DIGITALEUROPE

02 August 2024

Optimising NIS2 risk management and reporting compliance

Executive summary

The revised Directive on measures for a high common level of cybersecurity across the Union (NIS2) will expand the scope of the entities and sectors required to adopt comprehensive cybersecurity measures.[1] Effective implementation of NIS2 is necessary to achieve its intended goal of increasing the level of cybersecurity across the EU.

To this end, the European Commission is preparing an implementing act that outlines the technical and methodological requirements for cybersecurity risk-management measures and further specifies the criteria for determining when an incident is significant for relevant entities.[2]

In this paper, we put forward key concrete recommendations on the proposed implementing act:

- The implementing act should avoid overly detailed technical requirements. Some requirements, such as identifying the root cause of an incident or recovery objectives in business continuity plans, may not always be possible and should be revised. The final act and annex should allow for differences in resources, capacities and risk profiles between entities, including between large and smaller entities.
- The implementing act should reference existing cybersecurity standards. ENISA should promptly develop guidance on how these standards align with NIS2 requirements. A multistakeholder forum should be established without delay to identify the best available standards and deployment techniques.
- The one-stop-shop principle should be reinforced for efficient compliance and reporting, with entities communicating with a single dedicated authority in their main establishment. This principle should be optionally extended to other entities under NIS2.

[1] Directive (EU) 2022/2555.

[2] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- There are limits to what service providers can control, and they should be responsible only for environments they control, not those solely under customers' control.
- The annex appears to mandate a 'three lines of defence' model, appropriate for financial services but disproportionate for other entities. Organisations should have the flexibility to select a risk management approach that suits their needs.
- The requirement to log all incoming and outgoing traffic should either be removed or include information 'where appropriate.' Counterproductive requirements, such as centralised log storage, should be avoided, and physical and IT security events should be separated for clarity.
- Risk management within the supply chain should focus on critical direct suppliers or service providers to ensure a proportionate approach. Open-source software (OSS) should be excluded from the supply chain requirements.
- Significant incidents should be defined by meeting two or more criteria to avoid unnecessary burden and overreporting. Thresholds for significant incidents should focus on actual impact, such as a percentage of annual turnover for financial loss. Recurring incidents should focus on significant impacts affecting many customers.
- Timelines around availability and service level agreement (SLA) incidents should reflect commercial realities and service criticality. Reporting should focus on confirmed malicious actions following NIS2's risk-based thresholds.
- The clock for determining when an entity became 'aware' of an incident should start when the entity knows with a 'reasonable degree of certainty' that a significant incident threshold has been met.
- The implementing act will apply from October 2024, a very short timeframe for demonstrating compliance. We urge for one-year grace period, allowing entities to fully understand the requirements and develop implementation strategies.

Table of contents

Cybersecurity risk management measures

Level of prescriptiveness

The implementing act should avoid being overly detailed and prescriptive on technical matters.[3] Embedding technical and methodological requirements in a legal document would necessitate amendments whenever the state of the art evolves, leading to a cumbersome and lengthy update process.

Significant differences in resources, capacities and risk profiles between large and small entities should be considered. Compliance requirements designed for larger organisations may disproportionately burden smaller entities. Although Recital 5 acknowledges this issue, it is not consistently reflected in the annex. The Annex also contains ambiguous language, making compliance difficult. For example, terms like 'distinct systems' (clause 6.7.2) and 'systems administration systems' (clause 11.4) are undefined, complicating compliance efforts. Similarly, phrases such as 'one network and information system connecting to another' (Recital 19) and 'commitment to provide the appropriate resources' in Art. 1(1)(1)(g) lack clarity. We suggest simplifying the language to specify that policies should include provisions related to resource allocation.

Some annex requirements are unrealistic and should be revised. For instance, clause 3.6 requires identifying the root cause of an incident, which may not always be possible. Clause 4.1.2 mandates recovery objectives in business continuity and disaster recovery plans, which may not be suitable for all entities due to service level agreements with customers. Entities often have tailored mechanisms for incident management, including business continuity and disaster recovery plans. The language should be adjusted to account for different contexts, such as global companies with group-level risk management measures.

