Ref. Ares(2024)4640447 - 27/06/2024

EUROPEAN
COMMISSION

Brussels, XXX
[…](2024) XXX draft

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)[1], and in particular Articles 21(5), first subparagraph and 23(11), second subparagraph thereof, Whereas:

(1) With regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers as covered by Article 3 of Directive (EU) 2022/2555 (the relevant entities), this Regulation aims to lay down the technical and the methodological requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 and to further specify the cases in which an incident should be considered to be significant as referred to in Article 23(3) of Directive (EU) 2022/2555.

(2) Taking account of the cross-border nature of their activities and in order to ensure a coherent framework for trust service providers, this Regulation should, with respect to trust service providers, further specify the cases in which an incident shall be considered to be significant, in addition to laying down the technical and the methodological requirements of the cybersecurity risk-management measures.

(3) Following Article 21(5), third subparagraph of Directive (EU) 2022/2555, the technical and methodological requirements of the cybersecurity risk-management measures set out in the Annex to this Regulation are based on European and international standards and technical specifications relevant to the security of network and information systems.

(4) As regards the application of the technical and the methodological requirements of cybersecurity risk-management measures set out in the Annex to this Regulation, in line with the principle of proportionality, due account should be taken of the divergent risk exposure of relevant entities, such as the criticality of the relevant entity, the risks to which it is exposed, the relevant entity's size and structure as well as the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

(5) In line with the principle of proportionality, where relevant entities cannot implement the technical and the methodological requirements of the cybersecurity riskmanagement

[1] OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

measures due to their size, those entities should be able to take other compensating measures that are suitable to achieve the purpose of those requirements. For example, micro-sized entities might find it difficult to segregate conflicting duties and conflicting areas of responsibility. Such entities should be able to consider compensating measures such as targeted oversight by the entity's management or increased monitoring and logging.

(6) Competent authorities can decide to provide guidance to support relevant entities in the identification, analysis, and assessment of risks for the purpose of implementing the technical and the methodological requirements concerning the establishment and maintenance of an appropriate risk management framework. Such guidance can include, in particular, national and sectoral risk assessments as well as risk assessments specific for a certain type of entity. Moreover, competent authorities can support entities in identifying and implementing appropriate solutions to treat risks identified in such risk assessments. Such guidance should be without prejudice to the relevant entities' obligation to identify and document the risks posed to the security of network and information systems, and to the relevant entities' ability to implement the technical and the methodological requirements of the cybersecurity risk management measures set out in the Annex to this Regulation according to their needs and resources.

Commented [A1]: [General Comment]
Recital should put stringent obligations for national authorities to provide guidance to support relevant entities. This guidance should be provided by ENISA, in collaboration with national authorities.

(7) Network security measures in relation to: (i) the transition towards latest generation network layer communication protocols, (ii) the deployment of internationally agreed and interoperable modern e-mail communications standards, and (iii) the application of best practices for Internet routing security and routing hygiene entail specific challenges regarding the identification of best available standards and deployment techniques. To achieve as soon as possible a high common level of cybersecurity across networks, the Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA) and in collaboration with competent authorities, industry – including telecommunication industry – and other stakeholders, should support the development of a multistakeholder forum tasked to identify these best available standards and deployment techniques. Such multi-stakeholder guidance should be without prejudice to the relevant entities' ability to implement the technical and the methodological requirements of the cybersecurity risk management measures set out in the Annex to this Regulation.

(8) Pursuant to Article 21(2), point (a), of Directive (EU) 2022/2555, essential and important entities should have policies on information system security. For that purpose, the relevant entities should establish a policy on the security of network and information systems as well as topic-specific policies, such as policies on access control. All policies and topic-specific policies should be approved by an appropriate level of management of the relevant entities ~~The policy on the security of network and information systems should be the highest level document setting out the relevant entities' overall approach to their security of network and information systems and should be approved by the management bodies of the relevant entities. The topic-specific policies should be approved by an appropriate level of management.~~ The policy should lay down indicators and measures to monitor its implementation and the current status of relevant entities' level of network and information security, in particular to facilitate the oversight of the implementation of the cybersecurity risk-management measures through the management bodies.

Commented [A2]: [Suggestion to modify text]
It is important to state that the entity must have policies in place and that they need to be approved by the appropriate level of management but dictating specific governance models for such a wide variety of entities is not appropriate.

(9) For the purposes of the technical and the methodological requirements laid down in the Annex to this Regulation, the term 'user' should encompass all legal and natural persons which have access to the entity's network and information systems.

(10) To detect anomalous behaviour and ~~potential~~ incidents, the relevant entities should monitor their network and information systems ~~and should take actions to evaluate potential~~

Commented [A3]: [Suggestion to modify text]
Further clarification is needed on what does constitute a "potential" incident or otherwise it should be fully removed.

~~incidents~~. Those measures should be capable of allowing the detection of network-based attacks based on anomalous ingress or egress traffic patterns and distributed denial of service attacks in a timely manner.

(11) When the relevant entities conduct a business impact analysis, they are encouraged to carry out a comprehensive analysis establishing, as appropriate, maximum tolerable downtime, recovery time objectives, recovery point objectives and service delivery objectives.

(12) In order to mitigate risks stemming from a relevant entity's supply chain and its relationship with its suppliers the relevant entities should establish a supply chain security policy which governs their relations with their direct suppliers and service providers. These entities should specify in the contracts with their direct suppliers or service providers adequate security clauses, for example by requiring, where appropriate, cybersecurity risk-management measures according to Article 21(2) of Directive (EU) 2022/2555 or other similar legal requirements.

(13) The relevant entities should regularly carry out security tests based on a dedicated policy and procedures to verify whether the cybersecurity risk-management measures are implemented and function properly. Security tests may be performed on specific network and information systems or on the relevant entity as a whole and may include automated or manual tests, penetration tests, vulnerability scanning, static and dynamic application security tests, configuration tests or security audits. The relevant entities may conduct security tests on their network and information systems at set-up, after infrastructure or application upgrades or modifications that they deem significant, or after maintenance. The findings of the security tests should inform the relevant entities' policies and procedures the assessment of the effectiveness of their security measures, as well as independent reviews of their network and information security policies.

(14) In order to avoid significant disruption and harm caused by the exploitation of unpatched vulnerabilities in network and information systems, the relevant entities should set out and apply appropriate security patch management procedures which are aligned with the relevant entities' change management procedures. Relevant entities should take measures proportionate to their resources to ensure that security patches do not introduce additional vulnerabilities or instabilities. In case of planned inaccessibility to the service caused by the application of security patches, the relevant entities are encouraged to duly inform customers in advance.

(15) The relevant entities should manage the risks stemming from the acquisition of ICT products or ICT services from suppliers or service providers and should obtain assurance that the ICT products or ICT services achieve certain cybersecurity protection levels, for example by European cybersecurity certificates and EU statements of conformity for ICT products or ICT services issued under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council[2]. Where the relevant entities set out security requirements to apply to the ICT products to be acquired, they should take into account the cybersecurity essential requirements set out in the [Cyber Resilience Act].

(16) In order to protect against cyber threats and support the prevention and containment of data breaches, the relevant entities should implement network security solutions. Typical

[2] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

solutions for network security include the use of firewalls to protect the relevant entities' internal networks, the limitation of connections and access to services where it is absolutely needed, or the use of virtual private networks for remote access and allowing connections of service providers only after an authorisation request and for a set time period such as the duration of a maintenance operation.

(17) In order to protect the networks of the relevant entities and their information systems against malicious and unauthorised software, those entities should use malware detection and repair software. Where the relevant entities, based on the risk assessment, consider that the use of malware detection and repair software is not adequate or where the malware detection and repair software is not available at all times, those entities should consider additional measures and controls that prevent or detect the use of unauthorised software, and the use of known or suspected malicious websites. The relevant entities should also consider implementing measures to minimize the attack surface, reduce vulnerabilities that can be exploited by malware, control the execution of applications on user workstations or user end devices, and employ email and web application filters to reduce exposure to malicious content.

(18) Pursuant to Article 21(2), point (g), of Directive (EU) 2022/2555, Member States are to ensure that essential and important entities apply basic cyber hygiene practices and cybersecurity training. Cyber hygiene practices are a part of different technical and methodological requirements of the cybersecurity risk management measures set out in the Annex to this Regulation. With regard to basic cyber hygiene practices, the relevant entities should consider practices such as clear desk and screen policy, use of passwords and other authentication means, safe email use and web browsing, protection from phishing and social engineering, secure teleworking practices.

(19) In order to prevent unauthorised access to the relevant entities' information and assets, the relevant entities should establish and implement a topic-specific policy addressing access by network and information system processes such as one network and information system connecting to another.

(20) In order to avoid that employees can misuse, for instance, access rights within the relevant entity to harm and cause damage, relevant entities should consider adequate employee security management measures and raise awareness among personnel about such risks

(21) Multi-factor authentication can enhance the entities' cybersecurity and should be considered by the entities in particular when users access network and information systems from remote locations, or when they access sensitive information or privileged accounts and system administration accounts. Multi-factor authentication can be combined with other techniques to require additional factors under specific circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device or at an unusual time.

(22) The relevant entities should manage and protect the assets which are of value to them through a sound asset management which should also serve as the basis for the risk analysis and business continuity management. The relevant entities should manage both tangible and intangible assets and should create an asset inventory, associate the assets with a defined classification level, handle and track the assets and take steps to protect the assets throughout their lifecycle.

(23) Asset handling should involve classifying assets by their type, sensitivity, risk level, and security requirements and applying appropriate measures and controls to ensure their

Commented [A4]: [General Comment]
Recital (16) of the preamble refers to the importance of protecting against "data breaches" but in items (16) through (18) the focus is on network security as a means to protect against data breaches rather than recommending the use of techniques to secure the data itself.

availability, integrity and confidentiality. By classifying assets by risk level, the relevant entities should be able to apply appropriate security measures and controls to protect assets such as encryption, access control including perimeter and physical access control, auditing, backups, logging and monitoring, retention and disposal. When conducting a business impact analysis, the relevant entities may determine the classification level based on the consequences of disruption of assets for the entities. All employees of the entities handling assets should be familiar with the asset handling policies and instructions.

(24) As remote working has become increasingly widespread in recent years, it becomes vital for entities to define rules for personnel on how to handle entities' assets all along their employment and all along the assets' life cycles.

(25) The granularity of the asset inventory should be appropriate for the needs of the relevant entities. A comprehensive asset inventory should include, for each asset, at least a unique identifier, the owner of the asset, a description of the asset, the location of the asset, the type of asset, the type and classification of information processed in the asset, the date of last update or patch of the asset, the classification of the asset under the risk assessment, and the end of life of the asset. When identifying the owner of an asset, the relevant entities should also identify the person responsible for protecting said asset. Types of assets can be software, hardware, services, facilities, heating, ventilation and air conditioning systems, patents, copyrights, or physical records.

