# NIS2

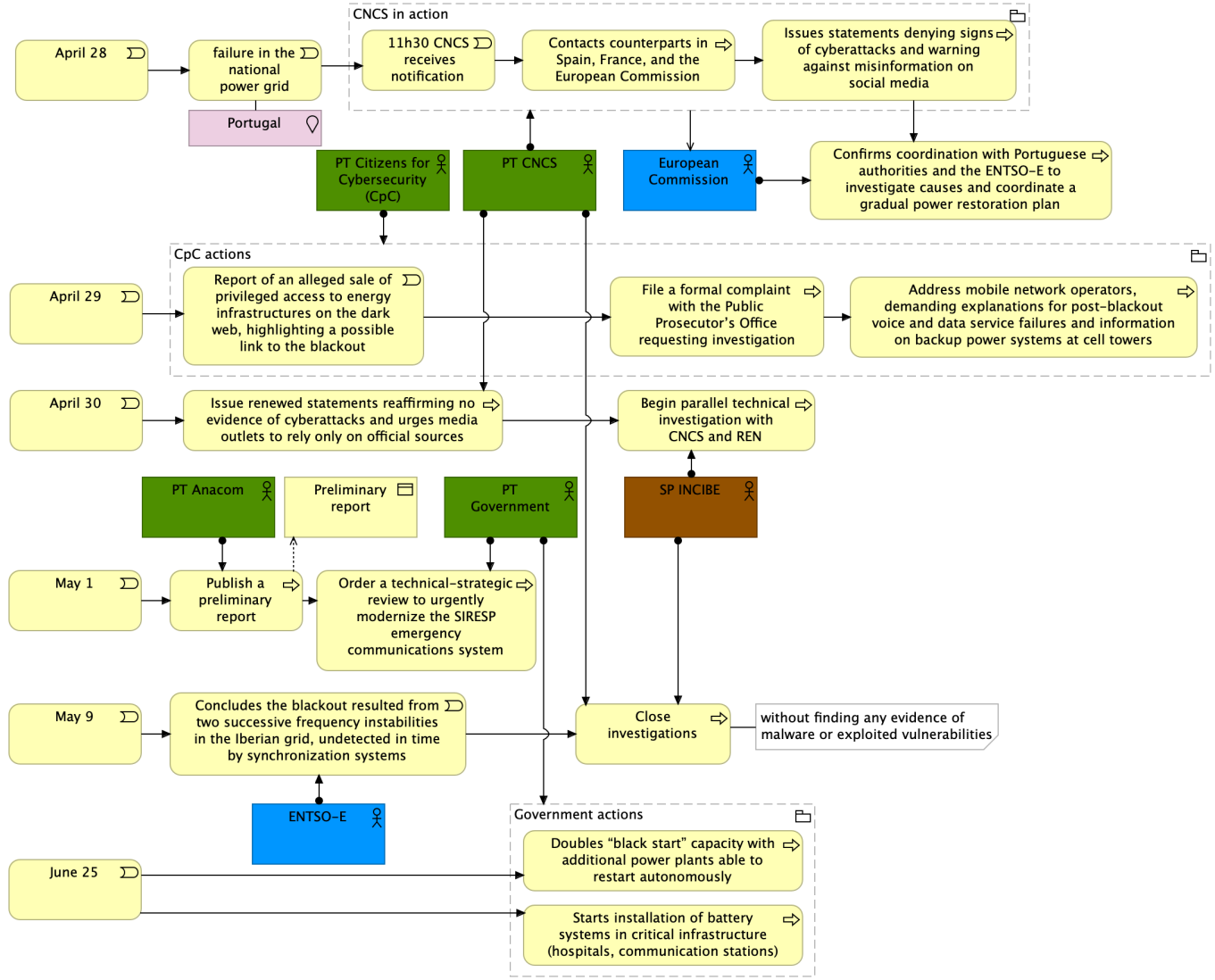
29 Sep 2025 14:43:26

# Purpose

# Views

## 2025 Blackout (PT)

*No viewpoint*



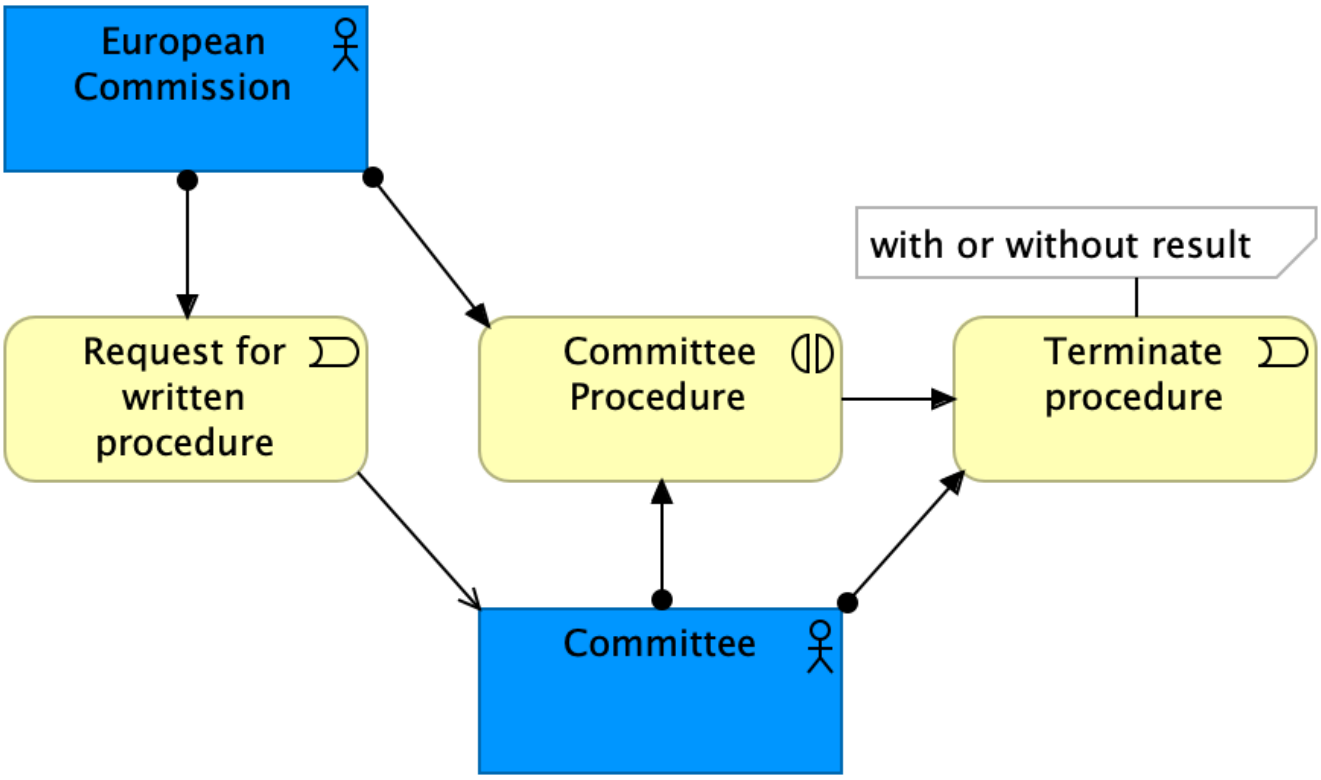

## Elements

| Element | Type |
|---|---|
| 11h30 CNCS  receives notification | Business Event |
| Address mobile network operators, demanding explanations for post-blackout voice and data service failures and information on backup power systems at cell towers | Business Process |
| April 28 | Business Event |
| April 29 | Business Event |
| April 30 | Business Event |
| Begin parallel technical investigation with CNCS and REN | Business Process |
| Close investigations | Business Process |
| CNCS in action | Grouping |

| Element | Type |
|---|---|
| Concludes the blackout resulted from two successive frequency instabilities in the Iberian grid, undetected in time by synchronization systems | Business Event |
| Confirms coordination with Portuguese authorities and the ENTSO-E to investigate causes and coordinate a gradual power restoration plan | Business Process |
| Contacts counterparts in Spain, France, and the European Commission | Business Process |
| CpC actions | Grouping |
| Doubles “black start” capacity with additional power plants able to restart autonomously | Business Process |
| ENTSO-E | Business Actor |
| European Commission | Business Actor |
| failure in the national power grid | Business Event |
| File a formal complaint with the Public Prosecutor’s Office requesting investigation | Business Process |
| Government actions | Grouping |
| Issue renewed statements reaffirming no evidence of cyberattacks and urges media outlets to rely only on official sources | Business Process |
| Issues statements denying signs of cyberattacks and warning against misinformation on social media | Business Process |
| June 25 | Business Event |
| May 1 | Business Event |
| May 9 | Business Event |
| Order a technical-strategic review to urgently modernize the SIRESP emergency communications system | Business Process |
| Portugal | Location |
| Preliminary report | Business Object |
| PT Anacom | Business Actor |
| PT Citizens for Cybersecurity (CpC) | Business Actor |
| PT CNCS | Business Actor |
| PT Government | Business Actor |
| Publish a preliminary report | Business Process |
| Report of an alleged sale of privileged access to energy infrastructures on the dark web, highlighting a possible link to the blackout | Business Event |
| SP INCIBE | Business Actor |
| Starts installation of battery systems in critical infrastructure (hospitals, communication stations) | Business Process |

# Committee procedure

*No viewpoint*




## Documentation

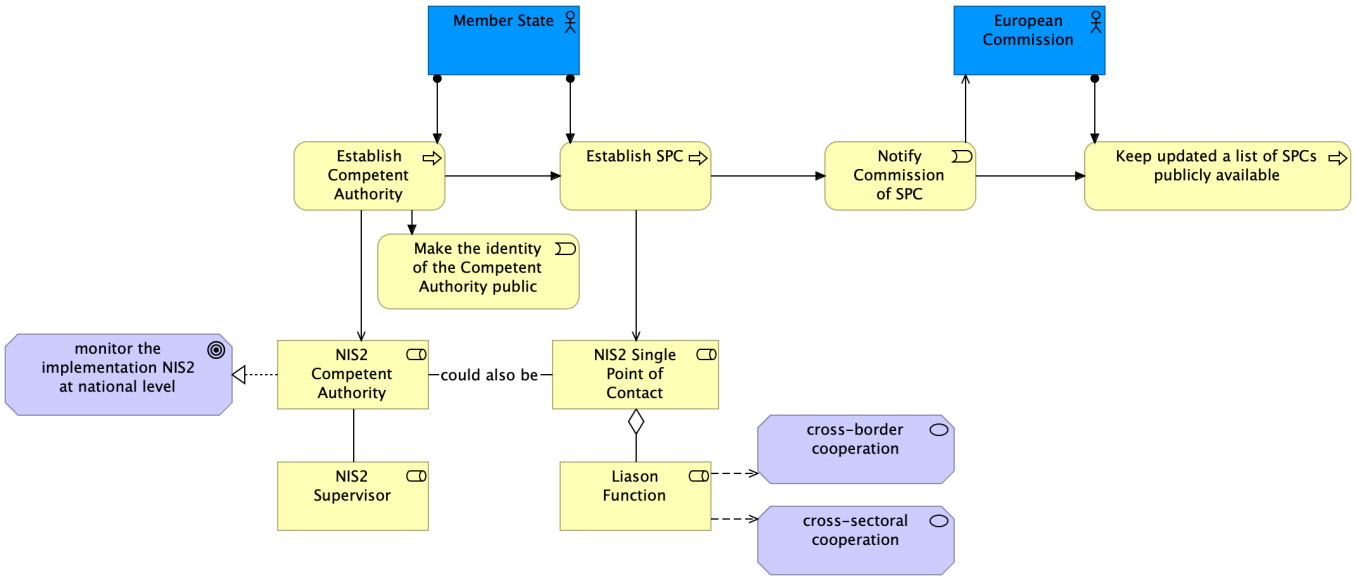
Numbering: 8.39

## Elements

| Element | Type |
|---|---|
| Committee | Business Actor |
| Committee Procedure | Business Interaction |
| European Commission | Business Actor |
| Request for written procedure | Business Event |
| Terminate procedure | Business Event |

# Competent authorities and Single points of contact

*No viewpoint*




## Documentation

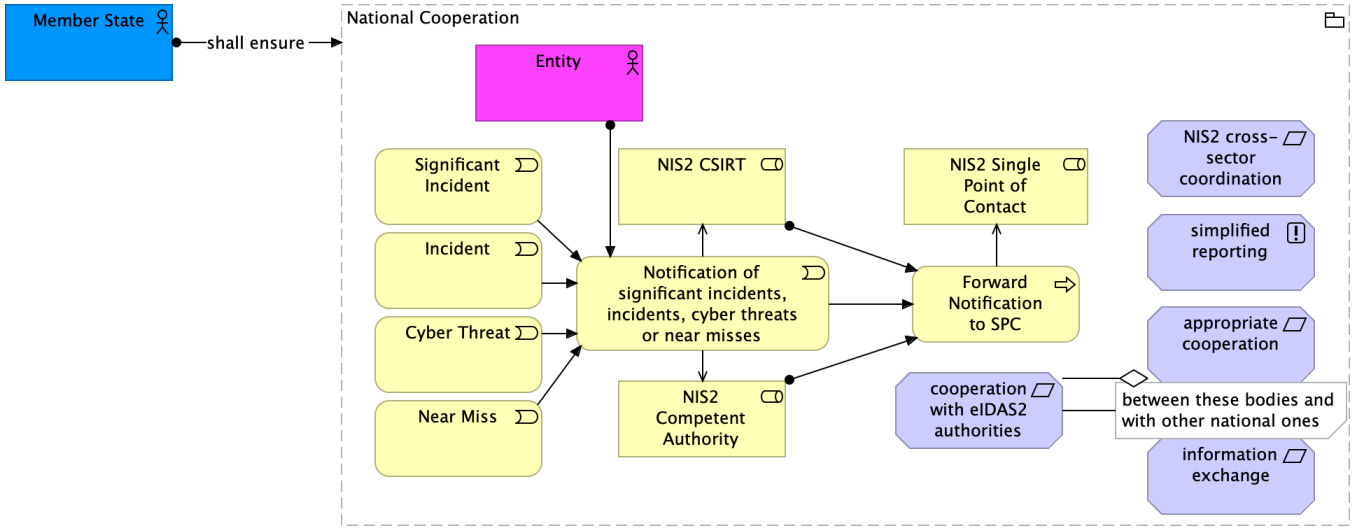
Numbering: 2.8

## Elements

| Element | Type |
|---|---|
| cross-border cooperation | Value |
| cross-sectoral cooperation | Value |
| Establish Competent Authority | Business Process |
| Establish SPC | Business Process |
| European Commission | Business Actor |
| Keep updated a list of SPCs publicly available | Business Process |
| Liason Function | Business Role |
| Make the identity of the Competent Authority public | Business Event |
| Member State | Business Actor |
| monitor the implementation NIS2 at national level | Goal |
| NIS2 Competent Authority | Business Role |
| NIS2 Single Point of Contact | Business Role |
| NIS2 Supervisor | Business Role |
| Notify Commission of SPC | Business Event |