We propose adding an article to the implementing act stating that the annex measures are guidelines to be applied with consideration of appropriateness, proportionality, risk-based approaches and implementation costs. The article should also clarify that alternative compliance pathways that achieve the same protection objectives should be considered equivalent.[4]

---

[3] Whilst NIS2 is not a market access product legislation, a similar approach to the New Legislative Framework (NLF) should be followed. This framework stipulates that EU laws should not be overly detailed and prescriptive on technical matters. Starting with the NLF's predecessor, the New Approach, EU law has focused on 'essential requirements' and left technical details to European harmonised standards, which led to the European standardisation policy supporting such legislation. The NLF expanded on this by including elements for effective conformity assessment, accreditation, market surveillance and control of non-EU products. The approach in the draft implementing act's Annex deviates from this established framework. For our position on EU standardisation policy, see DIGITALEUROPE, *Assessing merits and bottlenecks in Europe's standardisation system*, available at https://cdn.digitaleurope.org/uploads/2024/07/DIGITALEUROPE_Assessing-merits-and-bottlenecks-in-Europes-standardisation-system_.pdf.

[4] To this end, Recital 15 should be clarified or amended to state that sector-specific laws, e.g. the Medical Device Regulations (Regulations (EU) 2017/745 and 2017/746), are equivalent to the Cyber Resilience Act (CRA, COM/2022/454 final) and do not require separate certification

Alignment with existing standards

The annex detailing the technical and methodological requirements for cybersecurity risk management is overly prescriptive and extensive, with many requirements already covered by existing European and international standards.

The implementing act should reference, or align with, international cybersecurity and information security standards, ensuring the harmonisation and clarity necessary for industry, as these standards already encompass many cybersecurity requirements.[5] Compliance with ISO 27001 can directly demonstrate adherence to the cybersecurity risk management measures of Art. 21 NIS2, as evidenced by Member States already recognising compliance with NIS cybersecurity requirements through ISO/IEC 27001 certification or compatible national standards.[6]

Sector-specific information security standards also exist that can align with NIS2 security requirements.[7] Clear guidance on the extent to which these standards fulfil the NIS2 security requirements must be provided by the time the implementing act goes into effect. If additional requirements are necessary, the Commission should collaborate with standards organisations.

ENISA has previously published guidelines mapping security requirements against international standards, providing a roadmap for compliance.[8] Similar guidelines for NIS2 and the draft implementing act are essential, allowing companies sufficient time to address compliance gaps.

The extensive list of requirements in the annex will significantly impact SMEs, increasing their compliance efforts. Challenging requirements for SMEs include monitoring and logging (chapter 3.2), supply chain security (chapter 5.1) and audits (clause 5.1.4(f)). Streamlining obligations and aligning with existing standards will facilitate compliance and reduce administrative burden, particularly for SMEs.

Multistakeholder forum

under the Cybersecurity Act (Regulation (EU) 2019/881). Fragmented requirements would create disproportionate and unjustified market access barriers, conflicting with single market policies.

[5] Notably, these standards include ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 22301.

[6] For example, BSI IT-Grundschutz in Germany, E-ITS in Estonia and the Cyberfundamentals Framework in Belgium.

[7] These include CEN/TS 18026 for cloud services, ETSI EN 319 401 for trust services conformity assessment, EN IEC 62443 for OT environments and NIST standards like NIST SP 800-53.

[8] See ENISA, *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers*, available at https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers.

The relationship between the Annex requirements and the multistakeholder forum mentioned in Recital 7 of the draft implementing act is unclear.

This forum, which will include the Commission, ENISA, competent authorities, industry and other stakeholders, should have been established earlier to identify relevant standards and guidelines.

Mapping the security requirements to well-known international and European standards would have provided a solid foundation for compliance, making the process more practical compared to introducing a new set of requirements.

The multistakeholder forum should be established without delay to address this gap.

Maintaining the one-stop shop

The implementing act should reinforce the practical implementation of NIS2's one-stop-shop principle. We note that whilst this principle is mentioned in Recital 113 NIS2, it is not reflected in the draft implementing act.

To ensure a secure and effective single market, the main establishment principle should be emphasised. This is particularly important for reporting obligations, ensuring that relevant entities communicate with a single dedicated authority in their country of main establishment.

Additionally, we believe that the clarity and certainty provided by the one-stop-shop principle should be optionally extended to other entities under NIS2, even if not covered by this implementing act. We suggest including an article or recital specifying that the annex can also be used by other entities, such as digital infrastructure providers, service providers and digital providers, to demonstrate their conformity with the Art. 21 NIS2 measures.