(26) The allocation and organisation of cybersecurity roles, responsibilities and authorities should establish a consistent structure for the governance and implementation of cybersecurity within the relevant entities, and should ensure effective communication in case of incidents. When defining and assigning responsibilities for certain roles, the relevant entities should consider roles such as chief information security officer, information security officer, incident handling officer, auditor, or comparable equivalents.

(27) In accordance with Article 21(2) of Directive (EU) 2022/2555, the cybersecurity riskmanagement measures are to be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage to, and interference with, an essential or important entity's information and information processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. The technical and the methodological requirements of the cybersecurity riskmanagement measures should therefore also address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena. Further examples of physical and environmental threats can include earthquakes, explosions, sabotage, insider threat, civil unrest, toxic waste, and environmental emissions. Prevention of loss, damage or compromise of network and information systems or interruption to their operations due to the failure and disruption of supporting utilities should contribute to the goal of business continuity in the relevant entities. Moreover, protection against physical and environmental threats should contribute to security in network and information systems maintenance in the relevant

entities.

(28) When relevant entities design and implement protection measures against physical and environmental threats and determine minimum and maximum control thresholds for physical and environmental threats and monitor environmental parameters, they should consider in particular the establishment of a separate fire compartment for the data centre, the use of fire-

resistant materials, sensors for monitoring temperature and humidity, the connection of the building to a fire alarm system with an automated notification to the local fire department, and early fire detection and extinguishing systems. The relevant entities should also carry out regular fire drills and fire inspections. Furthermore, to ensure power supply, the relevant entities should consider overvoltage protection and corresponding emergency power supply, in accordance with relevant standards.

(29) This Regulation is to further specify the cases in which an incident should be considered to be significant for the purpose of Article 23(3) of Directive (EU) 2022/2555. The criteria should be such that relevant entities are able to assess whether an incident is significant, in order to notify the incident in accordance with Directive (EU) 2022/2555. Horizontal as well as relevant entity-type specific cases in which an incident should be considered to be significant should be set out.

(30) With a view to establishing whether an incident is significant, where relevant, relevant entities should count the number of users impacted by the incident. Where a relevant entity is unable to calculate the number of impacted users, the relevant entity's estimate of the possible maximum number of affected users should be considered for the purpose of calculating the total number of users affected by the incident.

Commented [A5]: [General Comment]
Explained for Article 3(4a&b).

(31) Maintenance operations resulting in the limited availability or unavailability of the services should not be considered as significant incidents if the limited availability or unavailability of the service occurs according to a planned maintenance operation.

(32) The duration of an incident should be measured from the disruption of the proper provision of the service in terms of availability, authenticity, integrity or confidentiality until the time of recovery. Where a relevant entity is unable to determine the moment when the disruption began, the duration of the incident should be measured from the moment the incident was detected, or from the moment when the incident was recorded in network or system logs or other data sources, whichever is earlier.

(33) Complete unavailability of a service should be measured from the moment the service is fully unavailable to users, to the moment when regular activities or operations have been restored to the level of service that was provided prior to the incident. Where a relevant entity is unable to determine when the complete unavailability of a service began, the unavailability should be measured from the moment it was detected by that entity.

(34) For the purpose of determining the financial losses resulting from an incident, relevant entities should take into account all the financial losses which they have incurred as a result of the incident, such as costs for replacement or relocation of software, hardware or infrastructure, staff costs, including costs associated with replacement or relocation of staff, recruitment of extra staff, remuneration of overtime and recovery of lost or impaired skills, fees due to non-compliance with contractual obligations, costs for redress and compensation to customers, losses due to forgone revenues, costs associated with internal and external communication, advisory costs, including costs associated with legal counselling, forensic services and remediation services, and ransoms paid. The relevant entities should calculate the amounts of financial losses based on available data and, where the actual amounts of financial losses cannot be determined, the entities should estimate those amounts.

(35) A large delay in response time should be considered to occur when a service provided by a relevant entity is considerably slower than average response time. Where possible, objective criteria based on the average response times of services provided by the relevant entities should be used to assess delay.

(36) For the purposes of this Regulation, a network and information system should be considered compromised when the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, the system is compromised.

(37) The Commission has exchanged advice and cooperated with the Cooperation Group and ENISA on the draft implementing act, in accordance with Articles 21(5) and 23(11) of Directive (EU) 2022/2555.

(38) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 (EC) of the European Parliament and of the Council[3], and delivered its opinion on [date of the opinion].

(39) This Regulation should apply from [18 October 2024].

(40) The measures provided for in this Regulation are in accordance with the opinion of the committee established in accordance with Article 39 of Directive (EU) 2022/2555,

HAS ADOPTED THIS REGULATION:

Commented [A6]: [General Comment]
While we welcome the opportunity to require a more holistic approach to data security by referring to the need to secure data that is "stored," "transmitted," and "processed." It is important, however, to clarify that "processed data" should include data "in use," as this is the most common state of data and it cannot be protected by traditional encryption techniques. The data security lifecycle begins from the moment a piece of data is created and that moment of creation could be the launching of a video conference, the use of an application to create a new song, the entry of a person's address into a database or the keystrokes of an author as they write their book. It is at that precise moment data security must begin because that is when data is at its most vulnerable since it must be usable by a human and, therefore, cannot be protected by traditional encryption techniques. Any NIS-2 Implementing Regulation should consider the full data security lifecycle and impose protective measures at each step of the cycle.

Incident reporting timeframe for "early warning"

Article 23 (4) a) of the NIS2 Directive provides that the entity must submit the "early warning" within 24 hours of "becoming aware of the significant incident", without a definition or clarification of what "becoming aware" means.

The current draft implementing act adds explanations on the duration of the incident from when the disruption started or was detected (though it is unclear who or which entity detected it) in Recitals 32 and 33. However, there remains a lack of clarity on how these points in time relate to "becoming aware", when the 24-hour early warning period begins, and how much time the entity has to determine if the incident should be reported.

It is important to recognize that after the incident has been detected by the service provider, there is a necessary "investigation phase" to confirm the validity of the incident. Only then can the incident be analyzed further to classify it as having fulfilled the "significant incident" criteria and trigger the reporting.

The following wording could be added in the Recitals: *After first being informed of a potential breach by an individual, a media organization, or another source, or when it has itself detected a security incident, the entity may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the entity may not be regarded as being "aware". The entity should be regarded as having become "aware" of the significant incident when that entity has a reasonable degree of certainty that a security incident has occurred and has led to a compromise of the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the cloud computing service".*

The above suggestion uses the wording from the European Data Protection Board guidance for personal data breach notification under GDPR on what it means that the controller becomes "aware". This could be leveraged to add a clarifying Recital for the purposes of this Draft Implementing Act, as the recognition of the investigation phase is crucial in efficient incident triage and reporting.

Commented [A7]: [Suggestion to insert a new Recital]

[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Article 1

Subject matter

This Regulation, with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (the relevant entities) lays down the technical and the methodological requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 and further specifies the cases in which an incident shall be considered to be significant as referred to in Article 23(3) of Directive (EU) 2022/2555.

Article 2

Technical and methodological requirements

For the relevant entities the technical and methodological requirements of cybersecurity risk management measures referred to in Article 21(2), points (a) to (j), of that Directive are set out in the Annex to this Regulation.

Article 3

Significant incidents

1. An incident shall be considered to be significant for the purposes of Article 23(3) of Directive 2022/2555 with regard to the relevant entities where one or more of the following criteria are fulfilled:

(a) the incident has caused or is ~~capable of causing~~ financial loss for the relevant entity that exceeds EUR 500 000~~100 000~~ or 5 % of the relevant entity's annual turnover, whichever is lower;

~~(b) the incident has caused or is capable of causing considerable reputational damage to the relevant entity in accordance with paragraph 2.~~

~~(c)~~(b) the incident has caused or is capable of causing the exfiltration of trade secrets as set out in Article 2(1), point (1), of Directive (EU) 2016/943 of the relevant entity;

~~(d)~~(c) the incident has caused or is ~~capable of causing~~ the death of a natural person;

~~(e)~~(d) the incident has caused or is ~~capable of causing~~ considerable damage to a natural person's health;

~~(f)~~(e) a successful, suspectedly malicious and unauthorised access to network and information systems occurred;

Commented [A8]: [Suggestion to modify text]
It is practically impossible to take a threshold of €100,000 or 5% of turnover as the extent of damage for a reporting obligation within 24 hours, and in line with Recital 34 on the determination of financial losses. Damage cannot be quantified within 24 hours. It is difficult to assess such an estimation during an incident.
Regarding the threshold value: A damage extent of €100,000 is reached very quickly especially for larger companies. Proposal should be: €500,000. This elevated value and the proportionality inherited in the 5% would account for both, larger and smaller entities. The impact is not considered further here.

In addition, 'capable of' introduces ambiguity and difficulty to determine how the loss will be assessed. It would be preferable to stick only to the percentage of the entity's annual turnover.

Commented [A9]: [Suggestion to modify text]
This is very ambiguous and should not be included as a parameter. "Reputation" may be harmed via biased media articles, or, on the contrary, an entity may retain its "reputation" even after a significant incident, due to its comms/marketing teams. This has nothing to do with cybersecurity and should not be included in EU secondary legislation.

Commented [A10]: [Suggestion to modify text]
Proposal to remove "capable of causing" as the language is too broad and has a high risk of causing over-reporting.

Additionally, it is necessary to specify that the incident causing such impact is of an IT nature.

Commented [A11]: [General Comment]
The mere information that a data/system compromise was due to malicious actions is not actionable. More important is knowing whether there is an impact on users. The possibility or confirmation of a deliberate cause should not be a condition as such but rather supplementary information included in the report. The primary conditions for reporting should be: compromised yes/no AND customers potentially impacted yes/no.

The same applies to the provisions in the Articles 7 and 8.

Additionally, this criteria should be further restricted by being conditioned to the kind of environment successful unauthorized access.

Finally, this point should be restricted to incidents of malicious cyber origin. Without this specification, the text's scope becomes too broad, particularly when considering hardware failures.

~~(g)~~(f) the incident meets the criteria set out in Article 4;

~~(h)~~(g) the incident meets one or more of the criteria set out in Articles 5 to 14.

2. For the purposes of determining the existence of a considerable reputational damage of an incident in accordance with paragraph 1, point (b) the relevant entities shall take into account whether one or more of the following criteria are met:

~~(a) the incident has been reported in the media;~~

~~(b)~~(a) the incident has resulted in formal complaints from different users or critical business relationships;

~~(c)~~(b) the entity will not be able to or is likely not to be able to meet regulatory requirements as a result of the incident;

~~(d)~~(c) the entity is likely to lose customers with a material impact on its business as a result of the incident.