# Cooperation at National Level

*No viewpoint*




## Documentation

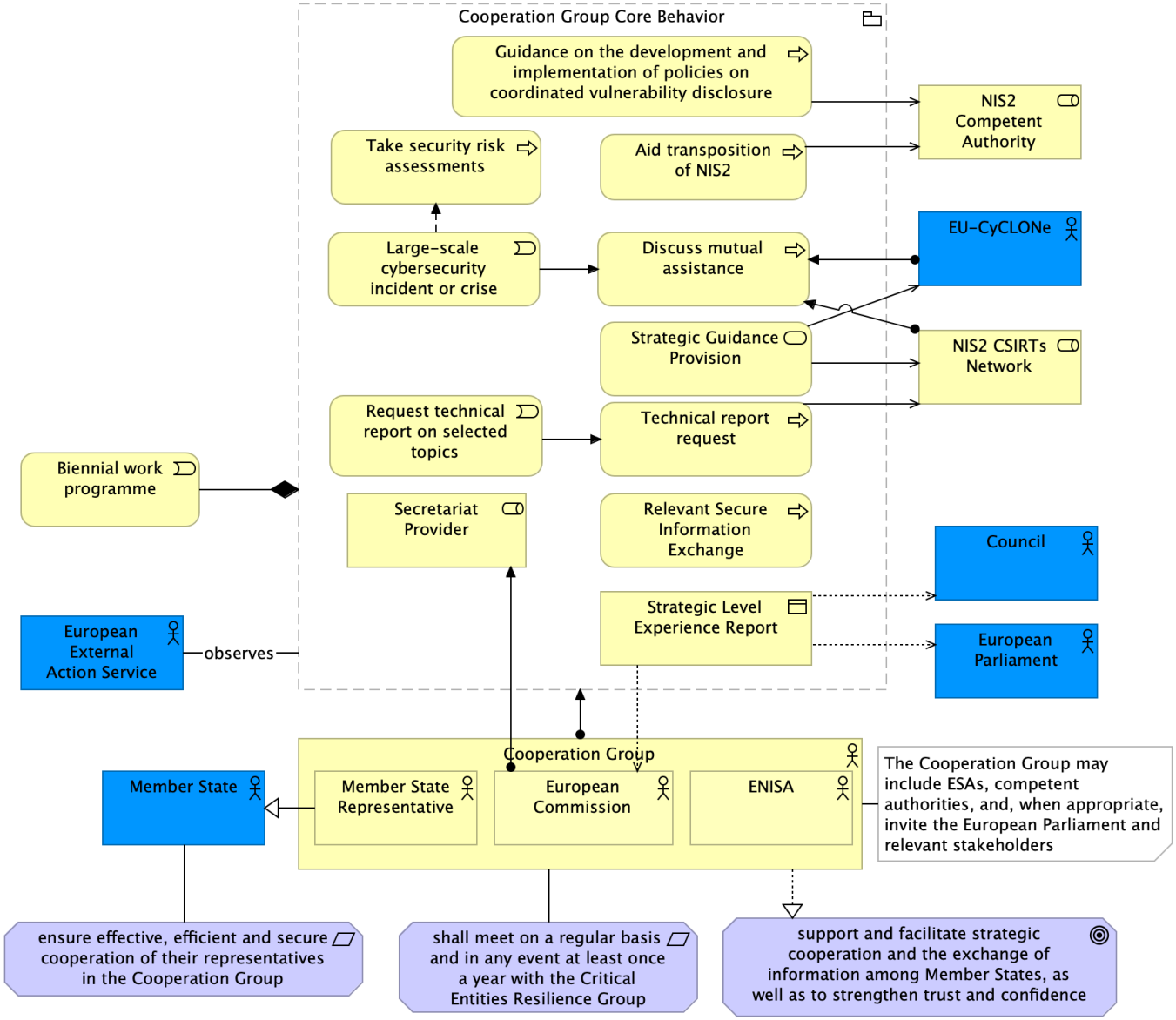
Numbering: 2.13

## Elements

| Element | Type |
|---|---|
| appropriate cooperation | Requirement |
| cooperation with eIDAS2 authorities | Requirement |
| Cyber Threat | Business Event |
| Entity | Business Actor |
| Forward Notification to SPC | Business Process |
| Incident | Business Event |
| information exchange | Requirement |
| Member State | Business Actor |
| National Cooperation | Grouping |
| Near Miss | Business Event |
| NIS2 Competent Authority | Business Role |
| NIS2 cross-sector coordination | Requirement |
| NIS2 CSIRT | Business Role |
| NIS2 Single Point of Contact | Business Role |
| Notification of significant incidents, incidents, cyber threats or near misses | Business Event |
| Significant Incident | Business Event |
| simplified reporting | Principle |

# Cooperation Group

*No viewpoint*




## Documentation

Numbering: 3.14

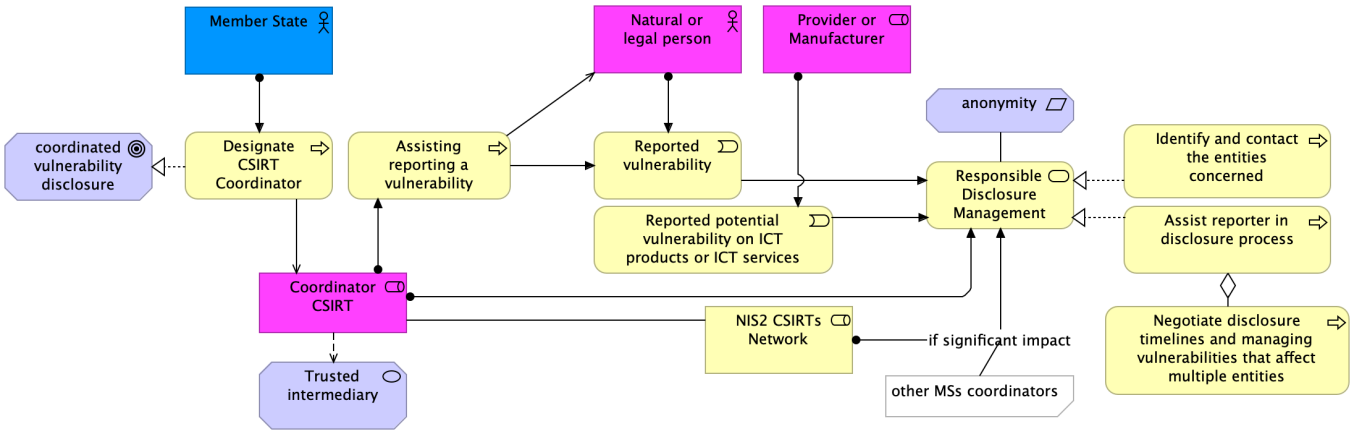
## Elements

| Element | Type |
|---|---|
| Aid transposition of NIS2 | Business Process |
| Biennial work programme | Business Event |
| Cooperation Group | Business Actor |
| Cooperation Group Core Behavior | Grouping |
| Council | Business Actor |
| Discuss mutual assistance | Business Process |
| ENISA | Business Actor |
| ensure effective, efficient and secure cooperation | Requirement |

| Element | Type |
|---|---|
| of their representatives in the Cooperation Group | |
| EU-CyCLONe | Business Actor |
| European Commission | Business Actor |
| European External Action Service | Business Actor |
| European Parliament | Business Actor |
| Guidance on the development and implementation of policies on coordinated vulnerability disclosure | Business Process |
| Large-scale cybersecurity incident or crise MS request | Business Event |
| Member State | Business Actor |
| Member State Representative | Business Actor |
| NIS2 Competent Authority | Business Role |
| NIS2 CSIRTs Network | Business Role |
| Relevant Secure Information Exchange | Business Process |
| Request technical report on selected topics | Business Event |
| Secretariat Provider | Business Role |
| shall meet on a regular basis and in any event at least once a year with the Critical Entities Resilience Group | Requirement |
| Strategic Guidance Provision | Business Service |
| Strategic Level Experience Report | Business Object |
| support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence | Goal |
| Take security risk assessments | Business Process |
| Technical report request | Business Process |

# Coordinated vulnerability disclosure

*No viewpoint*




## Documentation

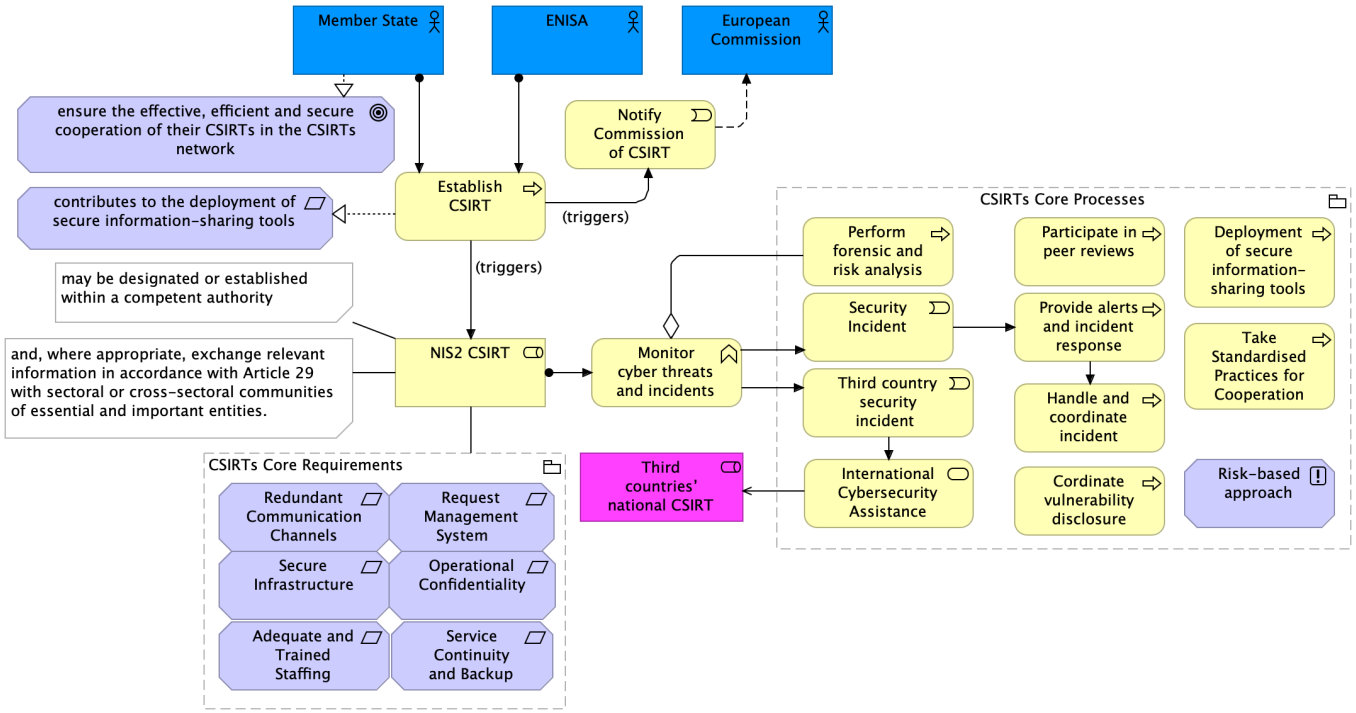
Numbering: 2.12

## Elements

| Element | Type |
|---|---|
| anonymity | Requirement |
| Assist reporter in disclosure process | Business Process |
| Assisting reporting a vulnerability | Business Process |
| coordinated vulnerability disclosure | Goal |
| Coordinator CSIRT | Business Role |
| Designate CSIRT Coordinator | Business Process |
| Identify and contact the entities concerned | Business Process |
| Member State | Business Actor |
| Natural or legal person | Business Actor |
| Negotiate disclosure timelines and managing vulnerabilities that affect multiple entities | Business Process |
| NIS2 CSIRTs Network | Business Role |
| Provider or Manufacturer | Business Role |
| Reported potential vulnerability on ICT products or ICT services | Business Event |
| Reported vulnerability | Business Event |
| Responsible Disclosure Management | Business Service |
| Trusted intermediary | Value |

# CSIRTs

*No viewpoint*




## Documentation

Numbering: 2.10, 2.11

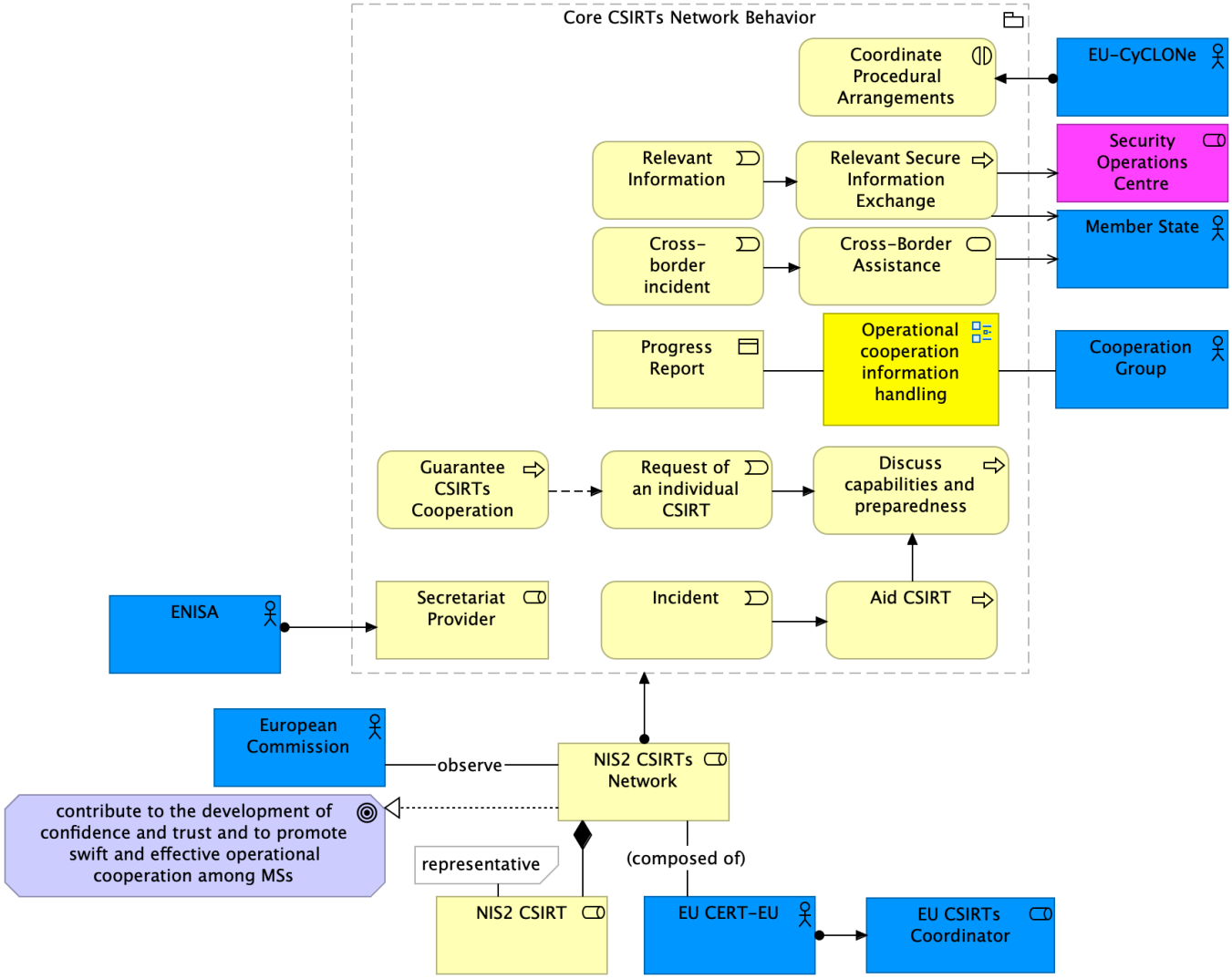
## Elements

| Element | Type |
|---|---|
| Adequate and Trained Staffing | Requirement |
| contributes to the deployment of secure information-sharing tools | Requirement |
| Cordinate vulnerability disclosure | Business Process |
| CSIRTs Core Processes | Grouping |
| CSIRTs Core Requirements | Grouping |
| Deployment of secure information-sharing tools | Business Process |
| ENISA | Business Actor |
| ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network | Goal |
| Establish CSIRT | Business Process |
| European Commission | Business Actor |
| Handle and coordinate incident | Business Process |
| International Cybersecurity Assistance | Business Service |
| Member State | Business Actor |
| Monitor cyber threats and incidents | Business Function |
| NIS2 CSIRT | Business Role |
| Notify Commission of CSIRT | Business Event |
| Operational Confidentiality | Requirement |
| Participate in peer reviews | Business Process |

| Element | Type |
|---|---|
| Perform forensic and risk analysis | Business Process |
| Provide alerts and incident response | Business Process |
| Redundant Communication Channels | Requirement |
| Request Management System | Requirement |
| Risk-based approach | Principle |
| Secure Infrastructure | Requirement |
| Security Incident | Business Event |
| Service Continuity and Backup | Requirement |
| Take Standardised Practices for Cooperation | Business Process |
| Third countries’ national CSIRT | Business Role |
| Third country security incident | Business Event |