Interplay with national transposition legislation

The relationship between the implementing act and national transposition laws must be clarified. As it stands, Member States can theoretically add to the implementing act's measures but cannot practically account for its provisions due to the simultaneous adoption deadline of 17 October 2024.

We recommend including an article or recital in the implementing act specifying it will be directly applicable to relevant entities even though NIS2 itself is not directly applicable, without needing to enact the implementing act's provisions into national legislation. Any national provisions conflicting with the implementing act should be disregarded.

Aligning requirements to a shared responsibility model

Service providers can outline, through their own risk assessment measures, guidelines or recommendations, how customers can best secure the infrastructure, use encryption tools, and configure the control environment and

threat detection. However, there are limits to what service providers can control and directly influence. Whilst certain components are managed and controlled by the service provider, others are controlled by the customer.

These limits should be recognised by the implementing act and by authorities during oversight. Service providers under the implementing act should be responsible only for reporting incidents and securing measures within the environments, i.e. the infrastructure, they control. Their responsibility should not extend to environments solely under customers' control.

In the cloud services sector and many platform services, this approach is known as the 'shared responsibility model,' allocating responsibilities between service providers and customers based on the level of control and information each possesses.[9]

Risk management policy

Sections 2.1–2.3 of the annex appear to mandate a 'three lines of defence' model, a risk management approach originating in financial services due to the sector's low-risk appetite, the high value of its data and assets, and its dependence on operational resilience and integrity. This model ensures rigorous compliance and management oversight, which is appropriate for the heavily regulated financial sector but disproportionate for the entities addressed in the annex.

Organisations should be allowed flexibility to select a risk management approach that best suits their needs, rather than mandating a specific methodology. For example, the requirement for relevant entities to establish and maintain risk criteria should be based on the services provided, not on an entity-wide basis.

Furthermore, both section 2.3 and clause 3.2.6 of the annex refer to independent reviews and monitoring. We suggest the annex clarify that internal employees not in the line of authority can be considered independent reviewers, as opposed to third-party reviewers.

Incident handling and business continuity

The annex requires entities to log all incoming and outgoing traffic, but the volume of such logs can be substantial, especially without a specified retention period. Organizations should use their risk management processes to determine which logs are relevant for effectively detecting and responding to attacks. Logging everything listed in this section can be costly and inefficient, as not all logs are useful for attack detection and response (e.g., logs for

[9] See Center for Internet Security, *Cloud Security and the Shared Responsibility Model with CIS*, available at https://learn.cisecurity.org/l/799323/2020-07-21/28q2r/799323/36462/CIS_Hardened_Images_Shared_Responsibility_White_Paper_2020.pdf.

privileged access to low-risk systems in highly controlled environments). The necessity of maintaining, documenting, and reviewing logs should depend on the nature of the service and its risk profile.

Additionally, relevant entities such as cloud service providers often have limited visibility into all inbound and outbound network traffic and may not be best placed to maintain comprehensive logs.[10] We propose either removing letters (a) and (b) of clause 3.2.3 or clarifying that logs should include the information 'where appropriate, considering the nature of the network, information systems and services.'

Clause 3(2)(5) requires relevant entities to maintain and back up logs for a predefined period, store them at a central location, and protect them from unauthorised access or changes. Storing logs at a central location, however, is counterproductive as it introduces a security risk. The phrase 'at a central location' should be removed.

The annex merges physical security events with digital application and cloud events for event management and problem detection. Few entities can manage both types of events concurrently. We recommend allowing the separation of physical security events from IT events to improve clarity and effectiveness.

Finally, whilst reviewing aggregate data on incidents regularly is important for tracking trends and potential recurring issues, a quarterly review as set out in clause 3.4.2(b) is not suitable for all incident types. Instead, we propose reviewing incidents on a 'regular basis,' allowing relevant entities to conduct their reviews in a targeted and flexible manner.

Backup management

The annex should clarify that backup management obligations apply only to the relevant entity's own data. Customers hosting data on the relevant entity's infrastructure are responsible for their own backup solutions. Additionally, due to the high volumes of data hosted by some relevant entities, offline backups may be impractical. Therefore, flexibility to host backups online is essential.

Supply chain security

The annex requires entities to include specific provisions and requirements in their contracts with suppliers and service providers. These clauses may pressure smaller providers to negotiate terms with more powerful parties, potentially forcing them to accept clauses they may struggle to support, resulting in significant challenges if they cannot fulfil these obligations.