3. Planned consequences of maintenance operations carried out by or on behalf of the relevant entities shall not be considered to be significant incidents.

4. When calculating the number of users impacted by an incident for the purpose of Articles 7 and 9 to 14, the relevant entities shall consider all of the following:

(a) the number of customers that have a contract with the relevant entity which grants them access to the relevant entity's network and information systems or services offered by, or accessible via, those network and information systems;

(b) the number of natural and legal persons associated with business customers that use the entities' network and information systems or services offered by, or accessible via, those network and information systems.

Article 4

Recurring incidents

~~Incidents that individually are not considered a significant incident within the meaning of Article 3, shall be considered collectively as one significant incident where they meet all of the following criteria:~~

~~(a) they have occurred at least twice within 6 months;~~

~~(b) they have the same apparent root cause.~~

Article 5

Significant incidents with regard to DNS service providers

With regard to DNS service providers, an incident shall be considered significant under Article 3 where it fulfils one or more of the following criteria:

(a) a recursive or authoritative domain name resolution service is completely unavailable for more than 10 minutes;

Commented [A12]: [Suggestion to modify text]
The reporting in media may take place at any moment since the incident took place (even after the 24hrs time-mark), so it cannot be the triggering point for reporting an incident.

Commented [A13]: [Suggestion to modify text]
This should be reworded to highlight the causality between the complaints and the incident.

Suggestion to add "formal" in order to separate customers and customer support.

Commented [A14]: [General Comment]
Any incident may cause temporary inability to meet regulatory obligations. It should perhaps contain a time-specification.

Commented [A15]: [General Comment]
It may be very difficult for the company to judge this causality.

Commented [A16]: [General Comment]
"Impact on its business" should be clarified: is the impact on the entities' business or on the customer ?

Commented [A17]: [General Comment]
The proposed parameters are too vague. There is no specification of how many customers would need to make a complaint to argue that there has been 'considerable reputational damage'. An alternative would be for the threshold to be defined as 'reported by a material number of customers', with specification of how materiality is established. A similar approach is needed for 'material impact on business', which is lacking a definition. 'Reported in the media' needs to be more specific and to protect from situations when these reports are generated intentionally by competitors or a malicious attacker. Moreover, companies may have limited ways to monitor media coverage, especially if the report is isolated to local or national media. Linking 'significant media coverage' to a known incident or similar predefined threshold would be more appropriate.

Commented [A18]: [General Comment]
The term user regularly leads to confusion as to whether they are corporate customers (B2B) or end-users. B2B companies cannot know at all the number of affected (end-)users of the cloud service or which of them are located in the EU. We recognize that the draft suggests using estimations, however even an estimation would highly speculative. Different threshold values should apply to corporate customers than to end-users. Therefore, only a) should apply to B2B.

This ambiguity should be harmonized with regard to the explanation in Recital 30.

Furthermore, such a requirement should further define what is meant by "incidents" and should notably exclude "events.

Commented [A19]: [General Comment and suggestion to modify text]

Article 4 should be removed due to ambiguity. We recommend to replace "shall" with "might" and to raise the threshold for the recurring incidents. Incidents should relate to the services based on which the relevant entity falls under NIS2. It should be clarified that the recurring incidents are significant only if, collectively, they meet the threshold for significant incidents as described above.

(b) for a period of more than one hour, the average response time of a recursive or authoritative domain name resolution service to DNS requests is more than 10

seconds,

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the management of the DNS is compromised, except in cases where the data of fewer than 1 000 domain names managed by the DNS service provider, amounting to no more than 1 % of the domain names managed by the DNS service provider, are not correct because of misconfiguration.

Article 6

Significant incidents with regard to TLD name registries

With regard to TLD name registries, an incident shall be considered significant under Article 3 where it fulfils one or more of the following criteria:

(a) an authoritative domain name resolution service is completely unavailable;

(b) for a period of more than one hour, the average response time of an authoritative domain name resolution service to DNS requests is more than 10 seconds,

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the administration of the TLD is compromised.

Article 7

Significant incidents with regard to cloud computing service providers

With regard to cloud computing service providers, an incident shall be considered significant under Article 3 where it fulfils one or more of the following criteria:

(a) one or more of the primary cloud computing services provided is completely unavailable for more than ~~10~~ 30 minutes;

(b) ~~for~~ one or more of the primary cloud computing services provided~~, the customer service level agreement is not met~~ **is partially unavailable** for more than 5 % of the cloud computing service users in the Union, or for more than 1 million of the cloud computing service users in the Union, whichever number is smaller, for a duration of more than ~~one~~ **four** hours;

~~(c) the availability of the cloud computing service of a provider that has no customer service level agreement in place is limited for more than 5 % of the cloud computing service users in the Union, or for more than 1 million of the cloud computing service users in the Union, whichever number is smaller, for a duration of more than one hour;~~

~~(d)~~(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the cloud computing service is compromised as a result of a suspectedly malicious action,

~~(e)~~(d) 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 in the Union.

Commented [A20]: [General Comment Articles 7 to 14]
Service unavailability should only be a criterion for a significant incident in terms of non-compliance with the needs of the service user.

Commented [A21]: [General Comment]
Suggestion to include guidelines on how cloud service providers should communicate with their customers during and after a significant incident.

Commented [A22]: [Suggestion to modify text]
The meaning of the "cloud service" is unclear; it is unsure whether the whole application/cloud product or microservice level should be considered. This unclarity and the 10 min duration will lead to massive (our assessment is ~500 per year per company) reporting needs. Furthermore, the value of this reporting is questionable in terms of their importance, authorities' capacity to manage such a volume of reports, and/or provide assistance when necessary.

We suggest extending the timeline from 10 to 30 minutes. Alternatively, we suggest to focus only on the number of direct customers that were affected as the length of an incident does not necessarily indicate how significant the incident is.

Additionally, the inclusion of total unavailability duration criteria, without excluding or referencing service level agreements (SLAs) concluded with the client, is unjustifiable and contradicts the articles that include an SLA non-compliance criterion.

Commented [A23]: [Suggestion to modify text]
In B2B scenarios, SLAs are provided to legal entities only and are determined by percentage of service availability on a monthly/yearly basis, not per hour or per day or per minute. Our suggestion is to simply have a distinct duration as in the case of a total outage.

According to our calculations, the partial outage of the cloud application/product should last roughly 4h to start significantly impacting the user.

Alternatively, we suggest to focus on the number of direct customers that were affected as the length of an incident does not necessarily indicate how significant the incident is.

Commented [A24]: [General Comment]
Some articles set almost identical rules whether or not there are SLAs (with ambiguity around the term "limited"), failing to consider that lower service levels can be offered at significantly lower prices (for example: organizations testing cloud services in a "sandbox" mode for development do not need to pay for high availability and will seek very low prices).

Commented [A25]: [General Comment]
The mere information that a data/system compromise was due to malicious actions is not actionable. More important is knowing whether there is an impact on users. The possibility or confirmation of a deliberate cause should not be a condition as such but rather supplementary information included in the report. The primary conditions for reporting should be: compromised yes/no AND customers potentially impacted yes/no.

Article 8

Significant incidents with regard to data centre service providers

With regard to data centre service providers, an incident shall be considered significant under Article 3 where it fulfils one or more of the following criteria:

(a) one or more of the data centre services of one or more of the data centres operated by the provider is completely unavailable;

(b) the customer service level agreement for one or more of the data centre services of one or more of the data centres operated by the provider is not met for a duration of more than one hour;

(c) the customer service level agreement for one or more of the data centre services of one or more data centres operated by the provider is not met as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the data centre service is compromised as a result of a suspectedly malicious action,

(e) physical access to one or more of the data centres operated by the provider is compromised.

Article 9

Significant incidents with regard to content delivery network providers

With regard to content delivery network providers, an incident shall be considered significant under Article 3 where it fulfils one or more of the following criteria:

(a) one or more of the content delivery networks is completely unavailable for more than 10 minutes;

(b) the customer service level agreement for content delivery network performance is not met for more than 5 % of the content delivery network users in the Union, or for more than 1 million of the content delivery network users in the Union, whichever number is smaller, for a duration of more than one hour;

(c) the availability of the content delivery network of a provider that has no customer service level agreement in place is impacted by the incident;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the content delivery network is compromised as a result of a malicious action,

(e) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the content delivery network is compromised with an impact on more than 5 % of the content delivery network users in the Union.

Article 10

Commented [A26]: [General Comment]
Security responsibilities shared between MSP/MSSP and their customers should be further defined.

Significant incidents with regard to managed service providers and managed security service providers

With regard to managed service providers and managed security service providers, an incident shall be considered significant under Article 3 where it fulfils one or more of the following criteria:

(a) one or more of the managed services or managed security services is completely unavailable for more than 10 minutes;

~~(b) for one or more of the managed services or managed security services provided, the customer service level agreement is not met for more than 5 % of the service users in the Union, or for more than 1 million of the service users in the Union, whichever number is smaller, for a duration of more than one hour;~~

~~(c) the availability of one or more of the managed or managed security services of a provider that has no customer service level agreement in place is impacted by the incident;~~

~~(d)~~(b) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the managed service or the managed security service is compromised as a result of a ~~suspectedly~~ malicious action,

~~(e)~~(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the managed service or the managed security service, is compromised with an impact on more than 5 % of the managed service or the managed security service users in the Union.

Article 11

Significant incidents with regard to providers of online marketplaces

With regard to providers of online marketplaces, an incident shall be considered significant under Article 3 where it fulfils one or more of the following criteria:

(a) the online marketplace or part of its functionality is completely unavailable for more than 5 % of the online marketplace users in the Union, or for more than 1 million of the online marketplace users in the Union, whichever number is smaller;

(b) more than 5 % of the online marketplace users in the Union, or more than 1 million of the online marketplace users in the Union, whichever number is smaller, are impacted by large delays in orders;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the online marketplace is compromised as a result of a suspectedly malicious action,

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the online marketplace is compromised with an impact on more than 5 % of the online marketplace users in the Union.

Article 12

Significant incidents with regard to providers of online search engines

With regard to providers of online search engines, an incident shall be considered significant under Article 3 where it fulfils one or more of the following criteria:

Commented [A27]: [General Comment]
Does this mean that MSSP shall fall under both, the requirements under article 3 and this article? If so, this should be clarified as follows: "*MSSP shall, in addition to requirements under article 3, apply the following requirements*"

Commented [A28]: [General Comment]
This is too short and it might not lead to a significant impact. If a service has been recovered after 10 minutes (and should no other serious harm happened due to the service unavailability) it should not be considered significant. It probably happens too often so this would lead to excessive reporting.

