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)

NIS 2

Published 14 Dec 2022; Supersedes NIS 1

General Purpose: Lay down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.

More Specifically, lay down:

- Obligations that require Member States to adopt national cybersecurity strategies and to designate or establish
  - Competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);
  - Cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities;
  - Rules and obligations on cybersecurity information sharing;
  - Supervisory and enforcement obligations on Member States

NIS 2 Scope

- Applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union
- Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where:
  - (a) services are provided by:
    - (i) providers of public electronic communications networks or of publicly available electronic communications services;
    - (ii) trust service providers;
    - (iii) top-level domain name registries and domain name system service providers;
  - (b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;
  - (c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;
  - (d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;
  - (e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;

NIS 2 Scope

- Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where:
  - (f) the entity is a public administration entity:
    - (i) of central government as defined by a Member State in accordance with national law; or
    - (ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities
- Regardless of their size, this Directive applies to entities identified as critical entities
- Regardless of their size, this Directive applies to entities providing domain name registration services
- Member States may provide for this Directive to apply to:
  - Public administration entities at local level;
  - Education institutions, in particular where they carry out critical research activities
- Does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences
- Does not apply to entities which Member States have exempted from the scope of Regulation

NIS 2
Essential and Important Entities

Essential Entities

- Entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in the Annex;
- Qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;
- Providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises in the Annex;
- Public administration entities;
- Any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities;
- Entities identified as critical entities referred to in this Directive;
- If the Member State so provides, entities which that Member State identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148 or national law

NIS 2
Key Definitions of Interest

- ‘security of network and information systems’: The ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems
- ‘national cybersecurity strategy ’: A coherent framework of a Member State providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them in that Member State
- ‘incident’: An event compromising 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
- ‘large-scale cybersecurity incident’: An incident which causes a level of disruption that exceeds a Member State’s capacity to respond to it or which has a significant impact on at least two Member States
- ‘risk’: The potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident
- ‘vulnerability’: A weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat

NIS 2
Key Definitions of Interest

- ‘entity’: A natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations
- ‘managed service provider’: An entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers’ premises or remotely
- ‘managed security service provider’: A managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management
- ‘social networking services platform’: A platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations
- ‘significant cyber threat’: A cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity’s services by causing considerable material or non-material damage
- ‘near miss’: An event that could have compromised 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, but that was successfully prevented from materialising or that did not materialise

NIS 2
National Cybersecurity Strategy

Each Member State is to adopt a national cybersecurity strategy that is to include:

- Objectives and priorities of the Member State's cybersecurity strategy covering in particular the sectors referred to in Annexes I and II;
- A governance framework to achieve the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in paragraph 2;
- A governance framework clarifying the roles and responsibilities of relevant stakeholders at national level;
- A mechanism to identify relevant assets and an assessment of the risks in that Member State;
- An identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors;
- A list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy;
- A policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate
- A plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens

NIS 2
National Cybersecurity Strategy

As part of the national cybersecurity strategy, Member States are to in particular adopt policies:

- Addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;
- On the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;
- Managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under this Dirctive;
- Related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables;
- Promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;
- Promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities;

NIS 2
National Cybersecurity Strategy

As part of the national cybersecurity strategy, Member States are to in particular adopt policies:

- Supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure;
- Including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law;
- Strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs;
- Promoting active cyber protection

Member States are to notify their national cybersecurity strategies to the Commission within three months of their adoption

Member States are to assess their national cybersecurity strategies on a regular basis and at least every five years on the basis of key performance indicators and, where necessary, update them

NIS 2
Competent Authorities / Single Points of Contact

- Each Member State is to designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VII (competent authorities)
- The competent authorities referred to above are to monitor the implementation of this Directive at national level
- Each Member State is to designate or establish a single point of contact. Where a Member State designates or establishes only one competent authority pursuant to paragraph 1, that competent authority is to also be the single point of contact for that Member State
- Each single point of contact is to exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities of other Member States, and, where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within its Member State
- Member States are to ensure that their competent authorities and single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive

