments above apply to other articles that include the same criteria (e.g. Article 9), respectively.

5 Article 8 - Significant incidents with regard to data centre service providers

Article 8(e) states that an incident shall be considered significant under Article 3 when physical access to one or more data centres operated by the provider is compromised. This provision should either be deleted or amended to specify that it must have resulted in actual damage.

6 Article 9 – Significant incidents with regard to content delivery network providers

The criterion of unavailability in Article 9(a) for more than 10 minutes leaves room for interpretation of what is meant with a single “content delivery network” (CDN) in this case. NIS2 defines “content delivery network” as “a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers.” In our members’ experience, organizations rarely operate CDNs that can be classified as discrete networks with clear service and up times. In practice, it is highly unlikely for a CDN to fail as a whole. And if individual Points of Presence fail, the impact may still not be significant. We would therefore recommend deleting Article 9(a) entirely.

According to 9(c), any form of impact on the availability of a CDN in the absence of SLAs would trigger an incident notification. This is way too broad and should be aligned with Article 7(c) relating to cloud computing services, which qualifies the impact with additional criteria (impacted users and duration).

We note that the comments on the criteria in Article 7 apply equally to those criteria in Article 9.

7 Article 10 - Significant incidents with regard to managed service providers and managed security service providers

The way the definitions of a significant incident are described, for a managed service provider (MSP) this means that a countless number of incidents would be affected. Threshold should be heightened or replaced by qualified criteria. It is furthermore unclear, how the implementing act draws a line for businesses that outsource services to MSPs. The current state of the draft bares the risk of uninvolved companies could be involved by responsibilities of their service providers.

Depending on the contract, there are high penalties for breaching SLAs. In such a case, damages could quickly exceed €100,000, even if the impact on the customer is minor. Damage can also be high if it takes a long time to resolve and process an incident (including turning it into a problem and lessons learnt, etc.), resulting in internal costs.

Almost every incident can lead to reputational damage if customers publicly discuss the incidents or if they complain (Article 3(2)(b)). This is again independent of the severity or actual reasons for the incident. Lastly, incidents whose root cause has not yet been found or resolved may well occur several times within 6 months (Article 4).

8 Article 14 – Significant incidents with regard to trust service providers

In general, it should be noted that a massive tightening has been made in the area of resilience, especially compared to the previously applicable guidelines. In our view, the requirements for trust services are far too strict. In the case of trust services, a distinction must be made between the individual services, functionalities and components when it comes to the resilience criterion. Ultra-high availability, as provided for in points Article 14(a-c), only makes sense and is standard market practice for components that are necessary for validation, in particular OCSP responders. In the case of signing services and comparable trust services, however, such ultra-high levels of availability are neither customary nor necessary. For example, it is not clear why an

eleven-minute outage of an application for creating advanced signatures for contract documents at three o'clock in the morning, without a customer or user even noticing it, should constitute a reportable incident. Significantly lower availability values apply here, as is customary in the industry. At this point, it should be noted that even compliance with an annual availability of 99.3% (in relation to lit. b), for lit. a) even above 99.99%), which can certainly be described as standard market practice, would regularly trigger a reportable incident in accordance with the thresholds set out here. The thresholds set out here are therefore far too strict and unrealistic. An adjustment and differentiation between individual trust services and components is therefore essential.

With regard to the availability of trust services, contractually agreed SLAs must also be taken into account when determining an incident. It is an obvious contradiction in terms of temporary service failures do not constitute a breach of contract vis-à-vis the customer but do constitute a reportable incident. Therefore, it should be included as that the service outages must exceed contractual or other statutory availability requirements as well as a measurement for the actual impact on customers and end users in the EU in order to trigger a reportable incident.

The same applies to maintenance windows announced to customers in advance; these also do not represent a breach of resilience in the narrower sense but would have to be reported as an incident in accordance with this text. Therefore, an explicit exception for maintenance windows announced in advance should also be included in order to avoid redundant, meaningless incident reports. Such an interpretation within the recitals is not sufficient, as recitals have no legal effect according to the jurisdiction of the ECJ.