Furthermore, MSSP provides different types of services (Cyber Threat Intelligence, Red Teaming, SOC monitoring, Incident Response, etc.) and not all of them are provided 24/7 without interruption. Also, not all these services are considered mission critical. If for example an attack hits the machine on which the platform for CTI runs, it creates an inconvenience to the clients, but it does not put them in danger in any way, also it does not put in danger the rest of the organisation if that machine is properly isolated from the network.

Commented [A29]: [Suggestion to remove the text]
To be removed because the SLA is already addressed in the contract between the provider and the client. The contract indicates what happens if the provider does not respect the SLA. Using the SLA as an indication of the criticality of an incident is therefore not a viable solution.

Furthermore, the 5% of the number of users threshold should only apply to Business to Consumers sectors, as in the Business to Business sector, user numbers is much more restricted and therefore the 5% threshold is too low.

Commented [A30]: [Suggestion to remove the text]
Proposing to delete this section as it is all-encompassing without any threshold criteria. Ref. section a)

Furthermore, it is confusing and misleading as even a trivial impact on the service provided to a client that has a contract that does not include a SLA would be significant.

Further clarification is required to describe the "impact".

Commented [A31]: [Suggestion to modify text]
Proposal to remove the word "suspectedly" as it is misleading. An action is either determined as malicious or it is not, without a forensic analysis, it is impossible to say if data has been manipulated by an attacker or not. Furthermore, this point must distinguish between sensitive data (like Personal Identifiable Information), and non-sensitive data (like the minutes of a project meeting).

Commented [A32]: [General Comment]
5% of the number of users threshold should only apply to Business to Consumers sectors, as in the Business to Business sector, user numbers is much more restricted and the 5% threshold can be reached quickly.

(a) the online search engine or part of its functionality is completely unavailable for more than 5 % of the online search engine users in the Union, or for more than 1 million of the online search engine users in the Union, whichever number is smaller;

(b) more than 5 % of the online search engine service users in the Union, or more than 1 million of the online search engine service users in the Union, whichever number is smaller, are impacted by large delays in response time;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the online search engine is compromised as a result of a suspectedly malicious action,

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the online search engine is compromised with an impact on more than 5 % of the online search engine users in the Union.

Article 13

Significant incidents with regard to providers of social networking services platforms

With regard to providers of social networking services platforms, an incident shall be considered significant under Article 3 where it fulfils one or more of the following criteria:

(a) the social networking service platform or part of its functionality is completely unavailable for more than 5 % of the social networking service platform users in the Union, or for more than 1 million of the social networking service platform users in the Union, whichever number is smaller;

(b) more than 5 % of the social networking service platform users in the Union, or more than 1 million of the social networking service platform users in the Union, whichever number is smaller, are impacted by large delays in response time;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the social networking service platform is compromised as a result of a suspectedly malicious action,

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the social networking service platform is compromised with an impact on more than 5 % of the social networking service platform users in the Union.

Article 14

Significant incidents with regard to trust service providers

With regard to trust service providers, an incident shall be considered significant under Article 3 where it fulfils one or more of the following criteria:

(a) a trust service, or a part of it, is completely unavailable for more than 10 minutes;

(b) a trust service, or a part of it, is unavailable to users, or relying parties, for more than one hour calculated on a calendar week basis;

(c) more than 1 % of the customers of the trust service in the Union are impacted by large delays in response time of the trust service;

(d) physical access to one or more of the areas where network and information systems

are located and to which access is restricted to trusted personnel of the trust service provider, or the protection of such physical access, is compromised;

(e) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the trust service is compromised with an impact on more than 1 % of the customers of the trust service in the Union.

Article 15

Repeal

Commission Implementing Regulation (EU) 2018/151[4] is repealed with effect from [18 October 2024].

Article 16

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall apply from [18 October 2024].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
Ursula von der Leyen
The President

Commented [A33]: [General Comment]
It is an unrealistic short timeframe to be able to demonstrate compliance. Therefore, a grace period should be introduced to establish relevant processes based on the final thresholds. Dependencies to potential national legislation delays, or the introduction of a unified notification portal need to be taken into account.

[4] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (OJ L 26, 31.1.2018, p. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

Ref. Ares(2024)4640447 - 27/06/2024

EUROPEAN COMMISSION

Brussels, XXX
[…](2024) XXX draft

ANNEX

ANNEX

to the

Commission Implementing Regulation laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

ANNEX

Technical and methodological requirements referred to in Article 2 of this Regulation

1. POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS (ARTICLE 21(2), POINT (A) OF DIRECTIVE (EU) 2022/2555)

1.1. Policy/ies on the security of network and information systems

1.1.1. For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the policy/ies on the security of network and information systems shall:

(a) set out the relevant entities' approach to managing the security of their network and information systems;

(b) be appropriate to and complementary with the relevant entities' business strategy and objectives;

(c) set out network and information security objectives;

(d) establish the risk tolerance level in accordance with the risk appetite of the relevant entities;

(e) include a commitment to satisfy applicable requirements related to the security of network and information systems;

(f) include a commitment to continual improvement of the security of network and information systems;

(g) include a commitment to provide the appropriate resources needed for its implementation, including the necessary staff, financial resources, processes, tools and technologies;

(h) be communicated to and acknowledged by relevant employees and relevant interested parties;

(i) lay down roles and responsibilities pursuant to point 1.2.;

(j) list the documentation to be kept;

(k) list the topic-specific policies;

(l) lay down indicators and measures to monitor its implementation and the current status of relevant entities' level of network and information security;

(m) indicate the date of the formal approval by the management bodies or relevant level of management of the relevant entities (the 'management bodies').

1.1.2. The network and information system policy as well as the topic-specific policies shall be reviewed and, where appropriate, updated by ~~management bodies~~ at planned intervals and when significant incidents or significant changes to operations or risks occur. The result of the reviews shall be documented.

1.2. Roles, responsibilities and authorities

1.2.1. As part of their policy on the security of network and information systems referred to in point 1.1, the relevant entities shall lay down responsibilities and authorities for

Commented [A1]: [Suggestion to modify text]
This addition to clarify that typically there is not only one policy but a set of policies defining all aspects of the security of network and information systems.

Commented [A2]: [Suggestion to modify text]
Management bodies do not update policies. It is usually subject matter experts.

network and information system security and assign them to roles, allocate them according to the relevant entities' needs, and communicate them to the management bodies.

1.2.2. The relevant entities shall require all personnel and third parties to apply network and information system security in accordance with the established network and information security policy, topic-specific policies and procedures of the relevant entities.

1.2.3. At least one person shall report directly to the management bodies on matters of network and information system security.

1.2.4. Depending on the size of the relevant entities, network and information system security shall be covered by dedicated roles or duties carried out in addition to existing roles.

1.2.5. Conflicting duties and conflicting areas of responsibility shall be segregated, where applicable.

1.2.6. Roles, responsibilities and authorities shall be reviewed and, where appropriate, updated by management bodies at planned intervals and when significant incidents or significant changes to operations or risks occur.

2. RISK MANAGEMENT POLICY (ARTICLE 21(2), POINT (A) OF DIRECTIVE (EU) 2022/2555)

2.1. Risk management framework

2.1.1. For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the relevant entities shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems. The relevant entities shall perform and document risk assessments and, based on the results, establish, implement and monitor a risk treatment plan. Risk assessment results and residual risks shall be accepted by management bodies or by risk owners, provided that the relevant entities ensure adequate reporting to the management bodies.

2.1.2. For the purpose of point 2.1.1., the relevant entities shall establish and communicate to their staff procedures for identification, analysis, assessment and treatment of risks ('cybersecurity risk management process'). The cybersecurity risk management process shall be an integral part of the relevant entities' overall risk management process, where applicable. As part of the cybersecurity risk management process, the relevant entities shall:

(a) include a risk management methodology and, where appropriate, tools based on relevant European standards and international standards;

(b) establish and maintain risk criteria relevant to the relevant entities;

(c) in line with an all-hazards approach, identify and document the risks posed to the security of network and information systems, in particular in relation to third parties and risks that could lead to disruptions in the availability, integrity, authenticity and confidentiality of the network and information systems, including the identification of single point of failures;

(d) identify risk owners;

Commented [A3]: [General Comment]
Suggestion to replace "shall" with "should" throughout the whole text to provide more room for flexibility.

We strongly advise to refer to existing European and international standards directly, instead of creating an overly prescriptive list of legal requirements. Existing certifications (e.g. C5) can be used to show presumption of conformity with the NIS2 Directive. Various sets of requirements and controls, such as ISO/IEC 27001, ISO/IEC 27002 and further international schemes for cybersecurity and information security requirements and controls should be considered to achieve a high common level of cybersecurity as soon as possible.

For the NIS1 Directive, ENISA published guidelines mapping security requirements against international standards, providing a practical roadmap for companies to prepare for compliance. We highly encourage a similar exercise for the NIS2 Directive and the cybersecurity risk-management measures.

Commented [A4]: [General Comment]
Measures provided in the annex should be taken into account considering the principles of adequacy, proportionality, and risk assessment, and considering the implementation cost.

(e) analyse the risks posed to the security of network and information systems, including threat, likelihood, impact, and risk level, taking into account cyber threat intelligence and vulnerabilities;

(f) evaluate the identified risks based on risk criteria;

(g) identify and prioritize appropriate risk treatment measures, taking account of the risk assessment results and the results of the procedure to assess the effectiveness of cybersecurity risk-management measures;

(h) identify who is responsible for implementing the cybersecurity risk management measures and when they should be implemented;

(i) make key personnel aware of the main risks and of the cybersecurity riskmanagement measures;

(j) document the chosen security measures and the reasons justifying the acceptance of residual risks in a comprehensible manner.

2.1.3. The relevant entities shall review and, where appropriate, update the risk assessment results and the risk treatment plan at planned intervals and when significant changes to operations or risks or significant incidents occur.

2.2. Compliance monitoring

2.2.1. The relevant entities shall regularly review the compliance with their policies on network and information system security, topic-specific policies, rules, and standards. The management bodies shall be informed of the status of network and information security on the basis of the compliance reviews by means of regular reporting.

2.2.2. The relevant entities shall put in place an effective compliance reporting system which shall be appropriate to their structures, operating environments and threat landscapes. The compliance reporting system shall be capable to provide to the management bodies an informed view of the current state of the relevant entities' management of risks.

2.2.3. The relevant entities shall perform the compliance monitoring at planned intervals and when significant incidents or significant changes to operations or risks occur.

2.3. Independent review of information and network security

2.3.1. The relevant entities shall review independently their approach to managing network and information system security and its implementation including people, processes and technologies.

2.3.2. The relevant entities shall develop and maintain processes to conduct independent reviews which shall be carried out by individuals with appropriate audit competence.