NIS 2
National Cyber Management Frameworks

- Each Member State is to designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States are to ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States are to ensure coherence with the existing frameworks for general national crisis management
- Where a Member State designates or establishes more than one cyber crisis management authority, it is to clearly indicate which of those authorities is to serve as the coordinator for the management of largescale cybersecurity incidents and crises
- Each Member State is to identify capabilities, assets and procedures that can be deployed in the case of a crisis for the purposes of this Directive

NIS 2
National Cyber Management Frameworks

Each Member State is to adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan is to lay down, in particular:

- The objectives of national preparedness measures and activities;
- The tasks and responsibilities of the cyber crisis management authorities;
- The cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels;
- National preparedness measures, including exercises and training activities;
- The relevant public and private stakeholders and infrastructure involved;
- National procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level

NIS 2
Computer Security Incident Response Teams (CSIRTs)

- Each Member State is to designate or establish one or more CSIRTs.
- The CSIRTs are to comply with the requirements set out in Slide 16 and are to cover at least the sectors, subsectors and types of entity referred to in Slides 37-39, and are responsible for incident handling in accordance with a well-defined process.
- Member States are to ensure that each CSIRT has adequate resources to carry out effectively its tasks as set out in Slide 17
- Member States are to ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders
- The CSIRTs are cooperate and, where appropriate, exchange relevant information with sectoral or cross-sectoral communities of essential and important entities
- The CSIRTs are to participate in peer reviews
- Member States are to ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network
- The CSIRTs may establish cooperation relationships with third countries' national computer security incident response teams

NIS 2
Computer Security Incident Response Teams (CSIRTs)

- Member States are to facilitate effective, efficient and secure information exchange with those third countries' national computer security incident response teams, using relevant information-sharing protocols, including the traffic light protocol. The CSIRTs may exchange relevant information with third countries' national computer security incident response teams, including personal data in accordance with Union data protection law
- The CSIRTs may cooperate with third countries' national computer security incident response teams or equivalent third-country bodies, in particular for the purpose of providing them with cybersecurity assistance
- Each Member State is to notify the Commission without undue delay of the identity of the CSIRT and the CSIRT designated as coordinator, of their respective tasks in relation to essential and important entities, and of any subsequent changes thereto
- Member States may request the assistance of ENISA in developing their CSIRT

NIS 2
Computer Security Incident Response Teams (CSIRTs)

CSIRTs are to comply with the following requirements:

- The CSIRTs are to ensure a high level of availability of their communication channels by avoiding single points of failure, and are to have several means for being contacted and for contacting others at all times; they are to clearly specify the communication channels and make them known to constituency and cooperative partners;
- The CSIRTs' premises and the supporting information systems are to be located at secure sites;
- The CSIRTs are to be equipped with an appropriate system for managing and routing requests, in particular to facilitate effective and efficient handovers;
- The CSIRTs are to ensure the confidentiality and trustworthiness of their operations;
- The CSIRTs are to be adequately staffed to ensure availability of their services at all times and they are to ensure that their staff is trained appropriately;
- The CSIRTs are to be equipped with redundant systems and backup working space to ensure continuity of their services

NIS 2
Computer Security Incident Response Teams (CSIRTs)

CSIRTs are to have the following tasks:

- Monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;
- Providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;
- Responding to incidents and providing assistance to the essential and important entities concerned, where applicable;
- Collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;
- Providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;
- Participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;
- Where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure;
- Contributing to the deployment of secure information-sharing tools

NIS 2
Coordinated Vulnerability Disclosure

Each Member State is to designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. The CSIRT designated as coordinator is to act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party

The tasks of the CSIRT designated as coordinator are to include:

- Identifying and contacting the entities concerned;
- Assisting the natural or legal persons reporting a vulnerability; and
- Negotiating disclosure timelines and managing vulnerabilities that affect multiple entities

ENISA is to develop and maintain, after consulting the Cooperation Group, a European vulnerability database. The database are to include:

- Information describing the vulnerability;
- The affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited;
- The availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable ICT products and ICT services as to how the risks resulting from disclosed vulnerabilities can be mitigated