# CSIRTs Network

*No viewpoint*




## Documentation

Numbering: 3.15

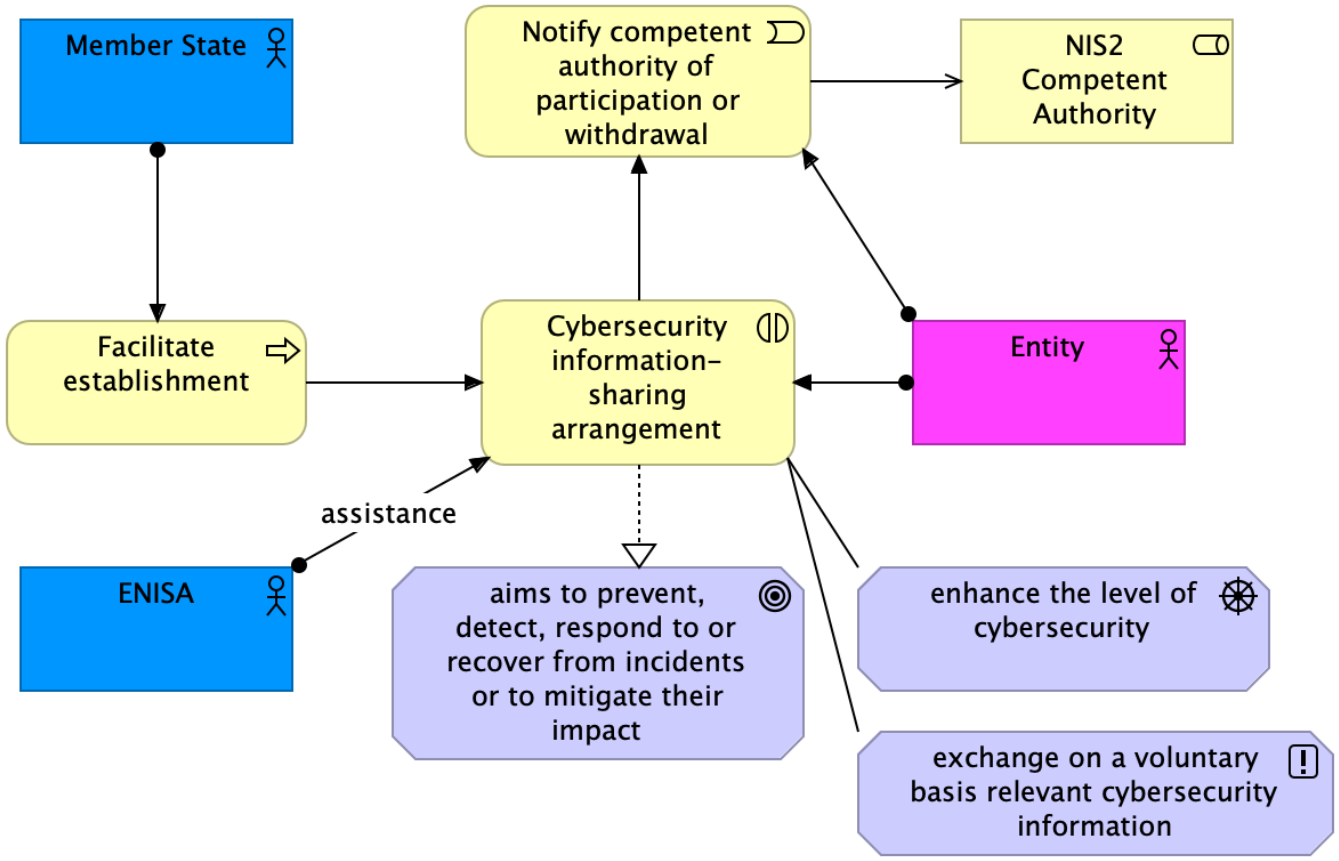
## Elements

| Element | Type |
|---|---|
| Aid CSIRT | Business Process |
| contribute to the development of confidence and trust and to promote swift and effective operational cooperation among MSs | Goal |
| Cooperation Group | Business Actor |
| Coordinate Procedural Arrangements | Business Interaction |
| Core CSIRTs Network Behavior | Grouping |
| Cross-Border Assistance | Business Service |
| Cross-border incident | Business Event |
| Discuss capabilities and preparedness | Business Process |
| ENISA | Business Actor |

| Element | Type |
|---|---|
| EU CERT-EU | Business Actor |
| EU CSIRTs Coordinator | Business Role |
| EU-CyCLONe | Business Actor |
| European Commission | Business Actor |
| Guarantee CSIRTs Cooperation | Business Process |
| Incident | Business Event |
| Member State | Business Actor |
| NIS2 CSIRT | Business Role |
| NIS2 CSIRTs Network | Business Role |
| Progress Report | Business Object |
| Relevant Information | Business Event |
| Relevant Secure Information Exchange | Business Process |
| Request of an individual CSIRT | Business Event |
| Secretariat Provider | Business Role |
| Security Operations Centre | Business Role |

# Cybersecurity information-sharing arrangements

*No viewpoint*




## Documentation

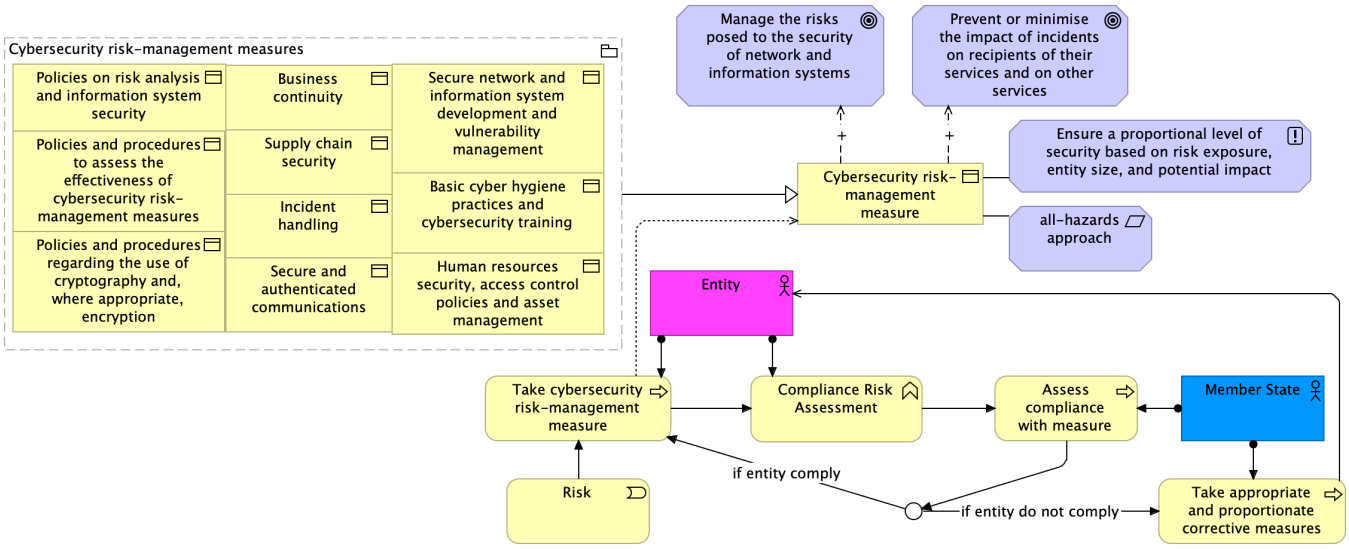
Numbering: 6.29

## Elements

| Element | Type |
|---|---|
| aims to prevent, detect, respond to or recover from incidents or to mitigate their impact | Goal |
| Cybersecurity information-sharing arrangement | Business Interaction |
| enhance the level of cybersecurity | Driver |
| ENISA | Business Actor |
| Entity | Business Actor |
| exchange on a voluntary basis relevant cybersecurity information | Principle |
| Facilitate establishment | Business Process |
| Member State | Business Actor |
| NIS2 Competent Authority | Business Role |
| Notify competent authority of participation or withdrawal | Business Event |

# Cybersecurity risk-management measures

*No viewpoint*




## Documentation

Numbering: 4.21

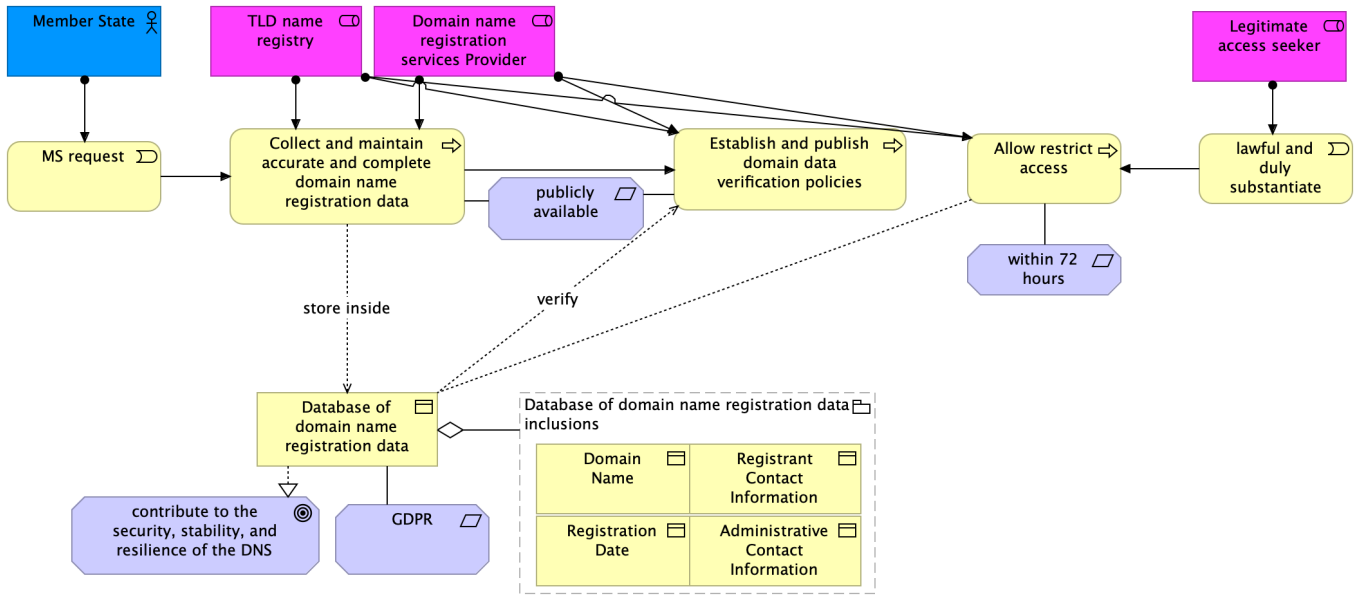
## Elements

| Element | Type |
|---|---|
| all-hazards approach | Requirement |
| Assess compliance with measure | Business Process |
| Basic cyber hygiene practices and cybersecurity training | Business Object |
| Business continuity | Business Object |
| Compliance Risk Assessment | Business Function |
| Cybersecurity risk-management measure | Business Object |
| Cybersecurity risk-management measures | Grouping |
| Ensure a proportional level of security based on risk exposure, entity size, and potential impact | Principle |
| Entity | Business Actor |
| Human resources security, access control policies and asset management | Business Object |
| Incident handling | Business Object |
| Manage the risks posed to the security of network and information systems | Goal |
| Member State | Business Actor |
| Policies and procedures regarding the use of cryptography and, where appropriate, encryption | Business Object |
| Policies and procedures to assess the effectiveness of cybersecurity risk-management measures | Business Object |
| Policies on risk analysis and information system security | Business Object |
| Prevent or minimise the impact of incidents on recipients of their services and on other services | Goal |

| Element | Type |
| --- | --- |
| Risk | Business Event |
| Secure and authenticated communications | Business Object |
| Secure network and information system development and vulnerability management | Business Object |
| Supply chain security | Business Object |
| Take appropriate and proportionate corrective measures | Business Process |
| Take cybersecurity risk-management measure | Business Process |

# Database of domain name registration data

*No viewpoint*




## Documentation

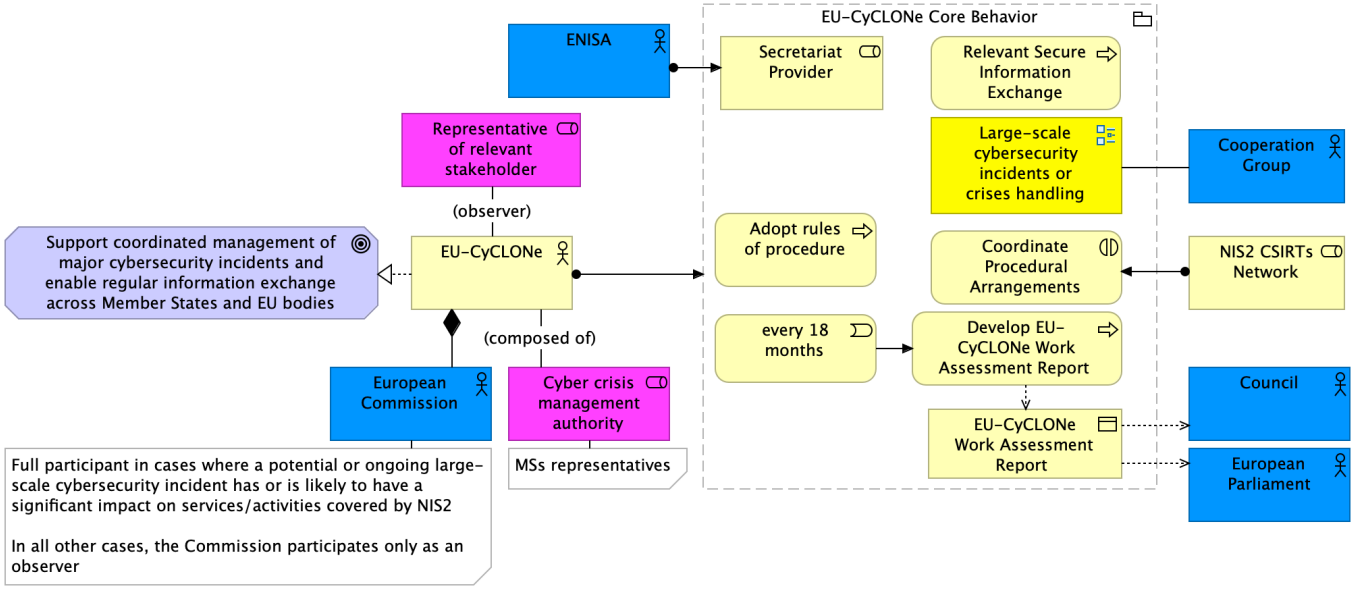
Numbering: 5.28

## Elements

| Element | Type |
|---|---|
| Administrative Contact Information | Business Object |
| Allow restrict access | Business Process |
| Collect and maintain accurate and complete domain name registration data | Business Process |
| contribute to the security, stability, and resilience of the DNS | Goal |
| Database of domain name registration data | Business Object |
| Database of domain name registration data inclusions | Grouping |
| Domain Name | Business Object |
| Domain name registration services Provider | Business Role |
| Establish and publish domain data verification policies | Business Process |
| GDPR | Requirement |
| lawful and duly substantiated request | Business Event |
| Legitimate access seeker | Business Role |
| Member State | Business Actor |
| MS request | Business Event |
| publicly available | Requirement |
| Registrant Contact Information | Business Object |
| Registration Date | Business Object |
| TLD name registry | Business Role |
| within 72 hours | Requirement |

# EU-CyCLONe

*No viewpoint*




## Documentation

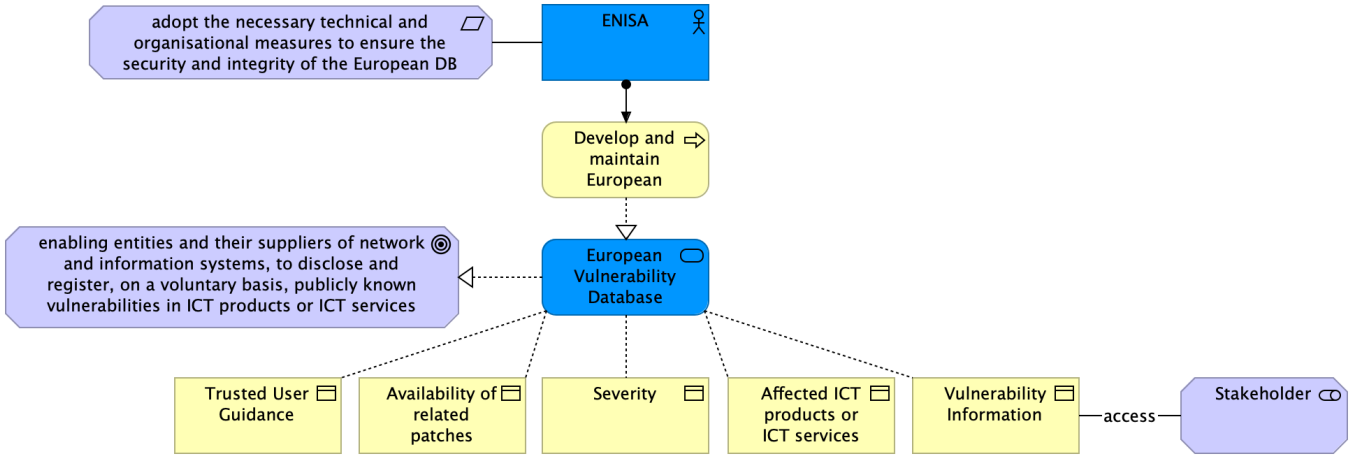
Numbering: 3.16

## Elements

| Element | Type |
|---|---|
| Adopt rules of procedure | Business Process |
| Cooperation Group | Business Actor |
| Coordinate Procedural Arrangements | Business Interaction |
| Council | Business Actor |
| Cyber crisis management authority | Business Role |
| Develop EU-CyCLONe Work Assessment Report | Business Process |
| ENISA | Business Actor |
| EU-CyCLONe | Business Actor |
| EU-CyCLONe Core Behavior | Grouping |
| EU-CyCLONe Work Assessment Report | Business Object |
| European Commission | Business Actor |
| European Parliament | Business Actor |
| every 18 months | Business Event |
| NIS2 CSIRTs Network | Business Role |
| Relevant Secure Information Exchange | Business Process |
| Representative of relevant stakeholder | Business Role |
| Secretariat Provider | Business Role |
| Support coordinated management of major cybersecurity incidents and enable regular information exchange across Member States and EU bodies | Goal |