As the threshold value of 1% in Article 14(c) relates to the respective trust service, it is quickly reached in the case of differentiated and specialized services with very few customers, even if only a single customer is affected and the outage therefore has very manageable effects. In this case, the assumption of a reportable incident is also not in the best interest. We therefore propose that the 1% should be based on the total number of all customers of the TSP or that differentiated, interest-based assessment factors and thresholds be created for this point.

"Large delays" is also an undefined legal term and should therefore also be legally defined within the implementing act or concrete values should be specified in order to create uniform, harmonized and clearer reporting obligations for the obligated parties and to avoid legal uncertainties. Similar to Article 7(b) and 9(e), there is a lack of clarity for understanding the term “customers” in Article 14(c). A clear distinction between "customers" and "users" would provide more legal certainty for companies.

Furthermore, in Article 14(d), the compromised physical access to areas where network and information systems are located and to which access is restricted, should be scoped to the network and information systems used to provide the trust services.

9 Article 16 – Entry into force and application

The timeline for entry into force following national implementation and registration requires clarification. The current timeframe for demonstrating compliance is unrealistically short. A grace period should be introduced to allow for the establishment of relevant processes based on the final thresholds. Additionally, dependencies on potential delays in national legislation or the introduction of a unified notification portal must be considered.

10 Annex

The annex imposes stringent security requirements on affected companies, closely mirroring established standards. Nonetheless, it lacks explicit references to these standards and is overly detailed and prescriptive, seeking to define "state of the art" independently of EU or international benchmarks. This methodology results in significant burdens for companies striving to reconcile these requirements with industry norms. Furthermore, it diverges from the New Legislative Framework (NLF), which stipulates that EU laws and regulations should avoid being overly detailed and prescriptive in technical matters. Any necessary modifications to a requirement in the implementing act would necessitate an amendment to the regulation itself, leading to a protracted and bureaucratic process.

To achieve the desired high security levels, the Commission should align with existing standards to ensure harmonization. To enhance the alignment with internationally recognized industry standards and compliance frameworks, the implementation of an official mapping to standards such as ISO 27001 is essential. While European standards such as ETSI EN 319 401, C5, SOC2, or EUCS are also valuable, international standards offer the broadest applicability for global business operations. The successful mappings already established for frameworks like NIS1 and GDPR serve as exemplary models that can be replicated. This alignment would be particularly beneficial for companies already adhering to these standards, thereby mitigating the extensive efforts necessitated by the current detailed requirements. If, in the view of the EU Commission, existing standards do not cover all necessary aspects, additional requirements can of course be defined in addition to the referencing of the standards, which can then be additionally audited or incorporated into the standards when they are updated. It is critical that these mappings be made available as early as possible, so that they can be most useful for regulated entities to carry out gap analysis and gap closure in preparation for compliance with NIS 2.

Recital 4 stipulates that the application of above-described cybersecurity risk-management measures must adhere to the principle of proportionality, contingent on the varying risk exposure of entities. The criteria for assessment include criticality, risk exposure, size and structure of the entity, and the likelihood and severity of incidents.

We endorse this risk-based approach and urge for explicit clarification within the Annex to prevent ambiguity among entities when implementing cybersecurity risk-management as per the requirements of the Annex.

Chapter 3(2)(3) contains provisions that require further precision. Specifically, (a) could be interpreted to mean that all traffic must be logged, which would necessitate specific and costly infrastructure for information storage. To prevent this misinterpretation, it is recommended to explicitly include the notion of "where appropriate" in the text. Furthermore, (h) states that the use of system resources should be monitored but not logged. This requirement is not suitable for this section and should be removed.

In Chapter 4(2), the use of backups needs to be discussed. Currently, low-cost services are available on the market without backups, and it is essential to properly inform the customer to avoid issues in case of incidents. The question arises whether these services should be discontinued due to security standards despite their affordability. This issue is also relevant in relation to the cloud's environmental footprint, as cloud providers are increasingly required to offer backup services even when they are not necessary.

Additionally, the provision in 4(2)(5) lacks clarity and requires further explanation.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Felix Kuhlenkamp | Policy Officer Cybersecurity
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Responsible Bitkom Committee
AK Sicherheitspolitik