NIS 2
Cooperation at the National Level

- Where they are separate, the competent authorities, the single point of contact and the CSIRTs of the same Member State is to cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive
- Member States are to ensure that their CSIRTs or, where applicable, their competent authorities, receive notifications of significant incidents and incidents, cyber threats and near misses
- Member States are to ensure that their CSIRTs or, where applicable, their competent authorities inform their single points of contact of notifications of incidents, cyber threats and near misses submitted pursuant to this Directive
- To ensure that the tasks and obligations of the competent authorities, the single points of contact and the CSIRTs are carried out effectively, Member States are to, to the extent possible, ensure appropriate cooperation between those bodies and law enforcement authorities, data protection, the national regulatory authorities, the competent authorities, as well as the competent authorities under other sector-specific Union legal acts, within that Member State
- Member States are to ensure that their competent authorities under this Directive and their competent authorities cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents affecting entities identified as critical entities, and the measures taken in response to such risks, threats and incidents. Member States are to also ensure that appropriate competent authorities exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats
- Member States are to simplify the reporting through technical means for notifications

NIS 2
Coordination Group

In order to support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence, a Cooperation Group is established

- The Cooperation Group is to carry out its tasks on the basis of biennial work programmes
- The Cooperation Group is to be composed of representatives of Member States, the Commission and ENISA. The European External Action Service is to participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) and the competent authorities may participate in the activities of the Cooperation Group
- The Cooperation Group is to have the following tasks:
  - To provide guidance to the competent authorities in relation to the transposition and implementation of this Directive;
  - To provide guidance to the competent authorities in relation to the development and implementation of policies on coordinated vulnerability disclosure;
  - To exchange best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, training, exercises and skills, capacity building, standards and technical specifications as well as the identification of essential and important entities;
  - To exchange advice and cooperate with the Commission on emerging cybersecurity policy initiatives and the overall consistency of sector-specific cybersecurity requirements;
  - To exchange advice and cooperate with the Commission on draft delegated or implementing acts adopted pursuant to this Directive;
  - To exchange best practices and information with relevant Union institutions, bodies, offices and agencies;

NIS 2
Coordination Group

- The Cooperation Group is to have the following tasks:
  - To exchange views on the implementation of sector-specific Union legal acts that contain provisions on cybersecurity;
  - Where relevant, to discuss reports on the peer review referred to in Article 19(9) and draw up conclusions and recommendations;
  - To carry out coordinated security risk assessments of critical supply chains;
  - To discuss cases of mutual assistance, including experiences and results from cross-border joint supervisory actions;
  - Upon the request of one or more Member States concerned, to discuss specific requests for mutual assistance;
  - To provide strategic guidance to the CSIRTs network and EU-CyCLONe on specific emerging issues;
  - To exchange views on the policy on follow-up actions following large-scale cybersecurity incidents and crises on the basis of lessons learned of the CSIRTs network and EU-CyCLONe;
  - To contribute to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the competent authorities or the CSIRTs;
  - To organise regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Cooperation Group and gather input on emerging policy challenges;

NIS 2
Coordination Group

- The Cooperation Group is to have the following tasks:
  - To discuss the work undertaken in relation to cybersecurity exercises, including the work done by ENISA;
  - To establish the methodology and organisational aspects of the peer reviews, as well as to lay down the self-assessment methodology for Member States, with the assistance of the Commission and ENISA, and, in cooperation with the Commission and ENISA, to develop codes of conduct underpinning the working methods of designated cybersecurity experts;
  - To prepare reports for the purpose of the review referred to in this Directive on the experience gained at a strategic level and from peer reviews;
  - To discuss and carry out on a regular basis an assessment of the state of play of cyber threats or incidents, such as ransomware

NIS 2
CSIRTs Network

In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of national CSIRTs is established

The CSIRTs network is to be composed of representatives of the CSIRTs designated or established and the computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU). The Commission is to participate in the CSIRTs network as an observer. ENISA is to provide the secretariat and are to actively provide assistance for the cooperation among the CSIRTs.