# European vulnerability database

*No viewpoint*




## Documentation

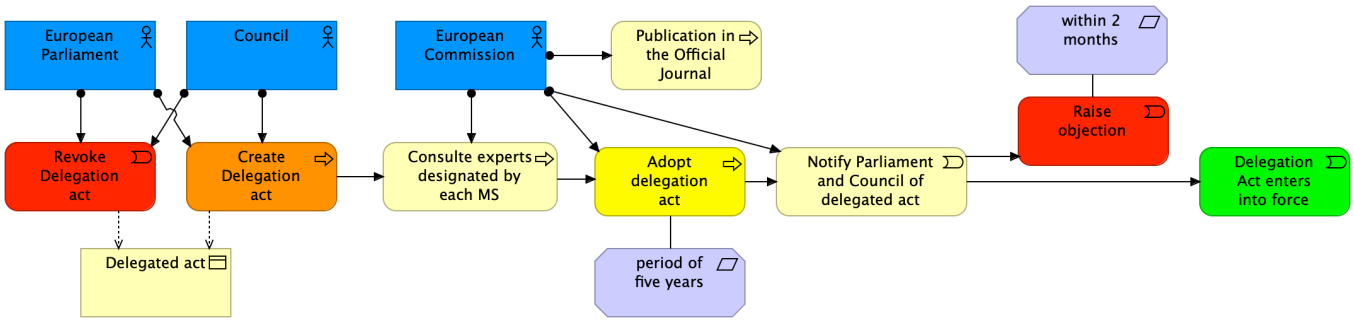
Numbering: 2.12

## Elements

| Element | Type |
|---|---|
| adopt the necessary technical and organisational measures to ensure the security and integrity of the European DB | Requirement |
| Affected ICT products or ICT services | Business Object |
| Availability of related patches | Business Object |
| Develop and maintain European Vulnerability DB | Business Process |
| enabling entities and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services | Goal |
| ENISA | Business Actor |
| European Vulnerability Database | Business Service |
| Severity | Business Object |
| Stakeholder | Stakeholder |
| Trusted User Guidance | Business Object |
| Vulnerability Information | Business Object |

# Exercise of the delegation

*No viewpoint*




## Documentation

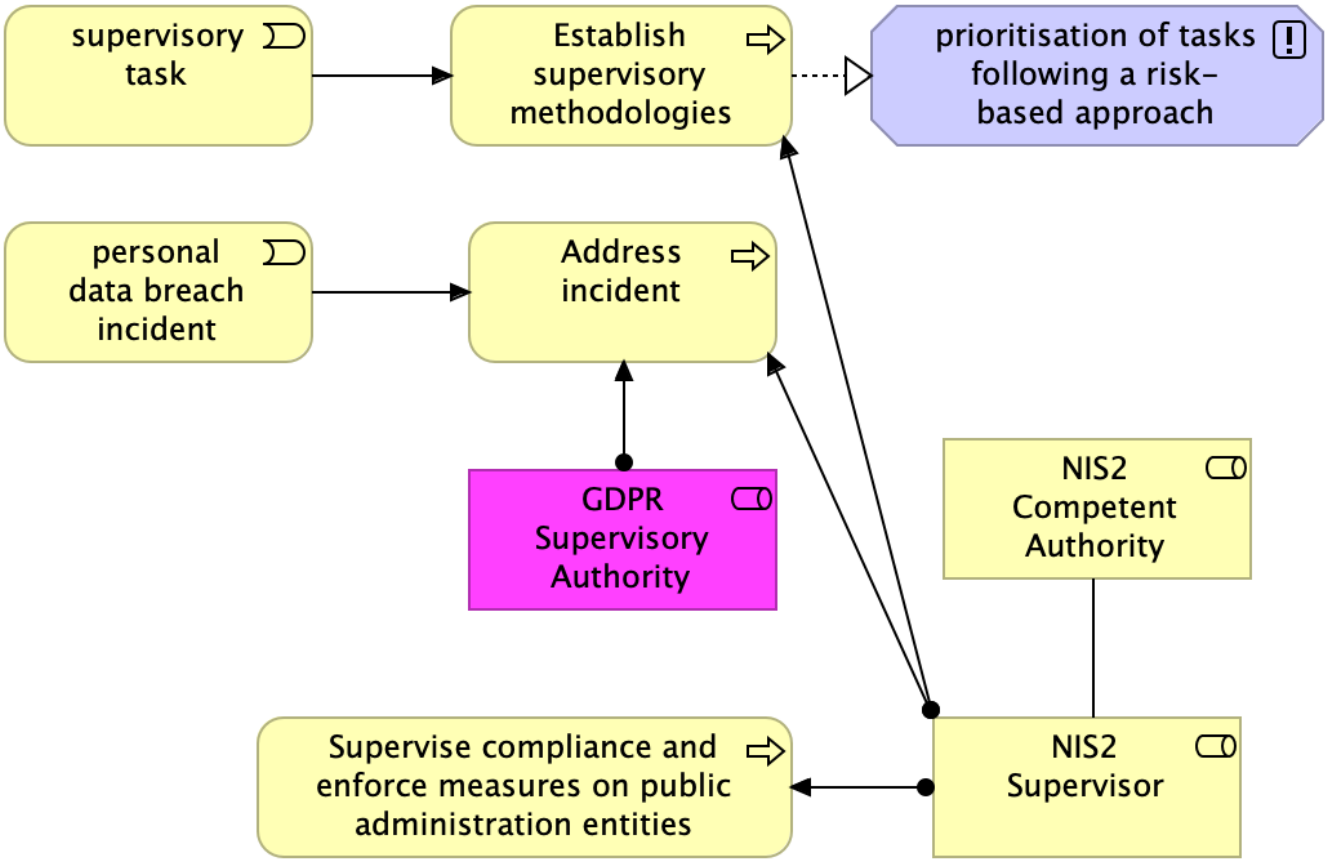
Numbering: 8.38

## Elements

| Element | Type |
|---|---|
| Adopt delegation act | Business Process |
| Consulte experts designated by each MS | Business Process |
| Council | Business Actor |
| Create Delegation act | Business Process |
| Delegated act | Business Object |
| Delegation Act enters into force | Business Event |
| European Commission | Business Actor |
| European Parliament | Business Actor |
| Notify Parliament and Council of delegated act | Business Event |
| period of five years | Requirement |
| Publication in the Official Journal | Business Process |
| Raise objection | Business Event |
| Revoke Delegation act | Business Event |
| within 2 months | Requirement |

# General aspects concerning supervision and enforcement

*No viewpoint*




## Documentation

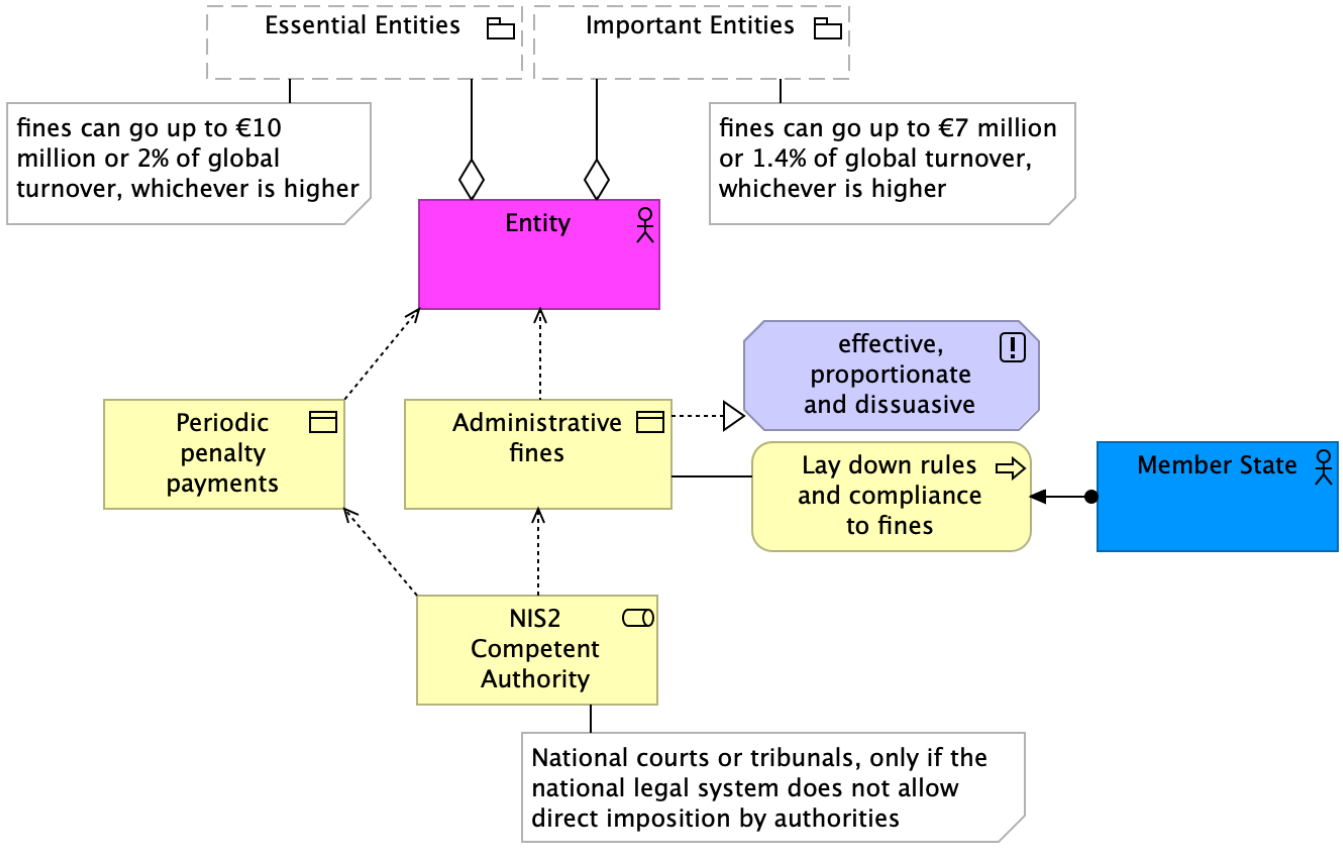
Numbering: 7.31

## Elements

| Element | Type |
|---|---|
| Address incident | Business Process |
| Establish supervisory methodologies | Business Process |
| GDPR Supervisory Authority | Business Role |
| NIS2 Competent Authority | Business Role |
| NIS2 Supervisor | Business Role |
| personal data breach incident | Business Event |
| prioritisation of tasks following a risk-based approach | Principle |
| Supervise compliance and enforce measures on public administration entities | Business Process |
| supervisory task | Business Event |

# General conditions for imposing administrative fines on essential and important entities

*No viewpoint*




## Documentation

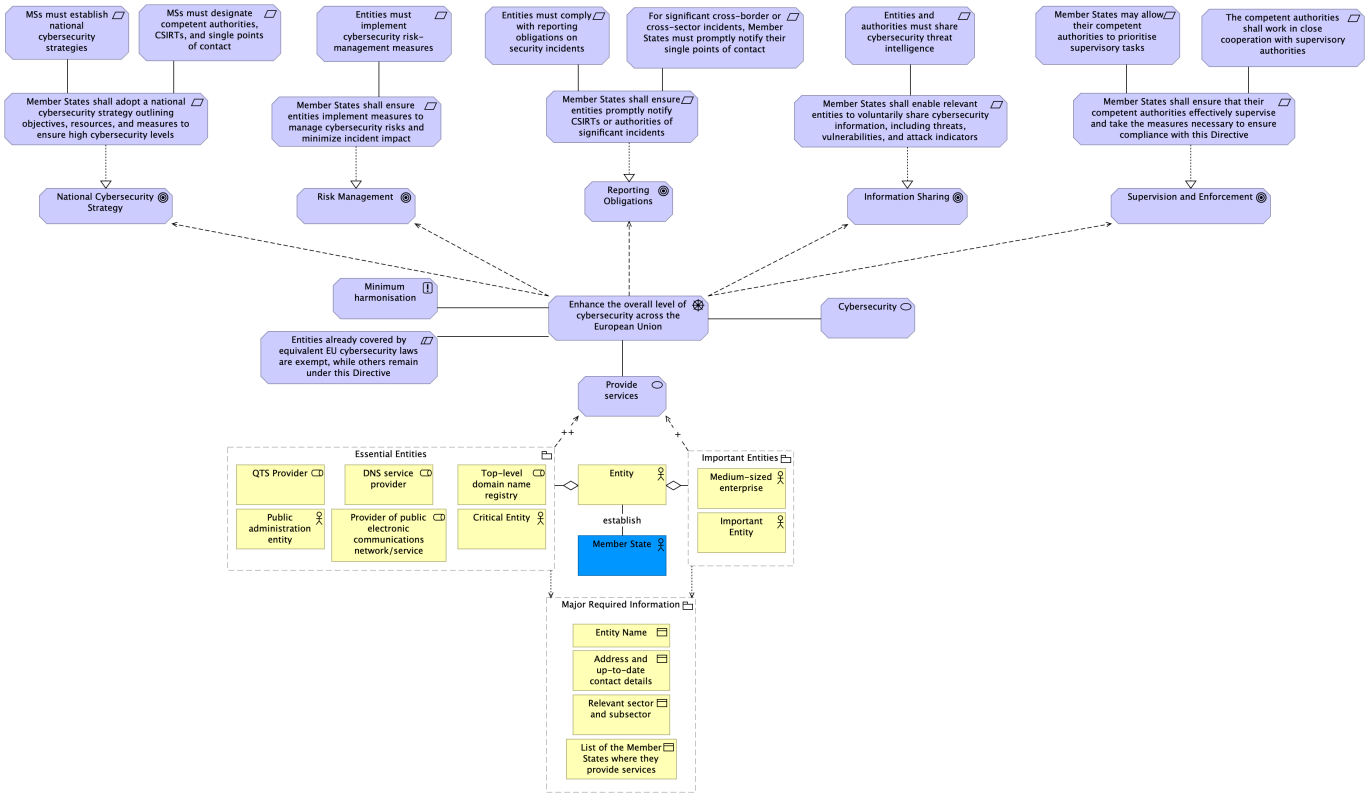
Numbering: 7.34

## Elements

| Element | Type |
|---|---|
| Administrative fines | Business Object |
| effective, proportionate and dissuasive | Principle |
| Entity | Business Actor |
| Essential Entities | Grouping |
| Important Entities | Grouping |
| Lay down rules and compliance to fines | Business Process |
| Member State | Business Actor |
| NIS2 Competent Authority | Business Role |
| Periodic penalty payments | Business Object |

# General Provisions

*No viewpoint*




## Documentation

Numbering: 1.1, 1.2, 1.3, 1.4, 1.5

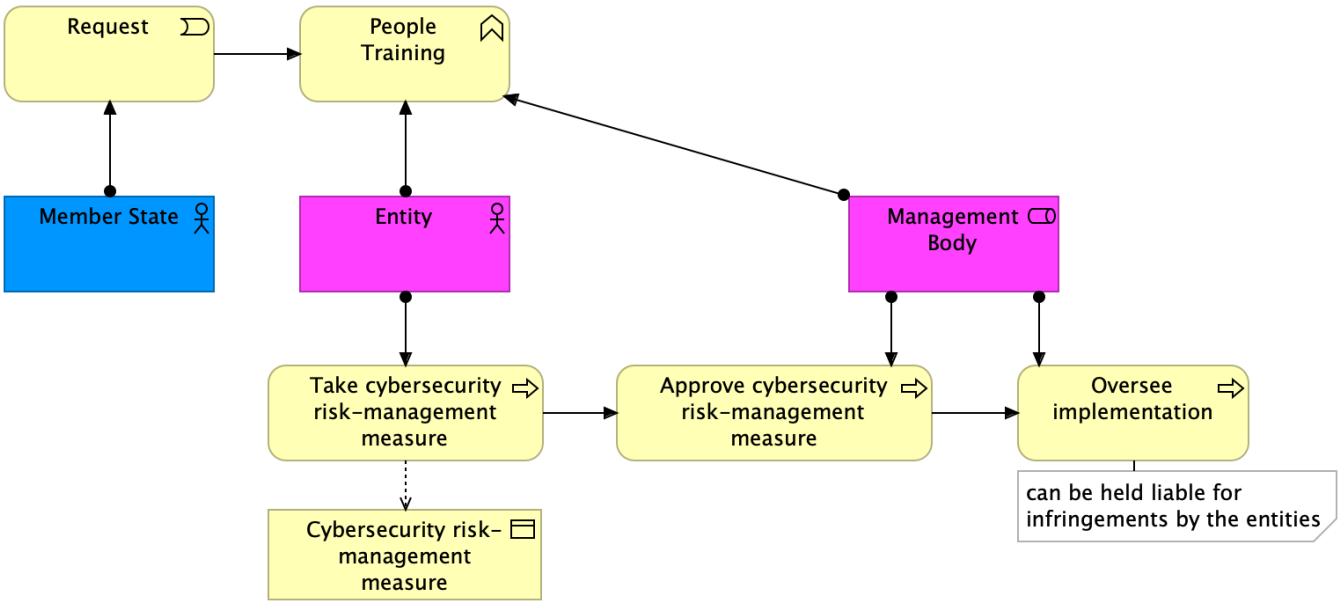
## Elements

| Element | Type |
|---|---|
| Address and up-to-date contact details | Business Object |
| Critical Entity | Business Actor |
| Cybersecurity | Value |
| DNS service provider | Business Role |
| Enhance the overall level of cybersecurity across the European Union | Driver |
| Entities already covered by equivalent EU cybersecurity laws are exempt, while others remain under this Directive | Constraint |
| Entities and authorities must share cybersecurity threat intelligence | Requirement |
| Entities must comply with reporting obligations on security incidents | Requirement |
| Entities must implement cybersecurity risk-management measures | Requirement |
| Entity | Business Actor |
| Entity Name | Business Object |
| Essential Entities | Grouping |
| For significant cross-border or cross-sector | Requirement |

| Element | Type |
|---|---|
| incidents, Member States must promptly notify their single points of contact | |
| Important Entities | Grouping |
| Important Entity | Business Actor |
| Information Sharing | Goal |
| List of the Member States where they provide services | Business Object |
| Major Required Information | Grouping |
| Medium-sized enterprise | Business Actor |
| Member State | Business Actor |
| Member States may allow their competent authorities to prioritise supervisory tasks | Requirement |
| Member States shall adopt a national cybersecurity strategy outlining objectives, resources, and measures to ensure high cybersecurity levels | Requirement |
| Member States shall enable relevant entities to voluntarily share cybersecurity information, including threats, vulnerabilities, and attack indicators | Requirement |
| Member States shall ensure entities implement measures to manage cybersecurity risks and minimize incident impact | Requirement |
| Member States shall ensure entities promptly notify CSIRTs or authorities of significant incidents | Requirement |
| Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive | Requirement |
| Minimum harmonisation | Principle |
| MSs must designate competent authorities, CSIRTs, and single points of contact | Requirement |
| MSs must establish national cybersecurity strategies | Requirement |
| National Cybersecurity Strategy | Goal |
| Provide services | Value |
| Provider of public electronic communications network/service | Business Role |
| Public administration entity | Business Actor |
| QTS Provider | Business Role |
| Relevant sector and subsector | Business Object |
| Reporting Obligations | Goal |
| Risk Management | Goal |
| Supervision and Enforcement | Goal |
| The competent authorities shall work in close cooperation with supervisory authorities | Requirement |
| Top-level domain name registry | Business Role |