[10] Customers usually set their own access controls and permissions under the 'shared responsibility model.' See 'Aligning requirements to a shared responsibility model' section above. In this model, cloud providers focus on the security of and access to hardware, software, networking and facilities running cloud services.

Moreover, the annex mandates that contracts include provisions for the right to audit or receive audit reports. Many companies already undergo rigorous certification processes to ensure service security. Existing certifications, such as the forthcoming European cybersecurity certification scheme for cloud services (EUCS) or international standards like ISO 27001, should be deemed sufficient to meet NIS2's objectives.

Focus on critical providers

Whilst relevant entities should identify and manage risks within their supply chain, these obligations should be proportionate to the risks posed by the direct supplier or service provider to the relevant entity's service delivery.

We recommend revising the annex's section 5 to focus on the relevant entity's critical direct suppliers or service providers. A relevant entity may use different direct suppliers or service providers for various purposes and with differing levels of importance. It is not appropriate, proportionate or operationally feasible for a relevant entity to impose all obligations on direct suppliers or service providers whose goods or services are not essential to the relevant entity's ultimate service delivery.

Furthermore, there is no objective standard for measuring the 'overall quality' of ICT products and services (clause 5.1.2(c)), as appropriateness varies by service and component criticality. These nuances cannot be effectively captured within a single supply chain policy.

Unintended consequences for open source

Whilst supply chain security requirements are vital for ensuring the overall security of services under NIS2, the current draft risks unintended consequences for OSS, potentially hindering its use in the EU.

OSS security benefits from collaborative innovation involving numerous contributors. These projects and contributors should not be considered 'suppliers' or 'service providers' under the implementing act. Requiring relevant entities to contract with OSS projects or contributors would undermine the open participation model of these communities.

Unlike proprietary software, where entities depend on a supplier, OSS provides the code and rights needed for entities to ensure compliance with NIS2 requirements. Given this conceptual difference, we suggest that the implementing act align with other cybersecurity regulations (notably the CRA) to exclude OSS from the scope of supply chain requirements.

Coordinated security risk assessments of critical supply chains

DIGITALEUROPE suggests adding the phrase 'in accordance with national law' at the end of clause 5.1.3. There is limited information about the

coordinated security risk assessments of critical supply chains under Art. 22(1) NIS2, and their outcomes are presently unpredictable.[11]

IT security, networks and asset management

Requiring cryptography for all information held by relevant entities is overly burdensome and unnecessary for adequate protection. A risk-based approach, considering the information's impact on network and system security, is more appropriate.

Letter (e) of clause 11.2.2 requires relevant entities to maintain a register of access rights. A single comprehensive register is impractical and too resource intensive. Instead, entities should have appropriate policies and processes to approve and review access rights, regardless of where they are stored.

We suggest replacing 'state-of-the-art,' when it comes to authentication methods at clause 11.6.3, with 'appropriate' to ensure more clarity and consistency with the rest of the draft act.

Clause 12.1.2 requires entities to classify all information and assets based on confidentiality, integrity, authenticity and availability to indicate protection needs. Whilst most criteria are established practices, the term 'authenticity' is unhelpful in this context and should be removed.

Incident reporting

Significant incidents

The proposed criteria defining 'significance' are excessively broad and would lead to overreporting, diverting resources from addressing real threats and major incidents for both relevant entities and CSIRTs.

To avoid this, an incident should be considered significant only if two or more criteria are met, specifically focusing on whether the incident impacts the relevant entity's ability to deliver critical services to its direct customers, affecting their business-critical functions. Additionally, a fault or responsibility condition should be introduced to ensure reporting obligations only cover actions or inactions of the relevant entities.

The broad definition of 'incident' and low reporting thresholds, combined with an all-hazards approach per Art. 21(2) NIS2, would result in an excessive number of reportable incidents. This approach does not differentiate between causes, focusing only on technical failures. For instance, the unavailability of a

[11] We stress that these assessments should align with national, EU and international legal principles, such as equal treatment/non-discrimination, free movement of goods and services, proportionality and legal certainty as enshrined in the Treaty on the Functioning of the EU (TFEU), the European Convention on Human Rights (ECHR) and the General Agreement on Tariffs and Trade (GATT).