The CSIRTs network are to have the following tasks:

- To exchange information about the CSIRTs' capabilities;
- To facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs;
- To exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities;
- To exchange information with regard to cybersecurity publications and recommendations;
- To ensure interoperability with regard to information-sharing specifications and protocols;
- At the request of a member of the CSIRTs network potentially affected by an incident, to exchange and discuss information in relation to that incident and associated cyber threats, risks and vulnerabilities;
- At the request of a member of the CSIRTs network, to discuss and, where possible, implement a coordinated response to an incident that has been identified within the jurisdiction of that Member State;

NIS 2
CSIRTs Network

The CSIRTs network is to have the following tasks:

- To provide Member States with assistance in addressing cross-border incidents pursuant to this Directive;
- To cooperate, exchange best practices and provide assistance to the CSIRTs designated as coordinators with regard to the management of the coordinated disclosure of vulnerabilities which could have a significant impact on entities in more than one Member State;
- To discuss and identify further forms of operational cooperation, including in relation to:
  - Categories of cyber threats and incidents;
  - Early warnings;
  - Mutual assistance;
  - Principles and arrangements for coordination in response to cross-border risks and incidents;
  - Contribution to the national large-scale cybersecurity incident and crisis response plan at the request of a Member State;
- To inform the Cooperation Group of its activities and of the further forms of operational cooperation discussed, and, where necessary, request guidance in that regard;
- To take stock of cybersecurity exercises, including those organised by ENISA;
- At the request of an individual CSIRT, to discuss the capabilities and preparedness of that CSIRT;

NIS 2
CSIRTs Network

The CSIRTs network is to have the following tasks:

- To cooperate and exchange information with regional and Union-level Security Operations Centres (SOCs) to improve common situational awareness on incidents and cyber threats across the Union;
- Where relevant, to discuss the peer-review reports referred to in this Directive;
- To provide guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation

NIS 2
European Cyber Crisis Liaison Organisation Network (EU-CyCLONe)

EU-CyCLONe is established to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies.

EU-CyCLONe is to be composed of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of this Directive, the Commission. In other cases, the Commission is to participate in the activities of EU-CyCLONe as an observer.

Where appropriate, EU-CyCLONe may invite representatives of relevant stakeholders to participate in its work as observers.

EU-CyCLONe is to have the following tasks:

- To increase the level of preparedness of the management of large-scale cybersecurity incidents and crises;
- To develop a shared situational awareness for large-scale cybersecurity incidents and crises;
- To assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;
- To coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;
- To discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans

NIS 2
International Cooperation

The Union may, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements are to comply with Union data protection law

NIS 2
Peer Review

The Cooperation Group is to establish, with the assistance of the Commission and ENISA, and, where relevant, the CSIRTs network, the methodology and organisational aspects of peer reviews. Participation in peer reviews is voluntary. The peer reviews are to be carried out by cybersecurity experts. The cybersecurity experts are to be designated by at least two Member States, different from the Member State being reviewed

The peer reviews are to cover at least one of the following:

- The level of implementation of the cybersecurity risk-management measures and reporting obligations laid down in this Directive
- The level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the competent authorities;
- The operational capabilities of the CSIRTs;
- The level of implementation of mutual assistance;
- The level of implementation of the cybersecurity information-sharing arrangements;
- Specific issues of cross-border or cross-sector nature

NIS 2
Peer Review

Other Peer Review Requirements:

- The methodology used is to include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States designate cybersecurity experts eligible to carry out the peer reviews. The Commission and ENISA is to participate as observers in the peer reviews
- Member States may identify specific issues for the purposes of a peer review.
- Before commencing a peer review Member States are to notify the participating Member States of its scope, including the specific issues identified
- Prior to the commencement of the peer review, Member States may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated cybersecurity experts
- Peer reviews are to entail physical or virtual on-site visits and off-site exchanges of information. The Member State subject to the peer review is to provide the designated cybersecurity experts with the information necessary for the assessment, without prejudice to Union or national law concerning the protection of confidential or classified information and to the safeguarding of essential State functions, such as national security
- The cybersecurity experts participating in the peer review are to not disclose any sensitive or confidential information obtained in the course of that peer review to any third parties