# Governance

*No viewpoint*




## Documentation

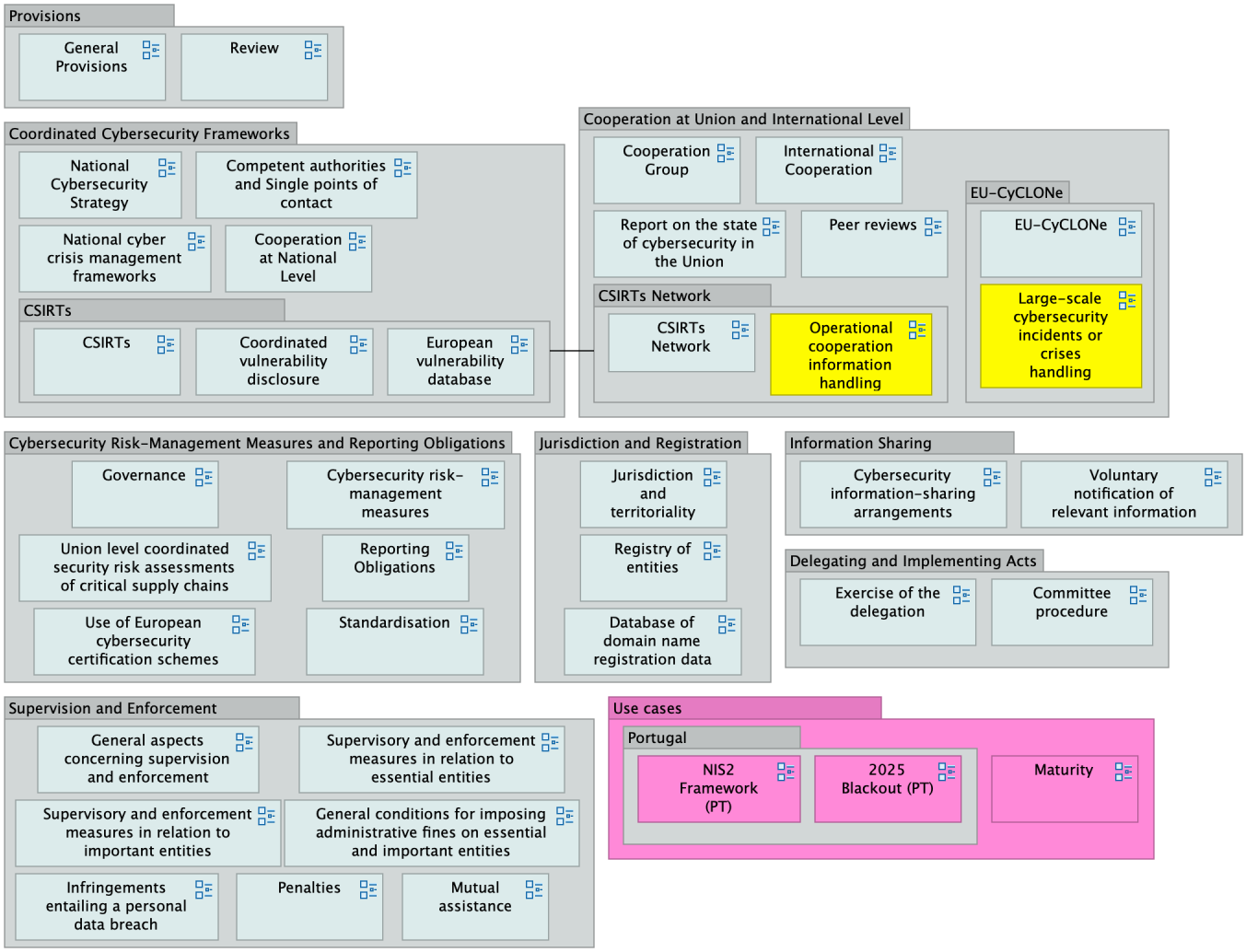
Numbering: 4.20

## Elements

| Element | Type |
|---|---|
| Approve cybersecurity risk-management measure | Business Process |
| Cybersecurity risk-management measure | Business Object |
| Entity | Business Actor |
| Management Body | Business Role |
| Member State | Business Actor |
| Oversee implementation | Business Process |
| People Training | Business Function |
| Request | Business Event |
| Take cybersecurity risk-management measure | Business Process |

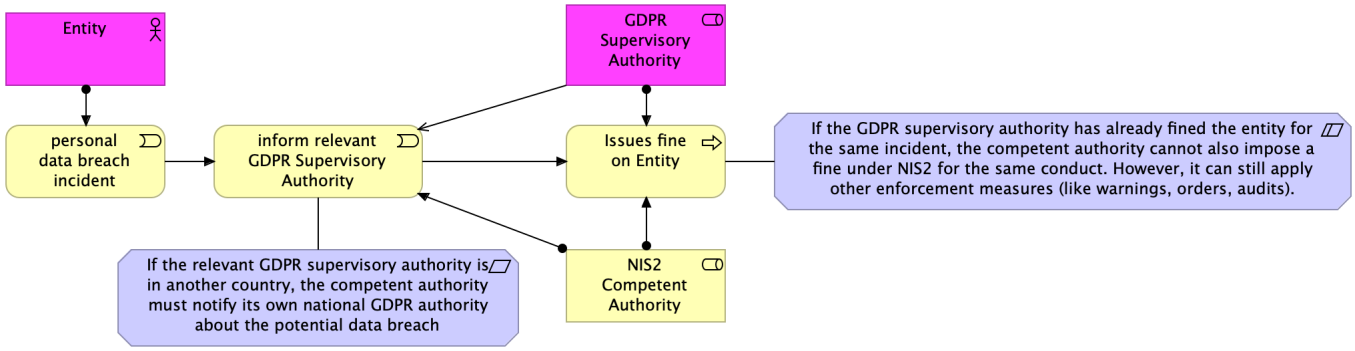
# Index

*No viewpoint*



# Infringements entailing a personal data breach

*No viewpoint*




## Documentation

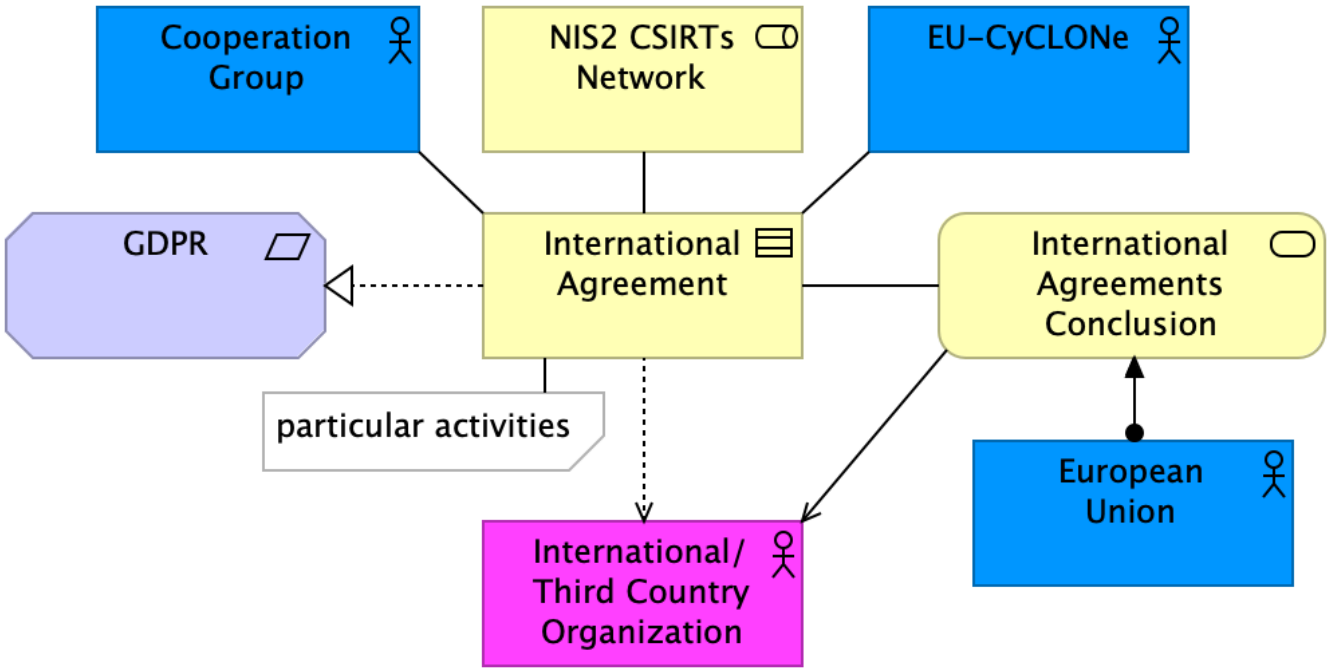
Numbering: 7.35

## Elements

| Element | Type |
|---|---|
| Entity | Business Actor |
| GDPR Supervisory Authority | Business Role |
| If the GDPR supervisory authority has already fined the entity for the same incident, the competent authority cannot also impose a fine under NIS2 for the same conduct. However, it can still apply other enforcement measures (like warnings, orders, audits). | Constraint |
| If the relevant GDPR supervisory authority is in another country, the competent authority must notify its own national GDPR authority about the potential data breach | Requirement |
| inform relevant GDPR Supervisory Authority | Business Event |
| Issues fine on Entity | Business Process |
| NIS2 Competent Authority | Business Role |
| personal data breach incident | Business Event |

# International Cooperation

*No viewpoint*




## Documentation

Numbering: 3.17

## Elements

| Element | Type |
|---|---|
| Cooperation Group | Business Actor |
| EU-CyCLONe | Business Actor |
| European Union | Business Actor |
| GDPR | Requirement |
| International Agreement | Contract |
| International Agreements Conclusion | Business Service |
| International/Third Country Organization | Business Actor |
| NIS2 CSIRTs Network | Business Role |

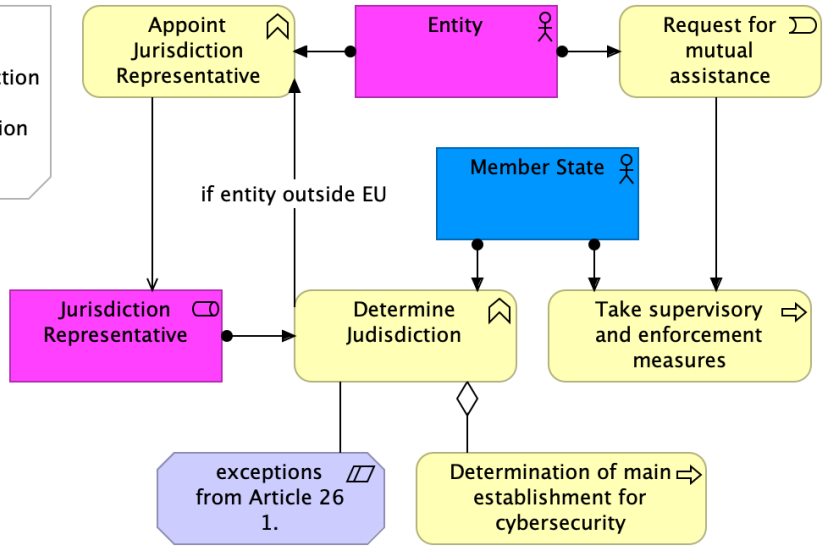
# Jurisdiction and territoriality

*No viewpoint*

Workflow:

1: If the Entity is within the EU → Determine Jurisdiction

2: If the Entity is outside the EU → Appoint Jurisdiction Representative → Determine Jurisdiction based on representative location




## Documentation

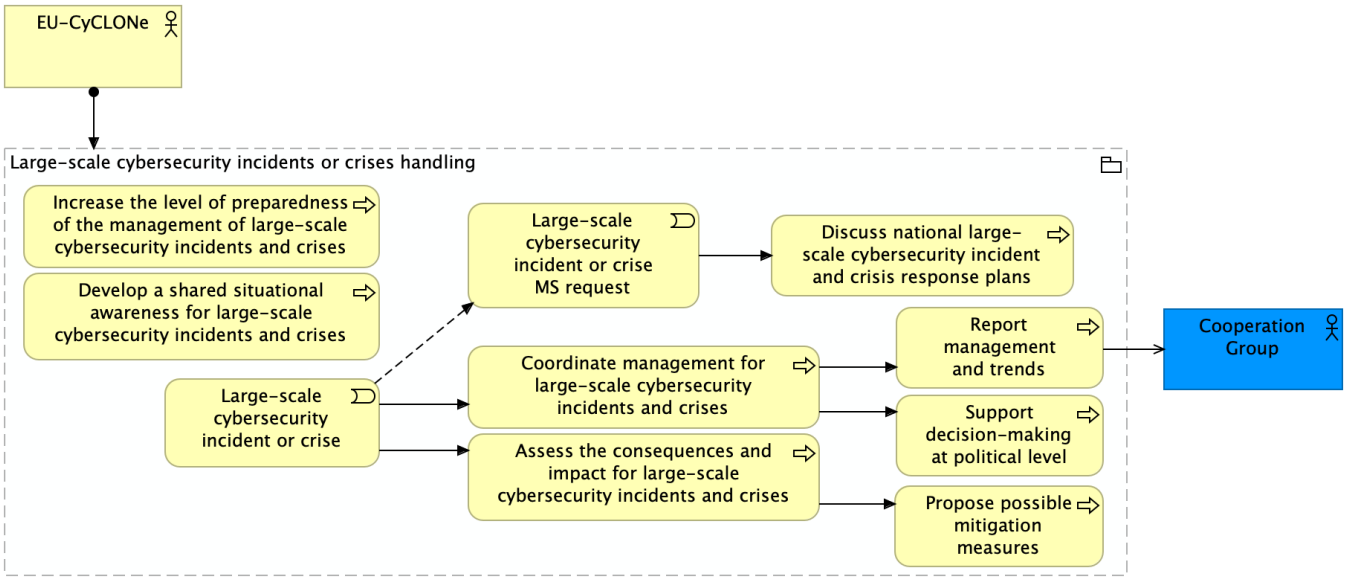
Numbering: 5.26

## Elements

| Element | Type |
|---|---|
| Appoint Jurisdiction Representative | Business Function |
| Determination of main establishment for cybersecurity oversight | Business Process |
| Determine Judisdiction | Business Function |
| Entity | Business Actor |
| exceptions from Article 26 1. | Constraint |
| Jurisdiction Representative | Business Role |
| Member State | Business Actor |
| Request for mutual assistance | Business Event |
| Take supervisory and enforcement measures | Business Process |