‘managed service’ due to staff shortages should not be reportable. Therefore, raising the thresholds is essential.

Additionally, prescriptive incident reporting thresholds do not align with a proportionality approach, as relevant entities vary in size, technology and business models. This can prevent accurate measurement of expected metrics and cause overreporting, leading to ‘reporting fatigue.’

Considerations for the proposed thresholds are provided below to illustrate these points.

Financial loss

The thresholds in the draft implementing act’s Art. 3(1)(a) include an actual or possible financial loss for the relevant entity. Financial loss is a metric that often fails to indicate the incident’s impact on customers or services, and can be difficult to calculate accurately.

Estimating financial loss immediately after an incident may delay assessing its significance. Therefore, financial loss should be considered a lower priority criterion in the early stages of incident response.

Additionally, the proposed thresholds can be very low for large companies and do not equate to ‘severe financial loss’ (Art. 23(3)(a) NIS2), especially when including administrative, staff and external counsel costs. The phrase ‘capable of’ is ambiguous and should be replaced with ‘is likely to.’

Incident response teams cannot completely rule out the possibility of financial loss within the first 24 hours, leading to unnecessary notifications. It is more practical to calculate financial loss with guidance from Recital 34 of the draft implementing act as part of the final report.

We recommend focusing only on the percentage of the entity’s annual turnover and the actual impact, excluding potential financial loss, to reduce ambiguity. It should be specified that the elements considered for calculating financial loss in Recital 34 are limited to costs directly resulting from the specific incident, as opposed to general cybersecurity costs.

Considerable reputational damage

The proposed parameters for determining considerable reputational damage in Art. 3(2) are too vague. For instance, they refer to potential capability of causing damage, which may not materialise. There is no clear specification of how many customer complaints constitute ‘considerable reputational damage.’ Instead, the threshold should be defined as ‘reported by a material number of customers,’ with a clear definition of materiality.

A similar approach is needed for ‘material impact on business.’ The term ‘reported in the media’ should also protect against reports generated by competitors, malicious actors, or those with inaccurate or misleading details.

Companies may have limited ways to monitor media coverage, especially if reports are local or national. There is no historical evidence that media coverage of well-managed security incidents leads to significant harm. In fact, proper handling of an incident can enhance an entity's reputation.

The criterion is further ambiguous due to the lack of a common standard for defining the credibility of media sources, including blogs and social media. Linking media coverage to a known incident or similar predefined threshold would be more appropriate. This criterion disproportionately impacts entities frequently in the media, as they would be penalised for reporting incidents simply mentioned in the press, even if these incidents do not meet the threshold of a 'significant' incident.

If a meaningful and measurable definition of 'considerable reputational damage' cannot be established, we suggest deleting this criterion.

Exfiltration of trade secrets

This criterion addresses incidents that have caused or could cause the exfiltration of trade secrets. However, it's unclear what scenarios this is meant to cover, as the exfiltration of trade secrets might not impact a relevant entity's service delivery.

For example, if an employee steals intellectual property and shares it with a competitor, it may not affect the services provided by the entity. This criterion conflicts with the NIS2 threshold. Without clearer guidelines and a risk-based link to actual impact, this criterion will likely cause confusion and unnecessary burden for relevant entities.

Additionally, the phrase 'is capable of' should be removed, as the potential for exfiltration might be unknown pending investigation, making this metric unworkable without objective evidence.

Damage to a natural person's health or death of a natural person

These criteria should be removed, as it is impossible for a relevant entity to have knowledge of such events. Relevant entities typically lack visibility, control or knowledge of how their customers use and configure their services due to contractual arrangements and the nature of service utilisation.

Malicious access to network and information systems

Unauthorised access alone does not necessarily impact the relevant entity's services. This criterion implies that any unauthorised access, even if no sensitive information or operational functions were affected, would automatically be considered a reportable significant incident.

This contradicts the NIS2 threshold, which focuses on the results and impact of incidents rather than their causes. Such a criterion would lead to excessive

reporting of incidents that have no impact or reasonable expectation of impact on service provision.

Additionally, the term ‘suspicious malicious activity’ could refer to unusual login patterns, attempts to access restricted areas or known malware signatures. Practical guidelines for identifying and assessing these activities, along with clear result and impact criteria, are essential for effective incident reporting and legal compliance.

Affected users

The parameters for determining incident significance by calculating the number of affected users in Arts 3(4)(a)–(b) are challenging to implement.