The persons conducting the reviews shall not be in the line of authority of the personnel of the area under review. If the size of the entities do not allow such separation of line of authority, the relevant entities shall put in place alternative measures to guarantee the impartiality of the reviews.

2.3.3. The results of the independent reviews, including the result from the compliance monitoring pursuant to point 2.2. and the monitoring and measurement pursuant to point 7, shall be reported to the management bodies. Corrective actions shall be taken or residual risk accepted according to the relevant entities' risk acceptance criteria.

2.3.4. The independent reviews shall take place at planned intervals and when significant incidents or significant changes to operations or risks occur.

3. INCIDENT HANDLING (ARTICLE 21(2), POINT (B), OF DIRECTIVE (EU) 2022/2555)

3.1. Incident handling policy

3.1.1. For the purpose of Article 21(2), point (b) of Directive (EU) 2022/2555, the relevant entities shall establish an incident handling policy laying down the roles, responsibilities, and procedures for detecting, analysing, containing or responding to, recovering, documenting and reporting of incidents in a timely manner.

3.1.2. The policy referred to in point 3.1.1shall include:

(a) a categorisation system for incidents;

(b) effective communication plans including for escalation and reporting;

(c) assignment of roles to detect and appropriately respond to incidents to competent employees;

(d) documents to be used in the course of incident detection and response such as incident response manuals, escalation charts, contact lists and templates;

(e) interfaces between the incident handling and business continuity management.

3.1.3. The roles, responsibilities and procedures laid down in the policy shall be tested and reviewed and, where appropriate, updated at planned intervals and after significant incidents or significant changes to operations or risks.

3.2. Monitoring and logging

3.2.1. The relevant entities shall lay down procedures and use tools to monitor and log activities on their network and information systems to detect events that could be considered as incidents and respond accordingly to mitigate the impact.

3.2.2. To the extent feasible, monitoring shall be automated and carried out either continuously or in periodic intervals, subject to business capabilities. The relevant entities shall implement their monitoring activities in a way which minimises false positives and false negatives.

3.2.3. The relevant entities shall maintain, document, and review logs. Logs shall include:

(a) outbound and inbound network traffic;

(b) creation, modification or deletion of users of the relevant entities' network and information systems and extension of the permissions;

(c) access to systems and applications;

(d) authentication-related events;

(e) all privileged access to systems and applications, and activities performed by administrative accounts;

(f) access or changes to critical configuration and backup files;

(g) event logs and logs from security tools, such as antivirus, intrusion detection systems or firewalls;

Commented [A5]: [General Comment]
Providing communication models could enhance the overall effectiveness of these guidelines.

Commented [A6]: [General Comment]
Further clarification of this paragraph is needed as it might imply that all traffic must be logged, necessitating specific and costly infrastructure (particularly for storing information). Since systematic logging is not feasible but may be justifiable in sensitive cases, we propose specifying that this action is performed "when appropriate."

~~(h) use of system resources, as well as their performance;~~

~~(i)~~(h) physical access to facilities, where appropriate;

~~(j)~~(i) access to and use of their network equipment and devices;

~~(k)~~(j) activation, stopping and pausing of the various logs;

~~(l)~~(k) environmental events, such as flooding alarms, where appropriate.

3.2.4. The logs shall be reviewed for any unusual or unwanted trends. The relevant entities shall lay down appropriate values for alarm thresholds. If the laid down values for alarm threshold are exceeded, an alarm shall be triggered, where appropriate, automatically. The responsible employee shall ensure that, in case of an alarm, a qualified and appropriate response is initiated.

3.2.5. The relevant entities shall maintain and back up logs for a predefined period and shall store the logs at a central location and protect them from unauthorised access or changes.

3.2.6. The relevant entities shall ensure that all systems have synchronised time sources to be able to correlate logs between systems for event assessment. The relevant entities shall establish and keep a list of all assets that are being logged and ensure that monitoring and logging systems are redundant. The availability of the monitoring and logging systems shall be monitored independently.

3.2.7. The procedures as well as the list of assets that are being logged shall be reviewed and, where appropriate, updated at regular intervals and after significant incidents.

3.3. Event reporting

3.3.1. The relevant entities shall put in place a simple mechanism allowing their employees, suppliers, and customers to report suspicious events.

3.3.2. The relevant entities shall communicate the event reporting mechanism to their suppliers and customers and shall regularly train their employees how to use the mechanism.

3.4. Event assessment and classification

3.4.1. The relevant entities shall assess suspicious events to determine whether they constitute incidents and, if so, determine their nature and severity.

3.4.2. For the purpose of point 3.4.1, the relevant entities shall act in the following manner:

(a) carry out the assessment based on predefined criteria laid down in advance, and on a triage to determine prioritisation of incident containment and eradication;

(b) assess the existence of recurring incidents as referred to in Article 4 of this Regulation on a quarterly basis;

(c) review the appropriate logs for the purposes of event assessment and classification;

(d) put in place a process for log correlation and analysis, and

(e) reassess and reclassify events in case of new information becoming available or after analysis of previously available information.

Commented [A7]: [Suggestion to modify text]
Logging the use of system resources does not seem relevant to the scope of this section and should be removed.

3.5. Incident response

3.5.1. The relevant entities shall respond to incidents in accordance with documented procedures and in a timely manner.

3.5.2. The incident response procedures shall include the following stages:

(a) incident containment, to prevent the consequences of the incident from spreading;

(b) eradication, to prevent the incident from continuing or reappearing, (c) recovery from the incident, where necessary.

3.5.3. The relevant entities shall establish communication plans and procedures:

(a) with the Computer Security Incident Response Teams (CSIRTs) or, where applicable, the competent authorities, related to incident notification; (b) with relevant internal and external stakeholders.

3.5.4. The relevant entities shall log incident response activities, and record evidence.

3.5.5. The relevant entities shall test at planned intervals their incident response procedures.

3.6. Post-incident reviews

3.6.1. The relevant entities shall carry out post-incident reviews that shall identify the root cause of the incident and result in lessons learned to reduce the occurrence and consequences of future incidents.

3.6.2. The relevant entities shall ensure that post-incident reviews contribute to improving their approach to network and information security, to risk treatment measures, and to incident handling, detection and response procedures.

3.6.3. The relevant entities shall review at planned intervals if significant incidents led to post-incident reviews.

4. BUSINESS CONTINUITY AND CRISIS MANAGEMENT (ARTICLE 21(2), POINT (C), OF DIRECTIVE (EU) 2022/2555)

4.1. Business continuity and disaster recovery plans

4.1.1. For the purpose of Article 21(2), point (c) of Directive (EU) 2022/2555, the relevant entities shall lay down and maintain a business continuity and disaster recovery plan to apply in the case of incidents.

4.1.2. The relevant entities' operations shall be restored according to the business continuity and disaster recovery plan. The plan shall be informed by the results of the risk assessment and shall include the following:

(a) purpose, scope and audience;

(b) roles and responsibilities;

(c) key contacts and (internal and external) communication channels;

(d) conditions for plan activation and deactivation;

(e) order of recovery for operations;

(f) recovery plans for specific operations, including recovery objectives;

(g) required resources, including backups and redundancies; (h) restoring and resuming activities from temporary measures; (i) interfaces to incident handling.

4.1.3. The relevant entities shall carry out a business impact analysis to assess the potential impact of severe disruptions to their business operations and shall, based on the results of the business impact analysis, establish continuity requirements for the network and information systems.

4.1.4. The business continuity plan and disaster recovery plan shall be tested, reviewed and, where appropriate, updated at planned intervals and following significant incidents or significant changes to operations or risks. The relevant entities shall ensure that the plans incorporate lessons learnt from such tests.

4.2. Backup management

4.2.1. The relevant entities shall maintain backup copies of information and provide sufficient available resources, including facilities, network and information systems and staff.

4.2.2. Based on the results of the risk assessment and the business continuity plan, the relevant entities shall lay down backup plans which include the following:

(a) recovery times;

(b) assurance that backup copies are complete and accurate, including configuration data and information stored in cloud computing service environment;

(c) storing backup copies (online or offline) in a safe location or locations, which are not in the same network as the system, and are at sufficient distance to escape any damage from a disaster at the main site;

(d) appropriate physical and logical access controls to backup copies, in accordance with the information classification level;

(e) restoring information from backup copies, including approval processes; (f) retention periods based on business and regulatory requirements.

4.2.3. The relevant entities shall perform regular integrity checks on the backup copies.

4.2.4. The relevant entities shall ensure sufficient availability of resources by at least partial redundancy of the following:

(a) network and information systems;

(b) assets, including facilities, equipment and supplies;

(c) personnel with the necessary responsibility, authority and competence; (d) appropriate communication channels.

4.2.5. The relevant entities shall ensure that monitoring and adjustment of resources, including facilities, systems and personnel, is duly informed by backup and redundancy requirements.

4.2.6. The relevant entities shall carry out regular testing of the recovery of backup copies and redundancies to ensure that, in recovery conditions, they can be relied upon and cover the copies, processes and knowledge to perform an effective recovery. The relevant entities shall document the results of the tests and, where needed, take corrective action.

Commented [A8]: [General Comment]
Currently, some lower-priced services available on the market do not include backups. While it is essential to properly inform clients to avoid any issues in case of incidents, there is a risk that these more affordable offers may be eliminated due to the application of this standard.
This issue is compounded by the fact that, concurrently and contradictorily, operators [especially cloud providers] are required, for environmental footprint management reasons, to avoid offering backup services systematically when not justified by the service provided.

4.3. Crisis management

4.3.1. The relevant entities shall put in place processes for crisis management.

4.3.2. The relevant entities shall ensure that crisis management processes address at least the following elements:

(a) roles and responsibilities for personnel, ensuring that all staff know their roles in crisis situations, including specific steps to follow;

(b) appropriate communication means between the relevant entities and relevant competent authorities;

(c) application of appropriate controls such as supporting systems, processes and additional capacity.

For the purpose of point (b), the flow of information between the relevant entities and relevant competent authorities shall include both obligatory communications, such as incident reports and related timelines, and nonobligatory communications.

4.3.3. The relevant entities shall implement a process for managing and making use of information received from the CSIRTs or, where applicable, the competent authorities, concerning incidents, vulnerabilities, threats or security controls.

4.3.4. The relevant entities shall test, review and, where appropriate, update the crisis management plan on a regular basis or following significant incidents or significant changes to operations or risks.

5. SUPPLY CHAIN SECURITY (ARTICLE 21(2), POINT (D), OF DIRECTIVE (EU) 2022/2555)

5.1. Supply chain security policy

5.1.1. For the purpose of Article 21(2), point (d) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a supply chain security policy which governs the relations with their direct suppliers and service providers in order to mitigate the identified risks to the security of network and information systems. In the supply chain security policy, the relevant entities shall identify their role in the supply chain and communicate it to their direct suppliers and service providers.