# Large-scale cybersecurity incidents or crises handling

*No viewpoint*




## Documentation

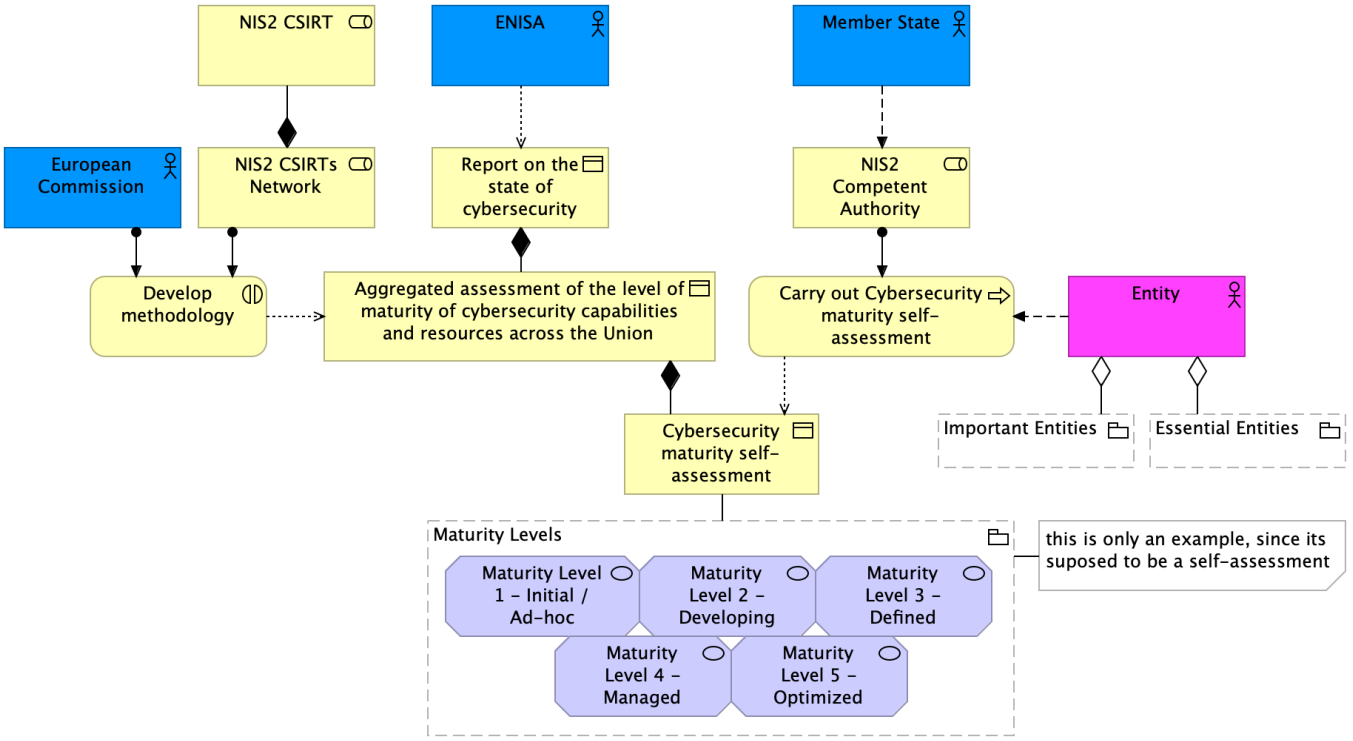
Numbering: 3.16.3, 3.16.5

## Elements

| Element | Type |
|---|---|
| Assess the consequences and impact for large-scale cybersecurity incidents and crises | Business Process |
| Cooperation Group | Business Actor |
| Coordinate management for large-scale cybersecurity incidents and crises | Business Process |
| Develop a shared situational awareness for large-scale cybersecurity incidents and crises | Business Process |
| Discuss national large-scale cybersecurity incident and crisis response plans | Business Process |
| EU-CyCLONe | Business Actor |
| Increase the level of preparedness of the management of large-scale cybersecurity incidents and crises | Business Process |
| Large-scale cybersecurity incident or crise | Business Event |
| Large-scale cybersecurity incident or crise MS request | Business Event |
| Large-scale cybersecurity incidents or crises handling | Grouping |
| Propose possible mitigation measures | Business Process |
| Report management and trends | Business Process |
| Support decision-making at political level | Business Process |

# Maturity

*No viewpoint*

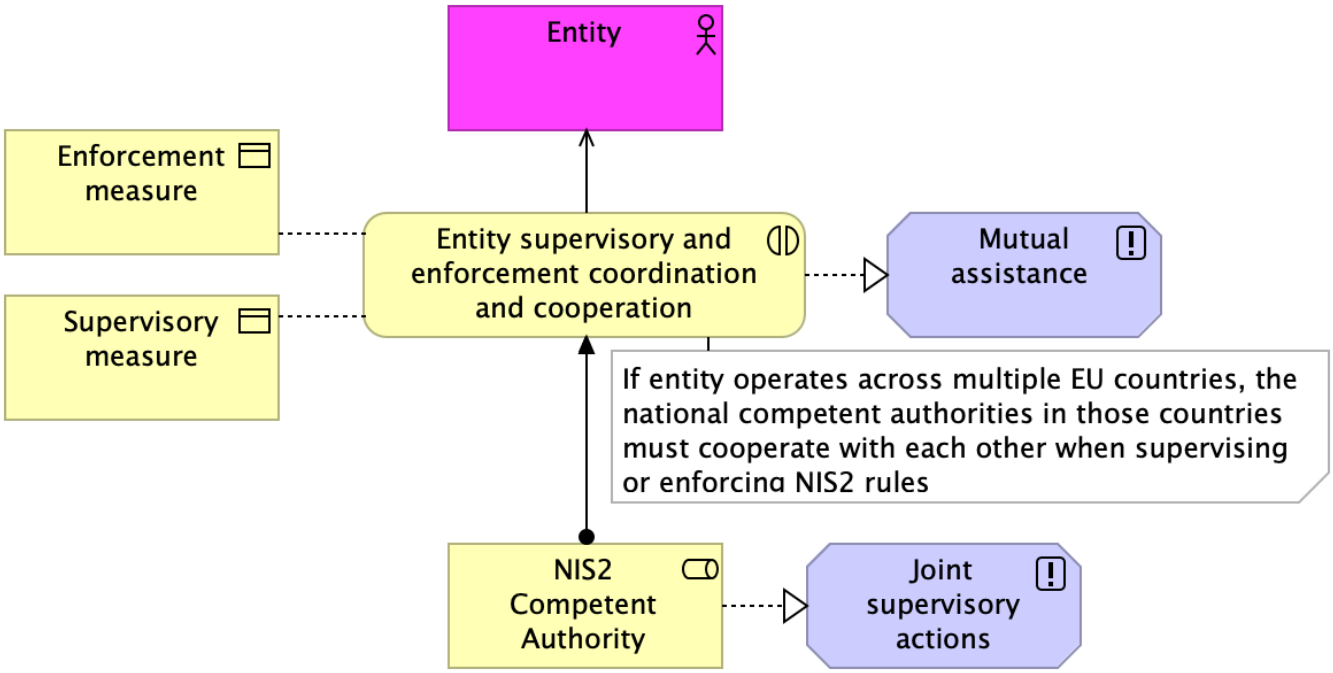



## Elements

| Element | Type |
|---|---|
| Aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union | Business Object |
| Carry out Cybersecurity maturity self-assessment | Business Process |
| Cybersecurity maturity self-assessment | Business Object |
| Develop methodology | Business Interaction |
| ENISA | Business Actor |
| Entity | Business Actor |
| Essential Entities | Grouping |
| European Commission | Business Actor |
| Important Entities | Grouping |
| Maturity Level 1 - Initial / Ad-hoc | Value |
| Maturity Level 2 - Developing | Value |
| Maturity Level 3 - Defined | Value |
| Maturity Level 4 - Managed | Value |
| Maturity Level 5 - Optimized | Value |
| Maturity Levels | Grouping |
| Member State | Business Actor |
| NIS2 Competent Authority | Business Role |
| NIS2 CSIRT | Business Role |
| NIS2 CSIRTs Network | Business Role |
| Report on the state of cybersecurity | Business Object |

# Mutual assistance

*No viewpoint*




## Documentation

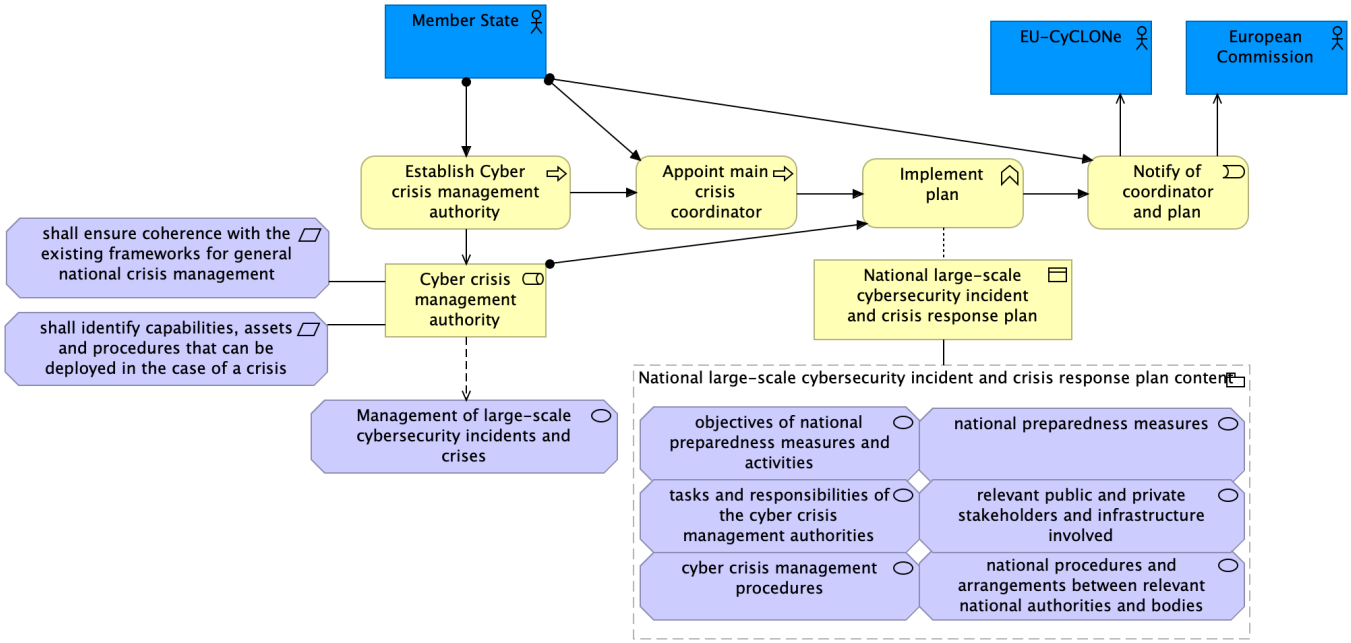
Numbering: 7.37

## Elements

| Element | Type |
|---|---|
| Enforcement measure | Business Object |
| Entity | Business Actor |
| Entity supervisory and enforcement coordination and cooperation | Business Interaction |
| Joint supervisory actions | Principle |
| Mutual assistance | Principle |
| NIS2 Competent Authority | Business Role |
| Supervisory measure | Business Object |

# National cyber crisis management frameworks

*No viewpoint*




## Documentation

Numbering: 2.9

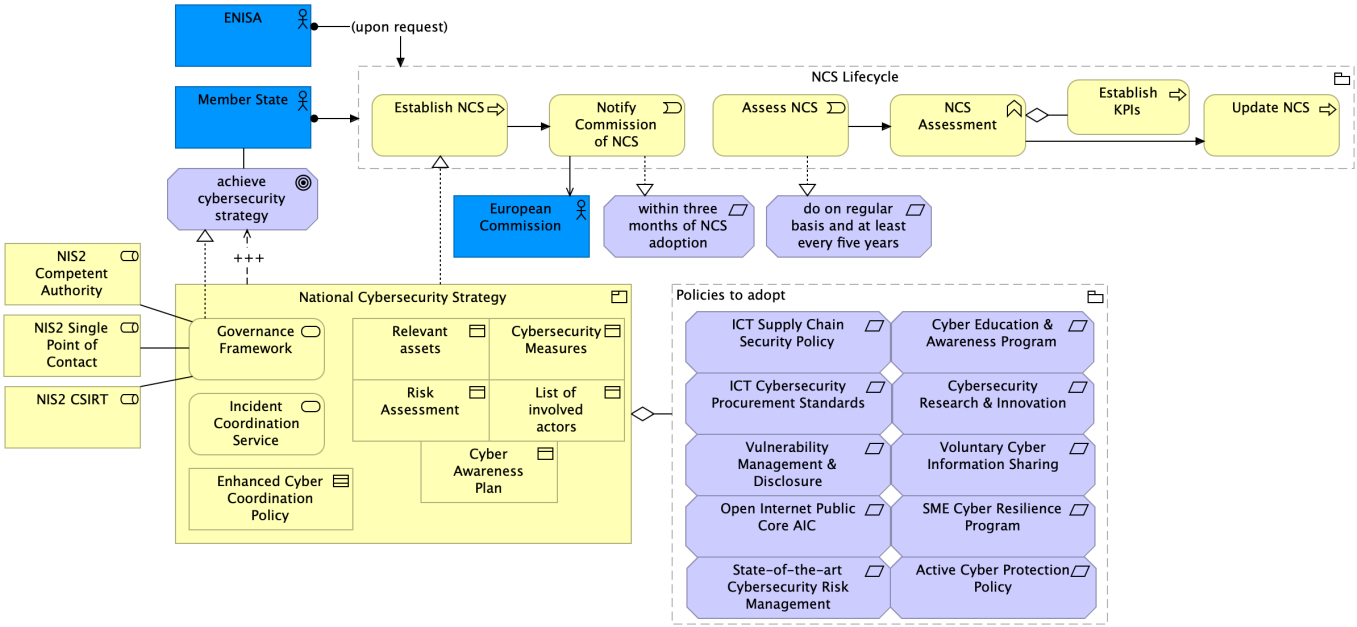
## Elements

| Element | Type |
|---|---|
| Appoint main crisis coordinator | Business Process |
| Cyber crisis management authority | Business Role |
| cyber crisis management procedures | Value |
| Establish Cyber crisis management authority | Business Process |
| EU-CyCLONe | Business Actor |
| European Commission | Business Actor |
| Implement plan | Business Function |
| Management of large-scale cybersecurity incidents and crises | Value |
| Member State | Business Actor |
| National large-scale cybersecurity incident and crisis response plan | Business Object |
| National large-scale cybersecurity incident and crisis response plan content | Grouping |
| national preparedness measures | Value |
| national procedures and arrangements between relevant national authorities and bodies | Value |
| Notify of coordinator and plan | Business Event |
| objectives of national preparedness measures and activities | Value |
| relevant public and private stakeholders and infrastructure involved | Value |

| Element | Type |
| --- | --- |
| shall ensure coherence with the existing frameworks for general national crisis management | Requirement |
| shall identify capabilities, assets and procedures that can be deployed in the case of a crisis | Requirement |
| tasks and responsibilities of the cyber crisis management authorities | Value |