Due to the nature of certain services, it is not always feasible to assess the exact number of impacted users. For example, cloud services often have a distributed and scalable architecture, where users access the service remotely. In such models, the service provider may not have a direct relationship with all end-users or visibility into the exact number of users accessing the service at any given time.

Cloud services designed for high availability and accessibility to many users make it difficult to track and count the exact number of individuals affected by a security incident. This also complicates tracking users’ locations, making estimates of the number and location of ‘users in the Union’ highly speculative. For example, a cloud-based email or collaboration service with millions of users may not have a precise count of affected users during a security breach.

Instead of monitoring individual users, error rates could be tracked and thresholds set at API endpoints. Relevant entities should report incidents based on available information, such as the number of direct customers impacted and the volume of complaints received.

Neither NIS2 nor the draft implementing act defines ‘user’ or ‘cloud computing service user,’ making it difficult to assess whether the customer SLA is not met for five percent of a cloud provider’s end-users or enterprise customers, as per Arts 7(b)–(c).[12]

The thresholds of one per cent or five per cent of service users should consider the incident type. For small services, this could mean only a few customers are affected, with minimal societal impact. Depending on the service type and criticality, such as availability, it would be more effective to focus on impactful incidents, like an outage affecting 100,000 people.

Differentiation in criteria based on service parts and incident types (availability vs. integrity) would enhance reporting effectiveness. Additionally, the five per cent threshold should distinguish between business-to-business (B2B) and

[12] We note that Recital 9 of the draft implementing act defines ‘users’ only for the technical and methodological requirements in the annex.

business-to-consumer (B2C) services. In B2B, user numbers are more restricted compared to B2C, making the five per cent threshold more achievable, which should not automatically trigger a notification obligation.

Distinguishing network and service criticality

A distinction should be made between critical and less critical networks within a company when it comes to the Art. 3(1)(f) criterion that 'a successful, suspectedly malicious and unauthorised access to network and information systems occurred.'

Critical networks, such as financial systems and customer databases, handle sensitive data and operations, and their compromise can lead to severe consequences. In contrast, less critical networks, like general office networks, pose a lower risk if breached. This distinction allows for tailored response measures and better resource allocation.

Similarly, reporting significant incidents should be reserved for services that are critical offerings of the relevant entity, not peripheral or minor services. The proposed drafting does not distinguish between the materiality of a given service to customers, meaning most incidents affecting any service will meet the proposed criteria.

Recurring incidents

Recurring incidents meeting the criteria of Art. 4 should not be classified as significant unless they also meet one or more criteria under Art. 3.

Only recurring incidents that significantly impact customers or relevant services should be captured. For example, confirmed incidents affecting over five per cent of customers with a contract with the relevant entity and occurring for at least 10 consecutive minutes, four times within a six-month period, should be considered.

Provisions of Art. 4 should exclude situations where multiple, unsuccessful attempts recur but do not result in an impactful intrusion. Organisations may need significant investigative time, e.g. several days or weeks, to determine the root cause of incidents. Requiring this for all minor, insignificant incidents would divert resources from responding to high-impact events. The focus on root cause is inconsistent with the NIS2 threshold, which emphasises the results and impact of incidents, not their causes.

Without these clarifications, the criteria for considering the significance of recurring incidents could be too low, leading to overreporting and unnecessary burdens.

Significant incidents with regards to specified relevant entities

SLAs for service availability

The draft implementing act's Arts 5–14 include prescriptive timelines around availability and SLA incidents. However, SLAs are negotiated between private commercial parties and can vary widely over time and based on market dynamics and bargaining power, making them unsuitable as a regulatory reporting threshold.

Using SLAs as criteria would require companies to review numerous contracts to determine if SLAs have been breached, diverting limited incident response resources. Moreover, SLAs often relate to customer convenience rather than security or resilience, making them irrelevant for determining significant incidents.

The length of a service outage does not necessarily indicate the significance of an incident. Instead, the focus should be on the impact, such as the number of direct customers affected. The draft's proposed 10-minute threshold for complete unavailability is very short, especially compared to the NIS implementing act's threshold (5,000,000 user-hours). This is inconsistent with NIS2, which considers an incident significant if it causes or is likely to cause 'severe' operational disruption.