5.1.2. As part of the supply chain security policy referred to in point 5.1.1, the relevant entities shall lay down criteria to select and contract suppliers and service providers. Those criteria shall include the following:

(a) the cybersecurity practices of the suppliers and service providers, including their secure development procedures;

(b) the ability of the suppliers and service providers to meet cybersecurity specifications set by the entities;

(c) the overall quality and resilience of ICT products and ICT services and the cybersecurity risk-management measures embedded in them, including the risks and classification level of the ICT products and ICT services;

(d) the ability of the relevant entities to diversify sources of supply and limit vendor lock-in.

Commented [A9]: [General Comment]
Useful to establish a minimum set of security requirements that apply to all suppliers.

Criteria differentiated by supplier type could be included, such as creating a checklist of security practices tailored to suppliers of various sizes and sectors.

5.1.3. When establishing their supply chain security policy, relevant entities shall take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) of Directive (EU) 2022/2555, where applicable.

5.1.4. Based on the supply chain security policy and taking into account the results of the risk assessment carried out in accordance with point 2.1. of this Annex, the relevant entities shall ensure that their contracts with the suppliers and service providers specify, where appropriate through service level agreements, specify the following, where appropriate:

(a) cybersecurity requirements for the suppliers or service providers, including requirements as regards the security in acquisition of ICT services or ICT products set out in point 6.1.;

(b) requirements regarding skills and training, and where appropriate professional certifications, required from the suppliers' or service providers' employees;

(c) requirements regarding background checks of the suppliers' and service providers' employees pursuant to point 10.2.;

(d) an obligation on suppliers and service providers to notify, without undue delay, the relevant entities of incidents that present a risk to the security of the network and information systems of those entities;

(e) provisions on repair times;

(f) the right to audit or right to receive audit reports;

(g) an obligation on suppliers and service providers to handle vulnerabilities that present a risk to the security of the network and information systems of the relevant entities;

(h) requirements regarding subcontracting and, where the relevant entities allow subcontracting, cybersecurity requirements for subcontractors in accordance with the cybersecurity requirements referred to in point (a);

(i) obligations on the suppliers and service providers at the termination of the contract, such as retrieval and disposal of the information obtained by the suppliers and service providers in the exercise of their tasks.

5.1.5. The relevant entities shall take into account the elements referred to in point 5.1.2 and 5.1.3. as part of the selection process of new suppliers and service providers, as well as part of the procurement process referred to in point 6.1.

5.1.6. The relevant entities shall review the supply chain security policy, and monitor, evaluate and, where necessary, act upon changes in the cybersecurity practices of suppliers and service providers, at planned intervals and when significant changes to operations or risks or significant incidents related to the provision of ICT services or having impact on the security of the ICT product from suppliers and service providers occur.

5.1.7. For the purpose of point 5.1.5., the relevant entities shall:

(a) regularly monitor reports on the implementation of the service level agreements, where applicable;

(b) review incidents related to ICT products and ICT services from suppliers and service providers;

(c) assess the need for unscheduled reviews and document the findings in a comprehensible manner;

Commented [A10]: [Suggestion to modify text]
Add "professional" to make it clearer in the text that staff should have the appropriate knowledge and skills demonstrated through professional certifications in line with their expected tasks.

(d) analyse the risks presented by changes related to ICT products and ICT services from suppliers and service providers and, where appropriate, take mitigating measures in a timely manner.

5.2. Directory of suppliers and service providers

The relevant entities shall maintain and keep up to date a registry of their direct suppliers and service providers, including:

(a) contact points for each direct supplier and service provider;

(b) a list of ICT products, ICT services, and ICT processes provided by the direct supplier or service provider to the entities.

6. SECURITY IN NETWORK AND INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE (ARTICLE 21(2), POINT (E), OF DIRECTIVE (EU) 2022/2555)

6.1. Security in acquisition of ICT services or ICT products

6.1.1. For the purpose of Article 21(2), point (e) of Directive (EU) 2022/2555, the relevant entities shall set and implement processes and procedures to manage risks stemming from the acquisition of ICT services or ICT products for components that are critical for the relevant entities' security of network and information systems, based on the risk assessment, from suppliers or service providers throughout their life cycle.

6.1.2. For the purpose of point 6.1.1., the processes and procedures referred to in point 6.1.1. shall include:

(a) security requirements to apply to the ICT services or ICT products to be acquired;

(b) requirements regarding security updates throughout the entire lifetime of the ICT services or ICT products, or replacement after the end of the support period;

(c) information describing the hardware and software components used in the ICT services or ICT products;

(d) information describing the implemented cybersecurity functions of the ICT services or ICT products and the configuration required for their secure operation;

(e) assurance that the ICT services or ICT products comply with the security requirements according to point (a);

(f) appropriate methods for validating that the delivered ICT services or ICT products are compliant to the stated security requirements, as well as documentation of the results of the validation.

6.1.3. The relevant entities shall review and, where appropriate, update the processes and procedures at planned intervals and when significant incidents occur.

6.2. Secure development life cycle

6.2.1. The relevant entities shall lay down, implement and apply rules for the secure development of network and information systems, including software, and apply them when acquiring or developing network and information systems. The rules shall cover

all development phases, including specification, design, development, implementation and testing.

6.2.2. The relevant entities shall:

(a) carry out an analysis of security requirements at the specification and design phases of any development or acquisition project undertaken by the relevant entities or on behalf of those entities;

(b) apply principles for engineering secure systems and secure coding principles to any information system development activities such as promoting cybersecurity-by-design, zero trust architectures;

(c) lay down security requirements regarding development environments;

(d) establish and implement security testing processes in the development life cycle;

(e) appropriately select, protect and manage security test information;

(f) sanitise and anonymise testing data according to the risk assessment.

6.2.3. For outsourced development and procurement of network and information systems, the relevant entities shall apply the policies and procedures referred to in points 5 and 6.1.

6.2.4. The relevant entities shall review and, where appropriate, update their secure development rules at planned intervals.

6.3. Configuration management

6.3.1. The relevant entities shall establish, document, implement, and monitor configurations, including security configurations of hardware, software, services and networks.

6.3.2. For the purpose of point 6.3.1., the relevant entities shall:

(a) lay down configurations, including security configurations, for their hardware, software, services and networks;

(b) lay down and implement processes and tools to enforce the laid down configurations, including security configurations, for hardware, software, services and networks, for newly installed systems as well as for operational systems over their lifetime.

6.3.3. The relevant entities shall review and, where appropriate, update configurations at planned intervals or when significant incidents or significant changes to operations or risks occur.

6.4. Change management, repairs and maintenance

6.4.1. The relevant entities shall apply management procedures to changes, repairs and maintenance to network and information systems. Where applicable, the procedures shall be consistent with the relevant entities' general policies concerning change management.

6.4.2. The procedures referred to in point 6.4.1. shall be applied for releases, modifications and emergency changes of any operational software, hardware and changes to the configuration.

6.4.3. In the event that the regular change control procedures could not be followed due to an emergency, the relevant entities shall document the result of the change, and the explanation for why the procedures could not be followed.

6.4.4. The relevant entities shall review and, where appropriate, update the procedures at planned intervals and when significant incidents or significant changes to operations or risks.

6.5. Security testing

6.5.1. The relevant entities shall establish, implement and apply a policy and procedures for security testing.

6.5.2. The relevant entities shall:

(a) establish, based on the risk assessment, the need, scope, frequency and type of security tests;

(b) carry out security tests according to a documented test methodology, covering the components identified as relevant for secure operation in a risk analysis;

(c) document the type, scope, time and results of the tests, including assessment of criticality and mitigating actions for each finding;

(d) apply mitigating actions in case of critical findings.

6.5.3. The relevant entities shall review and, where appropriate, update their security testing policies at planned intervals.

6.6. Security patch management

6.6.1. The relevant entities shall specify and apply procedures for ensuring that:

(a) security patches are applied within a reasonable time after they become available;

(b) security patches are tested before being applied in production systems;

(c) security patches come from trusted sources and are checked for integrity;

(d) additional measures are implemented and residual risks are accepted in cases where a patch is not available or not applied pursuant to point 6.6.2.

6.6.2. By way of derogation from point 1(a), the relevant entities may choose not to apply security patches when the disadvantages of applying the security patches outweigh the cybersecurity benefits. The relevant entities shall duly document and substantiate the reasons for any such decision.

6.7. Network security

6.7.1. The relevant entities shall take the appropriate measures to protect their network and information systems from cyber threats.

6.7.2. For the purpose of point 6.7.1., the relevant entities shall:

(a) document the architecture of the network in a comprehensible and up to date manner;

(b) determine and apply controls to protect the relevant entities' internal network domains from unauthorised access;

(c) configure controls to prevent accesses not required for the operation of the relevant entities;

(d) determine and apply controls for remote access to network and information systems, including access by service providers;

(e) not use systems used for administration of the security policy implementation for other purposes;

(f) explicitly forbid or deactivate unneeded connections and services;

(g) where appropriate, exclusively allow access to the relevant entities' network and information systems by devices authorised by those entities;

(h) allow connections of service providers only after an authorisation request and for a set time period, such as the duration of a maintenance operation;

(i) establish communication between distinct systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of their end points and protection of the channel data from modification or disclosure;

(j) adopt an implementation plan for the secure and full transition towards latest generation network layer communication protocols to reduce the attack surface of the networks and establish measures to accelerate such transition;

(k) adopt an implementation plan for the deployment of internationally agreed and interoperable modern e-mail communications standards to secure e-mail communications to mitigate vulnerabilities linked to e-mail-related threats and establish measures to accelerate such deployment;

(l) apply best practices for Internet routing security and routing hygiene of traffic originating from and destined to the network.

6.7.3. The relevant entities shall review and, where appropriate, update these measures at planned intervals and when significant incidents or significant changes to operations or risks occur.

6.8. Network segmentation

6.8.1. The relevant entities shall segment systems into networks or zones in accordance with the results of the risk assessment referred to in point 2.1. They shall segment their systems and networks from third parties' systems and networks.

6.8.2. For that purpose, the relevant entities shall:

(a) consider the functional, logical and physical relationship, including location, between trustworthy systems and services;

(b) apply the same security measures to all network and information systems in the same zone;

(c) grant access to a network or zone based on an assessment of its security requirements;

(d) keep all systems that are critical to the relevant entities operation or to safety in one or more secured zones;

(e) restrict access and communications between and within zones to those necessary for the operation of the relevant entities or for safety;

(f) separate the dedicated network for administration of network and information systems from the relevant entities' operational network;

(g) segregate network administration channels from other network traffic;

(h) separate the production systems for the entities' services from systems used in development and testing, including backups.