# National Cybersecurity Strategy

*No viewpoint*




## Documentation

Numbering: 2.7

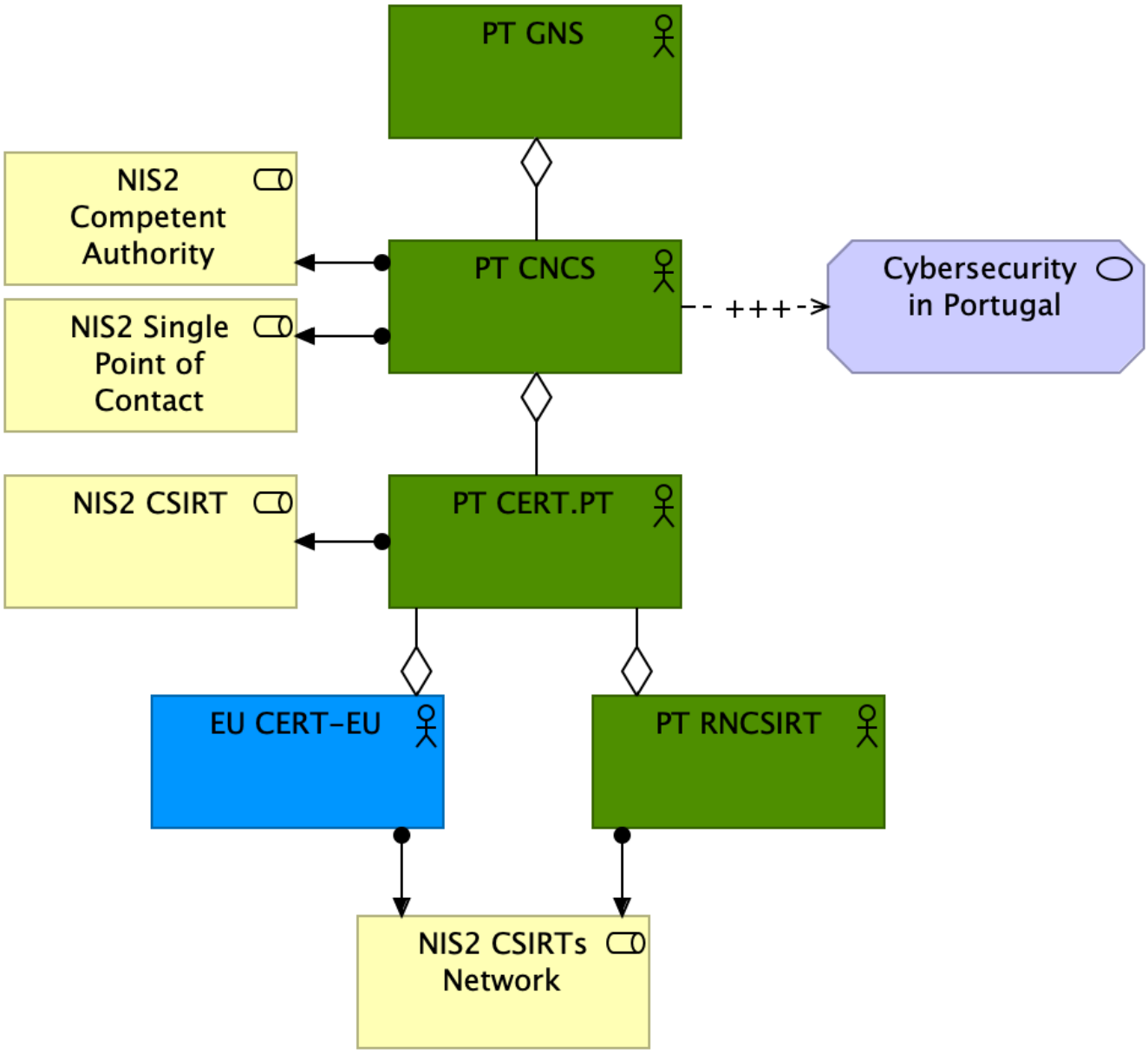
## Elements

| Element | Type |
|---|---|
| achieve cybersecurity strategy | Goal |
| Active Cyber Protection Policy | Requirement |
| Assess NCS | Business Event |
| Cyber Awareness Plan | Business Object |
| Cyber Education & Awareness Program | Requirement |
| Cybersecurity Measures | Business Object |
| Cybersecurity Research & Innovation | Requirement |
| do on regular basis and at least every five years | Requirement |
| Enhanced Cyber Coordination Policy | Contract |
| ENISA | Business Actor |
| Establish KPIs | Business Process |
| Establish NCS | Business Process |
| European Commission | Business Actor |
| Governance Framework | Business Service |
| ICT Cybersecurity Procurement Standards | Requirement |
| ICT Supply Chain Security Policy | Requirement |
| Incident Coordination Service | Business Service |
| List of involved actors | Business Object |
| Member State | Business Actor |
| National Cybersecurity Strategy | Product |
| NCS Assessment | Business Function |

| Element | Type |
| --- | --- |
| NCS Lifecycle | Grouping |
| NIS2 Competent Authority | Business Role |
| NIS2 CSIRT | Business Role |
| NIS2 Single Point of Contact | Business Role |
| Notify Commission of NCS | Business Event |
| Open Internet Public Core AIC | Requirement |
| Policies to adopt | Grouping |
| Relevant assets | Business Object |
| Risk Assessment | Business Object |
| SME Cyber Resilience Program | Requirement |
| State-of-the-art Cybersecurity Risk Management | Requirement |
| Update NCS | Business Process |
| Voluntary Cyber Information Sharing | Requirement |
| Vulnerability Management & Disclosure | Requirement |
| within three months of NCS adoption | Requirement |

# NIS2 Framework (PT)

*No viewpoint*

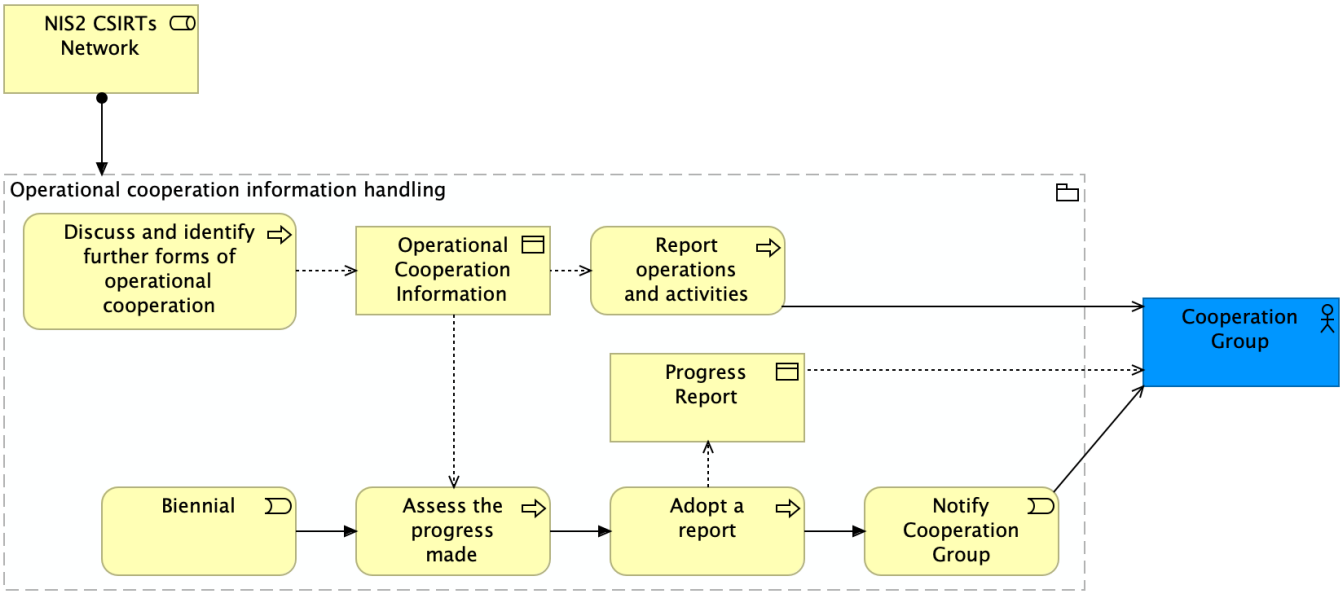



## Elements

| Element | Type |
|---|---|
| Cybersecurity in Portugal | Value |
| EU CERT-EU | Business Actor |
| NIS2 Competent Authority | Business Role |
| NIS2 CSIRT | Business Role |
| NIS2 CSIRTs Network | Business Role |
| NIS2 Single Point of Contact | Business Role |
| PT CERT.PT | Business Actor |
| PT CNCS | Business Actor |
| PT GNS | Business Actor |
| PT RNCSIRT | Business Actor |

# Operational cooperation information handling

*No viewpoint*




## Documentation

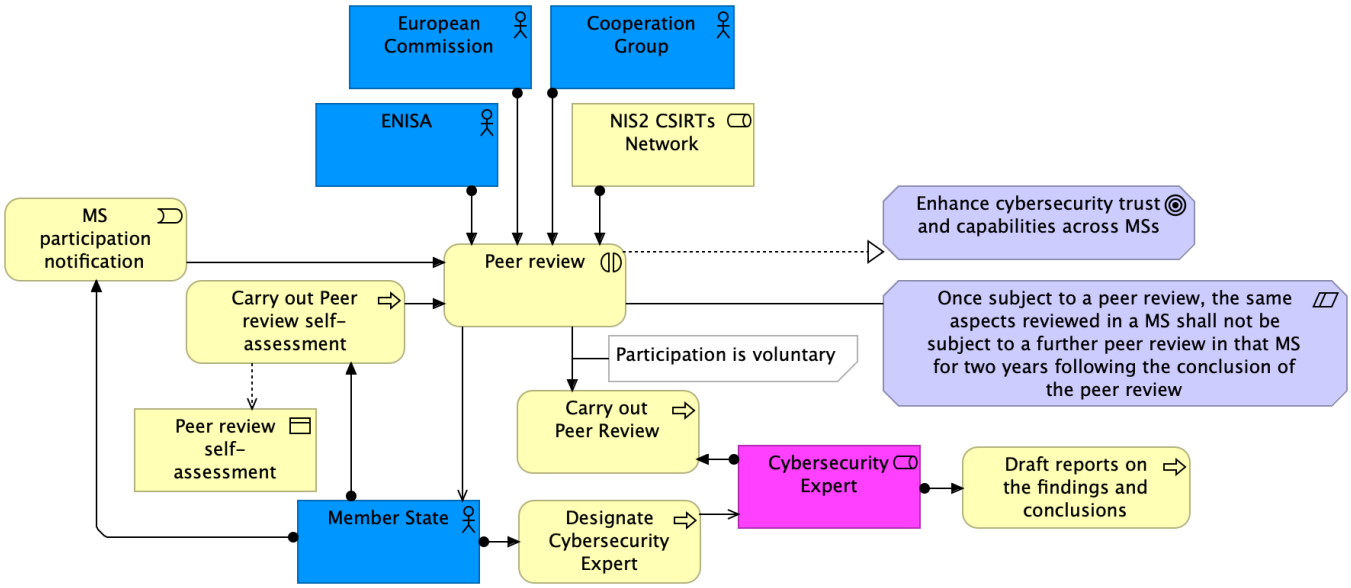
Numbering: 3.15.3.10.j

## Elements

| Element | Type |
|---|---|
| Adopt a report | Business Process |
| Assess the progress made | Business Process |
| Biennial | Business Event |
| Cooperation Group | Business Actor |
| Discuss and identify further forms of operational cooperation | Business Process |
| NIS2 CSIRTs Network | Business Role |
| Notify Cooperation Group | Business Event |
| Operational Cooperation Information | Business Object |
| Operational cooperation information handling | Grouping |
| Progress Report | Business Object |
| Report operations and activities | Business Process |

# Peer reviews

*No viewpoint*




## Documentation

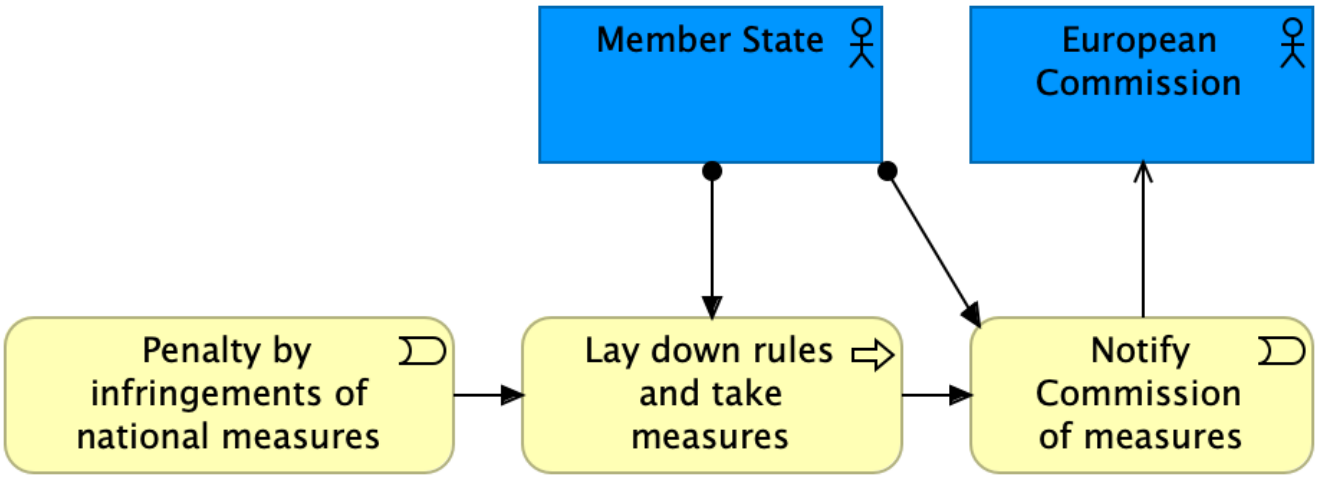
Numbering: 3.19

## Elements

| Element | Type |
|---|---|
| Carry out Peer Review | Business Process |
| Carry out Peer review self-assessment | Business Process |
| Cooperation Group | Business Actor |
| Cybersecurity Expert | Business Role |
| Designate Cybersecurity Expert | Business Process |
| Draft reports on the findings and conclusions | Business Process |
| Enhance cybersecurity trust and capabilities across MSs | Goal |
| ENISA | Business Actor |
| European Commission | Business Actor |
| Member State | Business Actor |
| MS participation notification | Business Event |
| NIS2 CSIRTs Network | Business Role |
| Once subject to a peer review, the same aspects reviewed in a MS shall not be subject to a further peer review in that MS for two years following the conclusion of the peer review | Constraint |
| Peer review | Business Interaction |
| Peer review self-assessment | Business Object |

# Penalties

*No viewpoint*




## Documentation

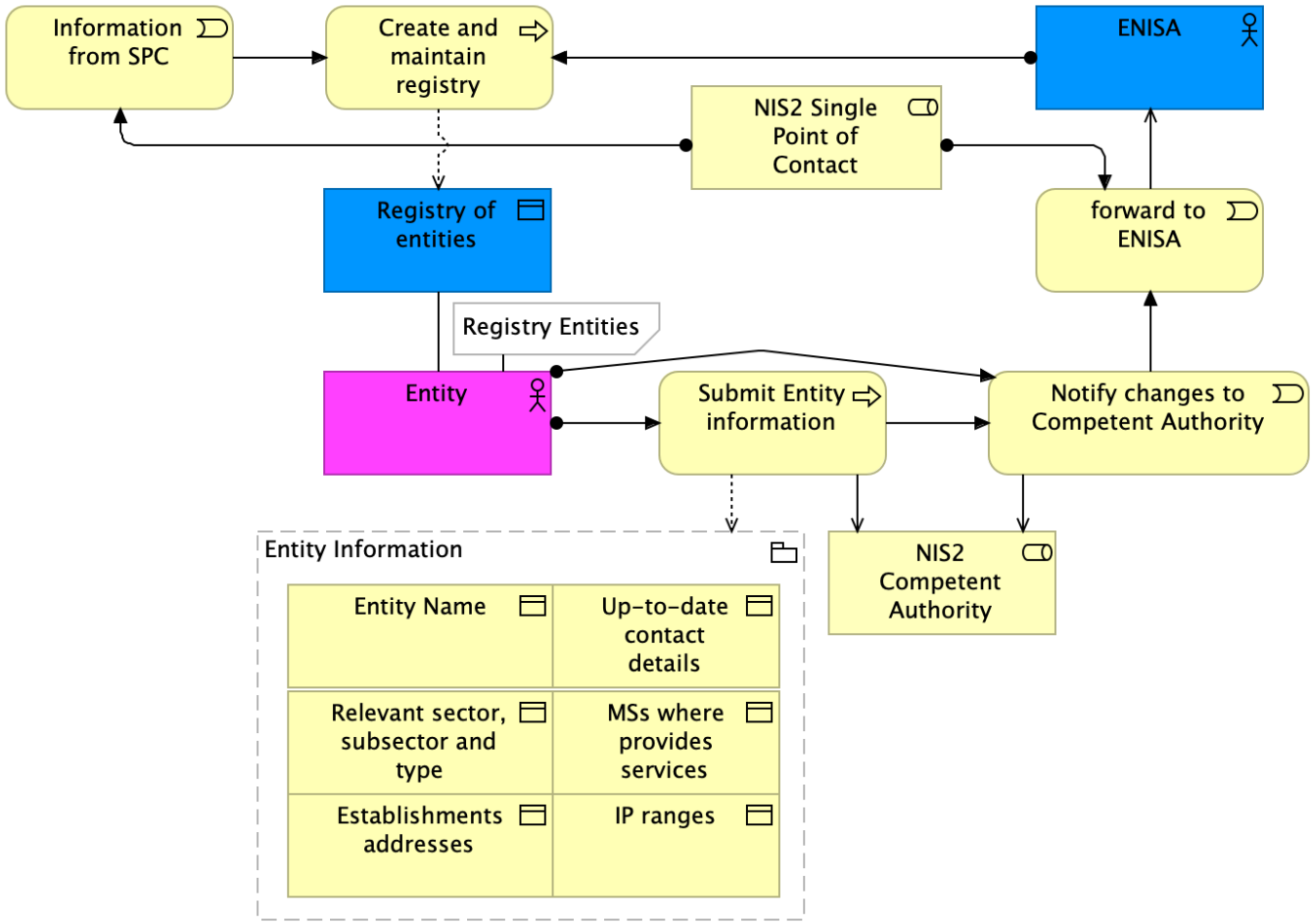
Numbering: 7.36

## Elements

| Element | Type |
|---|---|
| European Commission | Business Actor |
| Lay down rules and take measures | Business Process |
| Member State | Business Actor |
| Notify Commission of measures | Business Event |
| Penalty by infringements of national measures | Business Event |