Additionally, the geographical scope of the services is unclear. For example, do the criteria apply to incidents in the US affecting EU customers or incidents in Europe not affecting EU customers? The unavailability of the service could be limited to a single customer or location. The scope of services can significantly impact the interpretation and necessary actions. Depending on whether the unavailability is global, limited to Europe or only affects certain European customers, the implications differ.

The scope should be limited to services hosted within the EU, where a certain number or percentage of direct EU customers are affected, rather than using a time threshold. Planned and appropriately communicated maintenance and outages should not be classified as incidents.

Key services

The draft implementing act's Arts 5–14 apply when any service experiences an incident, regardless of its criticality. The duration of a service outage does not necessarily reflect the importance of the service or its availability during critical working hours or 24/7. Some services have very few customers, whilst others are critical to almost all customers and other services.

Significant incidents should be reserved for the relevant entity's critical services, not peripheral or minor ones. High availability requirements should be defined for critical service functions or their parts. Not all services require semi-permanent availability, and some downtime for technical support requests may have little consequence for cybersecurity, which the draft implementing act does not reflect.

For example, Art. 13, which applies to social networking service platforms, sets a broad threshold for reporting based on service unavailability. It requires reporting if the platform or 'part of its functionality' is completely unavailable for more than five per cent of users in the Union or more than one million users, whichever is smaller. Social networking platforms have numerous features of varying importance. The draft does not define 'part of its functionality,' making it unclear if a notification is required for the unavailability of a minor feature whilst the platform remains otherwise functional. To avoid confusion and minimize overreporting, these peripheral or minor incidents should be explicitly excluded in the final implementing act.

Suspected malicious action

The current wording mandates entities to report incidents resulting from 'suspected malicious action.' Until an investigation is complete, entities will not have enough information to determine whether an incident was malicious. This requirement will lead to substantial and inappropriate overreporting. Only confirmed malicious actions should be in scope.

The draft also eliminates numerical thresholds for reporting data from 'suspectedly malicious actions,' creating an undue burden on service providers even if a single user is impacted. We suggest establishing appropriate thresholds, such as 100,000 impacted users or direct customers. This aligns with the NIS2 threshold, which focuses on the results and impacts of incidents rather than their causes.

For example, social networking service platforms and their users are frequently targeted by bad actors. A low threshold for reporting would cover even minor instances of malicious activity, such as user account compromises due to weak passwords or users inadvertently granting access to their information. These incidents are not reflective of weaknesses in the platform's cybersecurity posture and can often be easily rectified, e.g. blocking the account and setting a new password. As currently drafted, the low threshold for determining significance will result in an unmanageable volume of notifications.

Data compromise

The criteria in Arts 6(c), 7(d), 8(d), 10(d), 11(c), 12(c) and 13(c) lack a risk-based threshold. They suggest that any compromise of data integrity, confidentiality or processing due to suspected malicious action requires reporting, regardless of impact. This contradicts the NIS2 threshold and would burden companies with overreporting insignificant incidents, without improving the security and resilience of services in the EU.

Impacted services

Whilst Recital 9 defines 'user' as 'all legal and natural persons who have access to the entity's network and information systems,' it is unclear if 'users' in Art.

10(b) refers to customers, individual machines or facilities. This ambiguity complicates compliance, as service providers may struggle to determine whom to notify during an incident, potentially leading to over- or under-communication.

Arts 9(c) and 10(c) of the draft implementing act add further ambiguity by stating that the availability of the content delivery network and managed service is 'impacted' by the incident, without defining or quantifying this impact. This could result in service providers reporting all incidents, regardless of severity. We suggest deleting both paragraphs to avoid unnecessary reporting.

Art. 7(a) sets a threshold for the significance of cloud service unavailability at more than 10 minutes, with similar criteria in Arts 5(a), 6(a), 8(a), 10(a) and 14(a). The draft does not consider that many services may be unavailable for reasons unrelated to cybersecurity, such as maintenance or upgrades. This could lead to overreporting and an excessive number of notifications. Extending the timelines would be helpful. This requirement is particularly challenging for smaller companies that cannot ensure 24/7 staff availability. A more practical approach would reference SLAs, making incidents significant only if they breach these commitments, aligning more closely with service providers' contractual expectations and capacities.

The term 'completely unavailable' also causes ambiguity. For instance, if an internet connection to a cloud service is lost, it is 'completely unavailable' to the end-user, whilst locally, the system functions well. It should be clarified that complete unavailability refers to the whole system and not just user access.