NIS 2
Peer Review

Other Peer Review Requirements:

- Once subject to a peer review, the same aspects reviewed in a Member State are to not be subject to a further peer review in that Member State for two years following the conclusion of the peer review, unless otherwise requested by the Member State or agreed upon after a proposal of the Cooperation Group
- Member States are to ensure that any risk of conflict of interest concerning the designated cybersecurity experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review
- Cybersecurity experts participating in peer reviews are to draft reports on the findings and conclusions of the peer reviews. Member States subject to a peer review may provide comments on the draft reports concerning them and such comments are to be attached to the reports. The reports are to include recommendations to enable improvement on the aspects covered by the peer review. The reports are to be submitted to the Cooperation Group and the CSIRTs network where relevant. A Member State subject to the peer review may decide to make its report, or a redacted version of it, publicly available.

NIS 2
Cybersecurity Risk-Management Measures

Member States are to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services

The 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 incidents, and are to include at least the following:

- Policies on risk analysis and information system security;
- Incident handling;
- Business continuity, such as backup management and disaster recovery, and crisis management;
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

NIS 2
Cybersecurity Risk-Management Measures

The 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 incidents, and are to include at least the following:

- Basic cyber hygiene practices and cybersecurity training;
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- Human resources security, access control policies and asset management;
- The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors

NIS 2
Use of EU Cybersecurity Certification Schemes

To demonstrate compliance with Cybersecurity Risk Management Measure requirements, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes

The Commission is empowered to adopt delegated acts to supplement this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme. Those delegated acts are to be adopted where insufficient levels of cybersecurity have been identified and are to include an implementation period.

Before adopting such delegated acts, the Commission is to carry out an impact assessment and is to carry out consultations

Where no appropriate European cybersecurity certification scheme for the purposes of this Directive is available, the Commission may, after consulting the Cooperation Group and the European Cybersecurity Certification Group, request ENISA to prepare a candidate scheme

NIS 2
Cybersecurity Information-Sharing Arrangements

Member States are to ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

- Aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;
- Enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities

Member States are to ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers. Such exchange is to be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared

NIS 2
Cybersecurity Information-Sharing Arrangements

Member States are to facilitate the establishment of cybersecurity information-sharing arrangements referred to in this Directive. Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements

Member States are to ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect

ENISA is to provide assistance for the establishment of cybersecurity information-sharing arrangements by exchanging best practices and providing guidance

NIS 2
Voluntary Notification of Relevant Information

Member States are to ensure that, in addition to the required notification obligation, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by:

- Essential and important entities with regard to incidents, cyber threats and near misses;
- Entities other than those referred to above, regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses

Member States are to process the notifications in accordance with the procedure laid down in this Directive. Member States may prioritise the processing of mandatory notifications over voluntary notifications.

Where necessary, the CSIRTs and, where applicable, the competent authorities are to provide the single points of contact with the information about notifications received pursuant to this Article, while ensuring the confidentiality and appropriate protection of the information provided by the notifying entity

NIS 2
Sectors of High Criticality

Sector	Subsector
Energy	Electricity
	District Heating and Cooling
	Oil
	Gas
	Hydrogen
Transport	Air
	Rail
	Water
	Road
Banking	
Financial Markets	
Health	
Drinking Water	

NIS 2
Sectors of High Criticality

Sector	Subsector
Waste Water	
Digital Infrastructure	
ICT service management (business-to-business)	
Public Administration	
Space	

NIS 2
Other Critical Sectors

Sector	Subsector
Postal and Courier Services	
Waste Management	
Manufacture, production and distribution of chemicals	
Production, processing and distribution of food	
Manufacturing	(a) Manufacture of medical devices and *in vitro* diagnostic medical devices
	(b) Manufacture of computer, electronic and optical products
	(c) Manufacture of electrical equipment
	(d) Manufacture of machinery and equipment n.e.c.
	(e) Manufacture of motor vehicles, trailers and semi-trailers
	(f) Manufacture of other transport equipment
Digital Providers	
Research	