6.8.3. The relevant entities shall review and, where appropriate, update network segmentation at planned intervals and when significant incidents or significant changes to operations or risks.

6.9. Protection against malicious and unauthorised software

6.9.1. The relevant entities shall protect their network and information systems against malicious and unauthorised software.

6.9.2. For that purpose, the relevant entities shall in particular ensure that their network and information systems are equipped with malware detection and repair software, which is updated regularly in accordance with the with the risk assessment and the contractual agreements with the providers.

6.10. Vulnerability handling and disclosure

6.10.1. The relevant entities shall obtain information about technical vulnerabilities in their network and information systems, evaluate their exposure to such vulnerabilities, and take appropriate measures to manage the vulnerabilities.

6.10.2. For the purpose of point 6.10.1., the relevant entities shall:

(a) monitor information about vulnerabilities through appropriate channels, such as announcements of CSIRTs, competent authorities or information provided by suppliers or service providers.

(b) perform, where appropriate, vulnerability scans, and record evidence of the results of the scans, at planned intervals;

(c) address, without undue delay, vulnerabilities identified by the relevant entities as critical to their operations;

(d) ensure that their vulnerability handling is compatible with their change management and incident management procedures;

(e) lay down a procedure for disclosing vulnerabilities in accordance with the applicable national coordinated vulnerability disclosure policy.

6.10.3. When justified by the potential impact of the vulnerability, the relevant entities shall create and implement a plan to mitigate the vulnerability. In other cases, the relevant entities shall document and substantiate the reason why the vulnerability does not require remediation.

6.10.4. The relevant entities shall review and, where appropriate, update at planned intervals the channels they use for monitoring vulnerability information.

7. POLICIES AND PROCEDURES TO ASSESS THE EFFECTIVENESS OF CYBERSECURITY RISK-MANAGEMENT MEASURES (ARTICLE 21(2), POINT (F), OF DIRECTIVE (EU) 2022/2555)

7.1.1. For the purpose of Article 21(2), point (f) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures to assess whether the policy on the security of network and information systems referred to in point 1.1. is effectively implemented and maintained.

7.1.2. The policy and procedures referred to in point 7.1. shall take into account results of the risk assessment pursuant to point 2.1. and past significant incidents. The procedures shall include security assessments and security testing. The relevant entities shall determine:

(a) what cybersecurity risk-management measures are to be monitored and measured, including processes and controls;

(b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

(c) when the monitoring and measuring is to be performed;

(d) who is responsible for monitoring and measuring the effectiveness of the cybersecurity risk-management measures;

(e) when the results from monitoring and measurement are to be analysed and evaluated;

(f) who has to analyse and evaluate these results.

7.1.3. The relevant entities shall review and, where appropriate, update the policy and procedures at planned intervals and when significant incidents or significant changes to operations or risks.

8. BASIC CYBER HYGIENE PRACTICES AND SECURITY TRAINING (ARTICLE 21(2), POINT (G), OF DIRECTIVE (EU) 2022/2555)

8.1. Awareness raising and basic cyber hygiene practices

8.1.1. For the purpose of Article 21(2), point (g) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees are aware of risks, are informed of the importance of cybersecurity and apply cyber hygiene practices.

8.1.2. The relevant entities shall offer to all employees, including members of management bodies, an awareness raising programme, which shall:

(a) be scheduled over time, so that the activities are repeated and cover new employees;

(b) be established in line with the network and information security policy, topicspecific policies and relevant procedures on network and information security;

(c) cover cybersecurity risk-management measures in place, contact points and resources for additional information and advice on cybersecurity matters, as well as cyber hygiene practices for users.

8.1.3. The awareness raising program shall be tested in terms of effectiveness, updated and offered at planned intervals taking into account changes in cyber hygiene practices, and the current threat landscape and risks posed to the relevant entities.

Commented [A11]: [General Comment]
NIS2 should be more prescriptive in types of hygiene practices, expectations for the adoption of protocols and controls, and how best to treat specific risk vectors. For example, industry and binding industrial guidance are moving in the direction of requiring DMARC. DMARC, which stands for "Domain-based Message Authentication, Reporting & Conformance", is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email. The Annex should introduce specific, long-standing protocols that are freely adoptable and empirically proven to treat some of the most pervasive threats.

8.2. Security training

8.2.1. The relevant entities shall ensure that employees, whose roles require security relevant skill sets and expertise, receive training on network and information system security **and possess professional certifications that are appropriate according to recognised market standards for the performance of their activities.**

8.2.2. The relevant entities shall establish, implement and apply a training program in line with the network and information security policy, topic-specific policies and other relevant procedures on network and information security which lays down the training needs for certain roles and positions based on criteria. The European Cybersecurity Skills Framework (ECSF) should be taken into account where relevant to establishing training needs.

8.2.3. The training referred to in point 8.2.1. shall be relevant to the job function of the employee and its effectiveness shall be assessed. Training shall take into consideration security measures in place and cover the following:

(a) regular and documented instructions regarding the secure configuration and operation of the network and information systems, including mobile devices;

(b) regular and documented briefing on known cyber threats;

(c) regular and documented training of the behaviour when security-relevant events occur.

8.2.4. The relevant entities shall apply training to staff members who transfer to new positions or roles which require security relevant skill sets and expertise.

8.2.5. The program shall be updated and run periodically taking into account applicable policies and rules, assigned roles, responsibilities, as well as known cyber threats and technological developments.

9. CRYPTOGRAPHY (ARTICLE 21(2), POINT (H), OF DIRECTIVE (EU) 2022/2555)

9.1.1. For the purpose of Article 21(2), point (h) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures related to cryptography, with a view to ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and integrity of information in line with the relevant entities' information classification and the results of the risk assessment.

9.1.2. The policy and procedures referred to in point 9.1 shall establish:

(a) in accordance with the relevant entities' classification of assets, the type, strength and quality of the cryptographic measures required to protect the relevant entities' assets;

(b) based on point (a), the protocols to be adopted, as well as cryptographic algorithms, cipher strength, cryptographic solutions and usage practices to be approved and required for use in the entities, following, where appropriate, a cryptographic agility approach;

(c) the relevant entities' approach to key management, including methods for the following:

(i) generating keys for different cryptographic systems and applications;

Commented [A12]: [Suggestion to modify text]
The Implementing Act should be internally consistent when it comes to requirements for internal personnel and external suppliers – the standard required in terms of security and qualifications should not be lower for internal staff. It should therefore be clearer in the text that staff should have the appropriate knowledge and skills demonstrated through professional certifications in line with their expected tasks.

Commented [A13]: [Suggestion to modify text]
European Cybersecurity Skills Framework (ECSF) has been a useful harmonised EU-level benchmark for cybersecurity profiles since it was established in 2022 – and indeed it is mentioned as a reference in recent pieces of cyber legislation such as the Cyber Solidarity Act. For this reason, it is important that the ECSF receive the same consideration and recognition also in the implementing Act and Annex. should be duly recognised here as well with the objective for determining training needs for staff.

(ii) issuing and obtaining public key certificates;

(iii) distributing keys to intended entities, including how to activate keys when received;

(iv) storing keys, including how authorised users obtain access to keys;

(v) changing or updating keys, including rules on when and how to change keys;

(vi) dealing with compromised keys;

(vii) revoking keys including how to withdraw or deactivate keys;

(viii) recovering lost or corrupted keys;

(ix) backing up or archiving keys;

(x) destroying keys;

(xi) logging and auditing of key management-related activities;

(xii) setting activation and deactivation dates for keys ensuring that the keys can only be used for the specified period of time according to the organization's rules on key management;

(xiii) handling legal requests for access to cryptographic keys.

9.1.3. The relevant entities shall review and, where appropriate, update their policy and procedures at planned intervals, taking into account the state of the art in cryptography.

10. HUMAN RESOURCES SECURITY (ARTICLE 21(2), POINT (I), OF DIRECTIVE (EU) 2022/2555)

10.1. Human resources security

10.1.1. For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees and direct suppliers and service providers, wherever applicable, understand, demonstrate and commit to their security responsibilities, as appropriate for the offered services and the job and in line with the relevant entities' policy on the security of network and information systems.

10.1.2. The requirement referred to in point 10.1.1. shall include the following:

(a) mechanisms to ensure that all employees, direct suppliers and service providers, wherever applicable, understand and follow the standard cyber hygiene practices that the entities apply pursuant to point 8.1.;

(b) mechanisms to ensure that all users with administrative or privileged access are aware of and follow their roles, responsibilities and authorities;

(c) mechanisms to ensure that management bodies understand their role, responsibilities and authorities regarding network and information system security;

(d) mechanisms for hiring qualified personnel, such as reference checks, vetting procedures, validation of professional certifications, or written tests.

Commented [A14]: [Suggestion to modify text]
Need to include "professional" for certifications for the reasons stated above.

10.1.3. The relevant entities shall review the assignment of personnel to specific roles as referred to in point 1.2., as well as their commitment of resources, at planned intervals and at least annually. They shall update the assignment where necessary.

10.2. Background checks

10.2.1. The relevant entities shall perform background checks for their employees, direct suppliers and service providers, if required for their role, responsibilities and authorisations.

10.2.2. For the purpose of point 10.2.1., the relevant entities shall:

(a) put in place criteria, which set out which roles, responsibilities and authorities shall only be exercised by persons who have undergone background checks;

(b) perform background verification checks on these persons before they start exercising these roles, responsibilities and authorities, which shall take into consideration the applicable laws, regulations, and ethics in proportion to the business requirements, the classification of the information and the network and information systems to be accessed, and the perceived risks.

10.2.3. The relevant entities shall review and, where appropriate, update the policy at planned intervals and update it where necessary.

10.3. Termination or change of employment procedures

10.3.1. The relevant entities shall ensure that network and information system security responsibilities and duties that remain valid after termination or change of employment of their employees are set out, enforced, communicated and understood.

10.3.2. For the purpose of point 10.3.1., the relevant entities shall:

(a) include in the individual's terms and conditions of employment, contract or agreement the responsibilities and duties that are still valid after termination of employment or contract, such as confidentiality clauses;

(b) put in place access control policies which ensure that access rights are modified accordingly upon the individual's termination or change of employment;

(c) ensure that, after a change of employment, the employee can perform the new tasks.

10.4. Disciplinary process

10.4.1. The relevant entities shall establish, communicate and maintain a disciplinary process for handling violations of network and information system security policies. The process shall take into consideration relevant legal, statutory, contractual and business requirements.

10.4.2. The relevant entities shall review and, where appropriate, update the disciplinary process at planned intervals, and when necessary due to legal changes or significant changes to operations or risks.