Although regulatory guidance on significant incidents is appreciated, the implementing act may require entities to monitor issues that are not always trackable or relevant. For example, Art. 10(a) would require notification of any downtime over 10 minutes for managed services, but not all managed services need such availability tracking. Clarification that entities are not required to monitor availability for services where it is not currently tracked would make the thresholds more flexible and practical.

Potential incidents

Recital 10 refers to 'potential incidents,' even though this term is not found in NIS2. For this reason, the part of Recital 10 that refers to potential incidents should be deleted.

Relationship between reporting and registration

The draft implementation act lacks specific elements regarding registration as per Art. 27 NIS2. This absence may lead to uneven implementation by Member States, and to uncertainty about which entities fall under its scope, potentially resulting in an incomplete overview of active incidents at ENISA.

Additionally, the draft does not clarify the relationship between registration and reporting. It is unclear whether incident reporting requires prior registration of the affected entity, or if a company ID is needed for incident reporting. Some Member States have even proposed a company account to define roles and impose procedural restrictions on incident reporting.

An EU-wide online portal with a standardised template for registration and incident reporting would be beneficial for all companies active across the EU.

Incident reporting timeframe for 'early warning'

Art. 23(4)(a) NIS2 mandates that an entity must submit an 'early warning' within 24 hours of 'becoming aware of the significant incident,' but does not define what 'becoming aware' means.

It is important to recognise that after detecting an incident, a service provider undergoes an 'investigation phase' to confirm its validity. Only then can the incident be analysed further to determine if it meets the 'significant incident' criteria, triggering the reporting process. Additionally, some threshold criteria in the draft implementing act, such as the percentage of users affected, customer SLA violations, and the incident's root cause, may not be immediately clear in the hours or days following the incident.

We suggest clarifying that the 24-hour clock for determining when an entity became 'aware' of an incident should start when the entity knows with a 'reasonable degree of certainty' that one of the defined thresholds for a 'significant incident' has been met. Adding a dedicated Recital to clarify this aspect would be beneficial. This could use wording from the European Data Protection Board (EDPB) guidance on personal data breach notifications to define what it means for the controller to become 'aware.'[13]

Reporting should only occur when there is sufficient evidence to indicate that a significant incident has taken place. Reporting on a speculative level is neither operationally feasible for entities nor desirable for customers or CSIRTs.

Implementation timeline

The implementing act will apply as of 18 October 2024, coinciding with the deadline for NIS2 enactment into national laws across the EU. This is an unrealistically short timeframe for demonstrating compliance, as it allows only a few months from its adoption and publication. In contrast, there were approximately 22 months between the publication of NIS2 in the Official Journal of the European Union (OJEU) on 27 December 2022 and the deadline for Member States to adopt necessary measures by 17 October 2024.

Considering the Commission has not yet published implementing acts related to NIS2, it is unreasonable to require immediate compliance without any

[13] Guidelines 9/2022.

transition period. The Belgian transposition law acknowledges this by introducing a gradual build-up of compliance measures to be completed by 18 April 2027.[14]

We propose developing a documented system security plan, drafted by relevant entities, to meet the requirements of the implementing act. This plan would include action plans and milestones for future compliance.

Additionally, we call for a one-year grace period, allowing relevant entities time to fully understand the requirements, develop and test implementation strategies, and ensure compliance without the immediate risk of penalties. This approach would lead to more effective and sustainable cybersecurity practices. A grace period would also give authorities the necessary time to prepare for oversight responsibilities and acquire the required resources, tools and mechanisms.

FOR MORE INFORMATION, PLEASE CONTACT:

- Rita Jonusaite
  Senior Policy Manager for Cybersecurity & Cloud
  rita.jonusaite@digitaleurope.org / +32 499 70 86 25
- Sid Hollman
  Policy Officer for Cybersecurity & Digital Infrastructure
  sid.hollman@digitaleurope.org / +32 491 37 28 73
- Milda Basiulyte
  Senior Director for Cyber, Infrastructure & Competitiveness
  milda.basiulyte@digitaleurope.org / +32 493 89 20 59
- Alberto Di Felice
  Policy and Legal Counsel
  alberto.difelice@digitaleurope.org / +32 471 99 34 25

[14] https://ccb.belgium.be/en/nis2.

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 110 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.