11. ACCESS CONTROL (ARTICLE 21(2), POINT (I), OF DIRECTIVE (EU) 2022/2555)

11.1. Access control policy

11.1.1. For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall establish, document and implement logical and physical access control policies for the access of persons and processes on network and information systems, based on business requirements as well as network and information system security requirements.

11.1.2. The policies referred to in point 11.1.1. shall:

(a) address access by persons, including staff, visitors, and external entities such as suppliers and service providers;

(b) address access by network and information system processes;

(c) ensure that access is only granted to users that have been adequately authenticated.

11.1.3. The relevant entities shall review and, where appropriate, update the policies at planned intervals and when significant incidents or significant changes to operations or risks occur.

11.2. Management of access rights

11.2.1. The relevant entities shall provide, modify, remove and document access rights to network and information systems in accordance with the access control policy referred to in point 11.1.

11.2.2. The relevant entities shall:

(a) assign and revoke access rights based on the principles of need-to-know, least privilege and separation of duties;

(b) ensure that access rights are modified accordingly upon termination or change of employment;

(c) ensure that access to network and information systems is authorised by their owner;

(d) ensure that access rights appropriately address third-party access, such as suppliers and service providers, in particular by limiting access rights in scope and in duration;

(e) maintain a register of access rights granted;

(f) apply logging to the management of access rights.

11.2.3. The relevant entities shall review access rights at planned intervals and shall modify them based on organisational changes. The relevant entities shall document the results of the review including the necessary changes of access rights.

11.3. Privileged accounts and system administration accounts

11.3.1. The relevant entities shall maintain policies for management of privileged accounts and system administration accounts.

11.3.2. The policies referred to in point 11.3.1. shall:

(a) establish strong identification, authentication such as multi-factor authentication, and authorisation procedures for privileged accounts and system administration accounts;

(b) set up specific accounts to be used for system administration operations exclusively, such as installation, configuration, management or maintenance;

(c) individualise and restrict system administration privileges to the highest extent possible,

(d) provide that system administration accounts are only used to connect to system administration systems.

11.3.3. The relevant entities shall review access rights of privileged accounts and system administration accounts at planned intervals and be modified based on organisational changes, and shall document the results of the review, including the necessary changes of access rights.

11.4. Administration systems

11.4.1. The relevant entities shall restrict and control the use of system administration systems.

11.4.2. For that purpose, the relevant entities shall:

(a) only use system administration systems for system administration purposes, and not for any other operations;

(b) separate logically such systems from application software not used for system administrative purposes,

(c) protect access to system administration systems through authentication and encryption.

11.5. Identification

11.5.1. The relevant entities shall manage the full life cycle of identities of network and information systems and their users.

11.5.2. For that purpose, the relevant entities shall:

(a) set up unique identities for network and information systems and their users;

(b) link the identity of users to a single person;

(c) ensure oversight of identities of network and information systems; (d) apply logging to the management of identities.

11.5.3. The relevant entities shall only permit identities assigned to multiple persons, such as shared identities, where they are necessary for business or operational reasons and are subject to an explicit approval process and documentation.

11.6. Authentication

11.6.1. The relevant entities shall implement secure authentication procedures and technologies based on access restrictions and the policy on access control.

11.6.2. For that purpose, the relevant entities shall:

(a) ensure the strength of authentication is appropriate to the classification of the asset to be accessed;

Commented [A15]: [General Comment]
Some of the below requirements are not available in the latest cloud-based Microsoft Entra ID (ex-Azure-AD) so it will be very difficult for the entities if these become mandatory.

Also, the separate credentials requirement should be worded to cover Amazon (AWS) way of providing admin-roles to be possible to implement.

(b) control the allocation to users and management of secret authentication information by a process that ensures the confidentiality of the information, including advising personnel on appropriate handling of authentication information;

(c) require the change of authentication credentials initially, and when suspicion that the credential is revealed to an unauthorised person;

(d) require the reset of authentication credentials and the blocking of users after a predefined number of unsuccessful log-in attempts;

(e) terminate inactive sessions after a predefined period of inactivity; and

(f) require separate credentials to access privileged access or administrative accounts.

11.6.3. The relevant entities shall use state-of-the-art authentication methods, in accordance with the associated assessed risk and the classification of the asset to be accessed, and unique authentication information.

11.6.4. The relevant entities shall regularly review the identities and, if no longer needed, deactivate them without delay.

11.7. Multi-factor authentication

11.7.1. The relevant entities shall ensure that users are authenticated by multiple authentication factors or continuous authentication mechanisms for accessing the entities' network and information systems, where appropriate, in accordance with the classification of the asset to be accessed.

11.7.2. The relevant entities shall ensure that the strength of authentication is appropriate for the classification of the asset to be accessed.

12. ASSET MANAGEMENT (ARTICLE 21(2), POINT (I), OF DIRECTIVE (EU) 2022/2555)

12.1. Asset classification

12.1.1. For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall lay down classification levels of all information and assets in scope of their network and information systems for the level of protection required.

12.1.2. For the purpose of point 12.1.1., the relevant entities shall:

(a) lay down a system of classification levels for information and assets;

(b) associate all information and assets with a classification level, based on confidentiality, integrity, authenticity and availability requirements, to indicate the protection required according to their sensitivity, criticality, risk and business value,

(c) align the availability requirements of the information and assets with the delivery and recovery objectives set out in their business and disaster recovery plans.

12.1.3. The relevant entities shall conduct periodic reviews of the classification levels of information and assets and update them, where appropriate.

Commented [A16]: [General Comment]
Reset is not available, accounts can be locked for 1 minute.

12.2. Handling of information and assets

12.2.1. The relevant entities shall establish, implement and apply a policy for the proper handling of information and assets in accordance with their network and information security policy, and shall communicate the policy to anyone who uses or handles information and assets.

12.2.2. The policy shall:

(a) cover the entire life cycle of the information and assets, including acquisition, use, storage, transportation and disposal;

(b) provide instructions on the safe use, safe storage, safe transport, and the irretrievable deletion and destruction of the information and assets;

(c) provide that equipment, hardware, software and data may be transferred to external premises only after approval by bodies authorised by management bodies in accordance with the policies,

(d) provide that the transfer shall take place in a secure manner, in accordance with the type of asset or information to be transferred.

12.2.3. The relevant entities shall review and, where appropriate, update the policy at planned intervals and when significant incidents or significant changes to operations or risks occur.

12.3. Removable media policy

12.3.1. The relevant entities shall establish, implement and apply a policy on the management of removable storage media and communicate it to their employees and third parties who handle removable storage media at the relevant entities' premises or other locations where the removable media is connected to the relevant entities' network and information systems.

12.3.2. The policy shall:

(a) provide for a technical prohibition of the connection of removable media unless there is an organisational reason for their use;

(b) provide for disabling self-execution from such media and scanning the media for malicious code before they are used on the entities' systems;

(c) provide measures for controlling and protecting portable storage devices containing data while in transit and in storage;

(d) where appropriate, provide measures for the use of cryptographic techniques to protect information on removable storage media.

12.3.3. The relevant entities shall review and, where appropriate, update the policy at planned intervals and when significant incidents or significant changes to operations or risks occur.

12.4. Asset inventory

12.4.1. The relevant entities shall develop and maintain a complete, accurate, up-to-date and consistent inventory of their assets. They shall record changes to the entries in the inventory in a traceable manner.

12.4.2. The granularity of the inventory of the assets shall be at a level appropriate for the needs of the relevant entities. The inventory shall include the following:

(a) the list of operations and services and their description,

(b) the list of network and information systems and other associated assets supporting the entities' operations and services.

12.4.3. The relevant entities shall regularly review and update the inventory and their assets and document the history of changes.

12.5. Return or deletion of assets upon termination of employment

The relevant entities shall establish, implement and apply procedures which ensure that their assets which are under custody of personnel are returned upon termination of employment, and shall document the deposit and return of those assets.

13. Environmental and physical security (Article 21(2), points (c), (e) and (i) of Directive (EU) 2022/2555)

13.1. Supporting utilities

13.1.1. For the purpose of Article 21(2)(c) of Directive (EU) 2022/2555, the relevant entities shall prevent loss, damage or compromise of network and information systems or interruption to their operations due to the failure and disruption of supporting utilities.

13.1.2. For that purpose, the relevant entities shall:

(a) protect facilities from power failures and other disruptions caused by failures in supporting utilities such as electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning;

(b) where appropriate, consider the use of redundancy in utilities services;

(c) protect utility services for electricity and telecommunications, which transport data or supply network and information systems, against interception and damage;

(d) monitor the utility services referred to in point (c) and report to the competent internal or external personnel events outside the permissible control range referred to in point 13.2.2(b) affecting the utility services;

(e) where appropriate, conclude contracts for the emergency supply with corresponding services, such as for the fuel for emergency power supply;

(f) ensure continuous effectiveness, monitor, maintain and test the supply of the network and information systems necessary for the operation of the service offered, in particular the electricity, temperature and humidity control, telecommunications and Internet connection.

For the purpose of point (d), the relevant entities shall document, communicate and make available policies and instructions which describe the maintenance, in particular the remote maintenance, deletion, updating and reuse of assets that process information, including those in outsourced premises or by external personnel. The entities shall equip assets that process information with automatic fail-safes and other redundancies.

13.1.3. The relevant entities shall test, review and, where appropriate, update the protection measures on a regular basis or following significant incidents or significant changes to operations or risks.

13.2. Protection against physical and environmental threats

13.2.1. For the purpose of Article 21(2)(e) of Directive (EU) 2022/2555, the relevant entities shall prevent or reduce the consequences of events originating from physical and environmental threats, such as natural disasters and other intentional or unintentional threats.

13.2.2. For that purpose, the relevant entities shall:

(a) based on the results of the risk assessment, design and implement protection measures against physical and environmental threats;

(b) determine minimum and maximum control thresholds for physical and environmental threats;

(c) monitor environmental parameters and report events outside the minimum and maximum control thresholds referred to in point (b).

13.2.3. The relevant entities shall test, review and, where appropriate, update the protection measures against physical and environmental threats on a regular basis or following significant incidents or significant changes to operations or risks.

13.3. Perimeter and physical access control

13.3.1. For the purpose of Article 21(2)(i) of Directive (EU) 2022/2555, the relevant entities shall prevent and monitor unauthorised physical access, damage and interference to their network and information systems.

13.3.2. For that purpose, the relevant entities shall:

(a) on the basis of the risk assessment, lay down and use security perimeters to protect areas where network and information systems and other associated assets are located;

(b) protect the areas referred to in point (a) by appropriate entry controls and access points;

(c) design and implement physical security for offices, rooms and facilities, (d) continuously monitor their premises for unauthorised physical access.

13.3.3. The relevant entities shall test, review and, where appropriate, update the physical access control measures on a regular basis or following significant incidents or significant changes to operations or risks.