# Registry of entities

*No viewpoint*




## Documentation

Numbering: 5.27

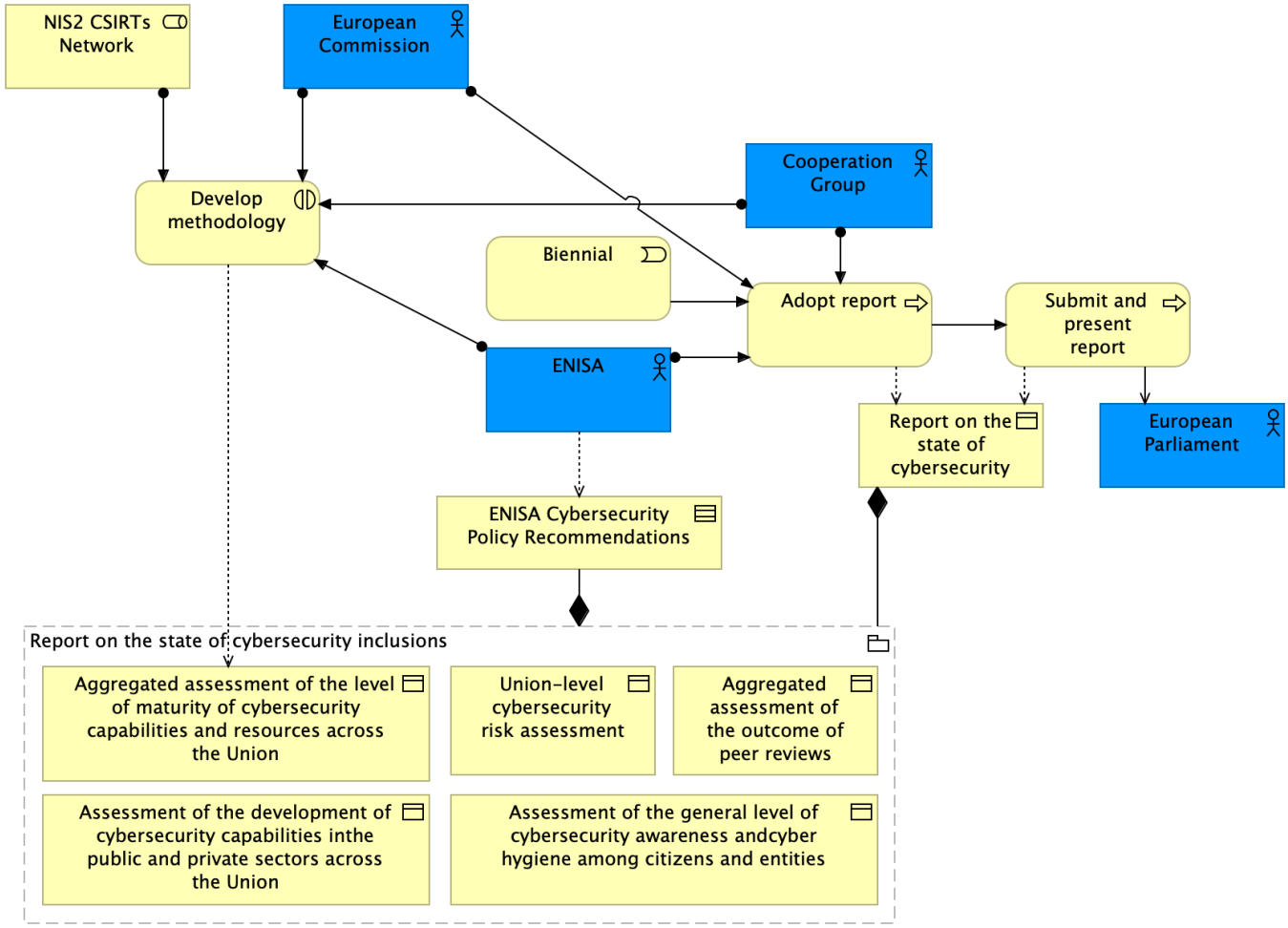
## Elements

| Element | Type |
|---|---|
| Create and maintain registry | Business Process |
| ENISA | Business Actor |
| Entity | Business Actor |
| Entity Information | Grouping |
| Entity Name | Business Object |
| Establishments addresses | Business Object |
| forward to ENISA | Business Event |
| Information from SPC | Business Event |
| IP ranges | Business Object |
| MSs where provides services | Business Object |
| NIS2 Competent Authority | Business Role |
| NIS2 Single Point of Contact | Business Role |
| Notify changes to Competent Authority | Business Event |

| Element | Type |
| --- | --- |
| Registry of entities | Business Object |
| Relevant sector, subsector and type | Business Object |
| Submit Entity information | Business Process |
| Up-to-date contact details | Business Object |

# Report on the state of cybersecurity in the Union

*No viewpoint*




## Documentation

Numbering: 3.18

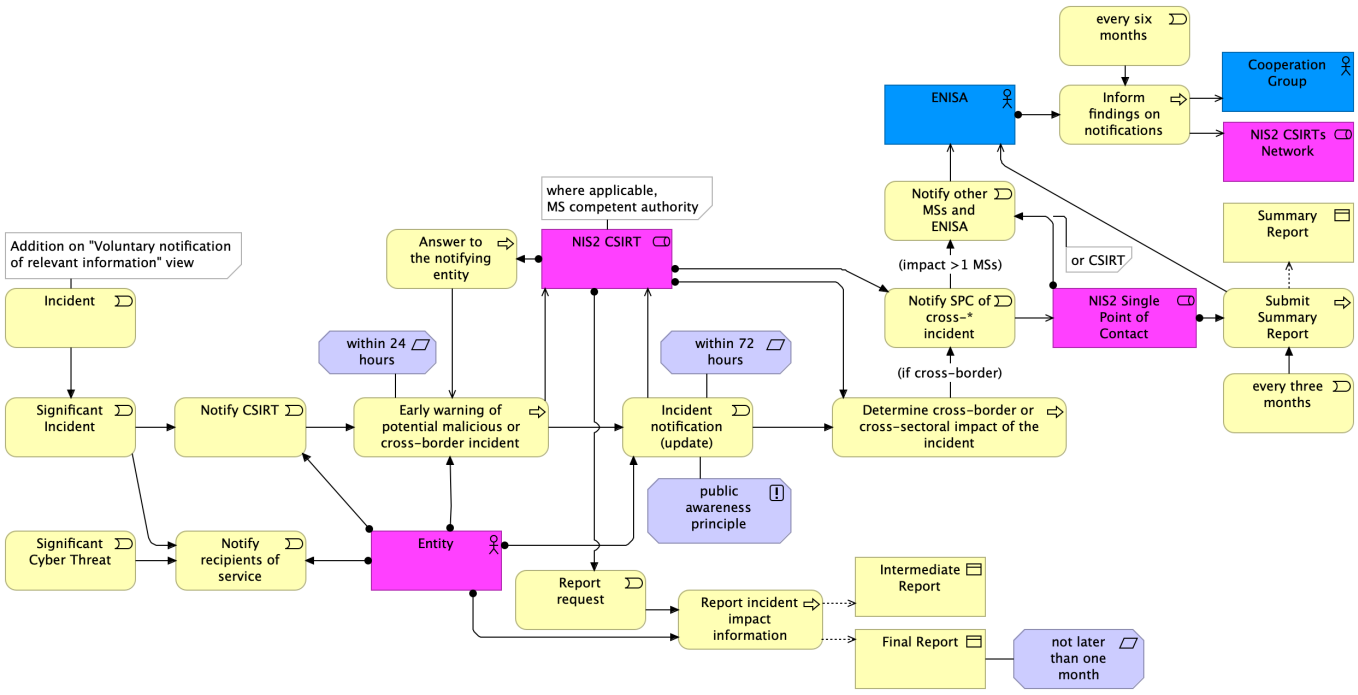
## Elements

| Element | Type |
|---|---|
| Adopt report | Business Process |
| Aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union | Business Object |
| Aggregated assessment of the outcome of peer reviews | Business Object |
| Assessment of the development of cybersecurity capabilities inthe public and private sectors across the Union | Business Object |
| Assessment of the general level of cybersecurity awareness andcyber hygiene among citizens and entities | Business Object |
| Biennial | Business Event |
| Cooperation Group | Business Actor |
| Develop methodology | Business Interaction |

| Element | Type |
| --- | --- |
| ENISA | Business Actor |
| ENISA Cybersecurity Policy Recommendations | Contract |
| European Commission | Business Actor |
| European Parliament | Business Actor |
| NIS2 CSIRTs Network | Business Role |
| Report on the state of cybersecurity | Business Object |
| Report on the state of cybersecurity inclusions | Grouping |
| Submit and present report | Business Process |
| Union-level cybersecurity risk assessment | Business Object |

# Reporting Obligations

*No viewpoint*




## Documentation

Numbering: 4.23

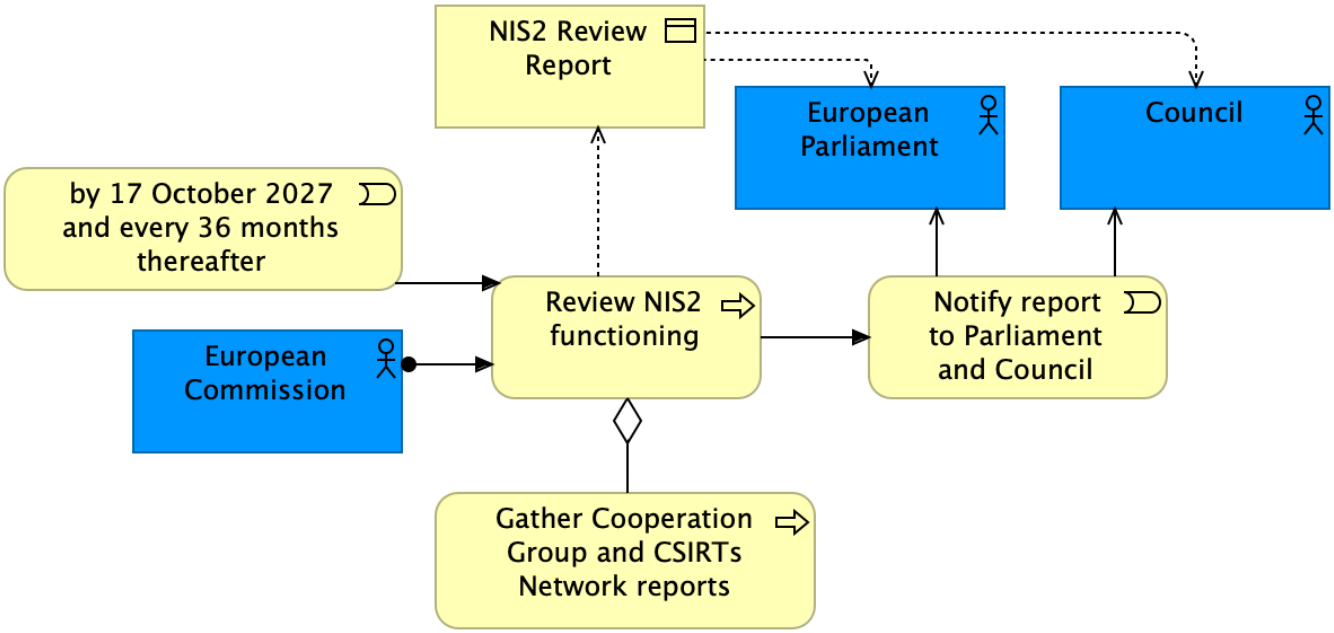
## Elements

| Element | Type |
|---|---|
| Answer to the notifying entity | Business Process |
| Cooperation Group | Business Actor |
| Determine cross-border or cross-sectoral impact of the incident | Business Process |
| Early warning of potential malicious or cross-border incident | Business Process |
| ENISA | Business Actor |
| Entity | Business Actor |
| every six months | Business Event |
| every three months | Business Event |
| Final Report | Business Object |
| Incident | Business Event |
| Incident notification (update) | Business Event |
| Inform findings on notifications | Business Process |
| Intermediate Report | Business Object |
| NIS2 CSIRT | Business Role |
| NIS2 CSIRTs Network | Business Role |
| NIS2 Single Point of Contact | Business Role |
| not later than one month | Requirement |
| Notify CSIRT | Business Event |

| Element | Type |
| --- | --- |
| Notify other MSs and ENISA | Business Event |
| Notify recipients of service | Business Event |
| Notify SPC of cross-* incident | Business Event |
| public awareness principle | Principle |
| Report incident impact information | Business Process |
| Report request | Business Event |
| Significant Cyber Threat | Business Event |
| Significant Incident | Business Event |
| Submit Summary Report | Business Process |
| Summary Report | Business Object |
| within 24 hours | Requirement |
| within 72 hours | Requirement |

# Review

*No viewpoint*




## Documentation

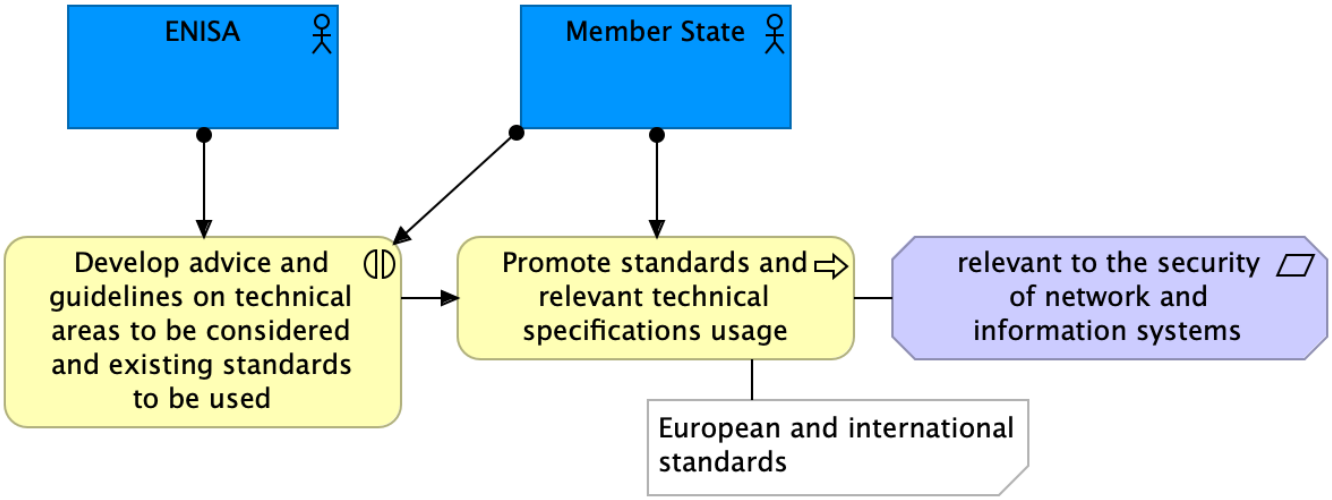
Numbering: 9.40

## Elements

| Element | Type |
|---|---|
| by 17 October 2027 and every 36 months thereafter | Business Event |
| Council | Business Actor |
| European Commission | Business Actor |
| European Parliament | Business Actor |
| Gather Cooperation Group and CSIRTs Network reports | Business Process |
| NIS2 Review Report | Business Object |
| Notify report to Parliament and Council | Business Event |
| Review NIS2 functioning | Business Process |

# Standardisation

*No viewpoint*




## Documentation

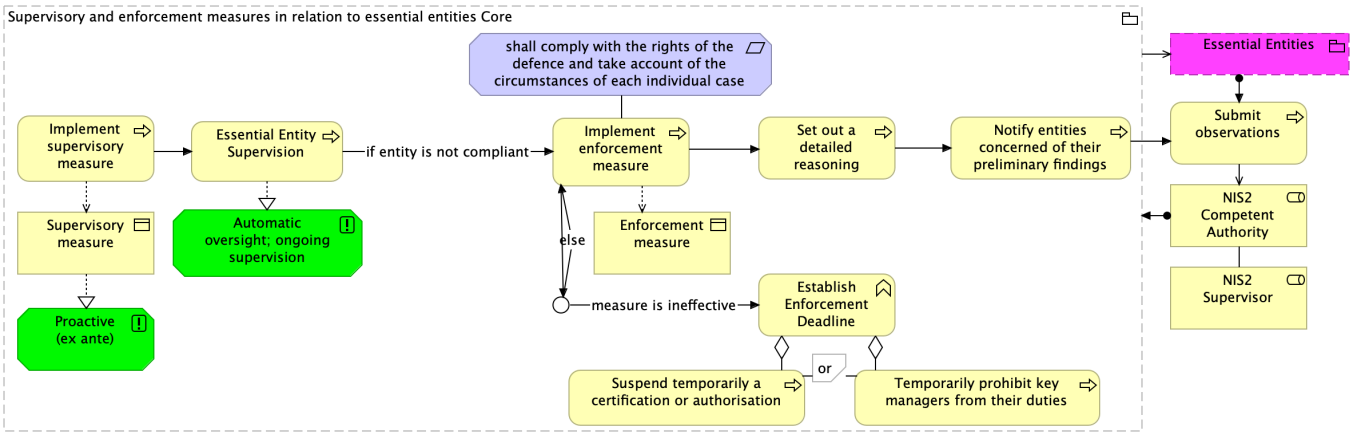
Numbering: 4.25

## Elements

| Element | Type |
|---|---|
| Develop advice and guidelines on technical areas to be considered and existing standards to be used | Business Interaction |
| ENISA | Business Actor |
| Member State | Business Actor |
| Promote standards and relevant technical specifications usage | Business Process |
| relevant to the security of network and information systems | Requirement |

# Supervisory and enforcement measures in relation to essential entities

*No viewpoint*




## Documentation

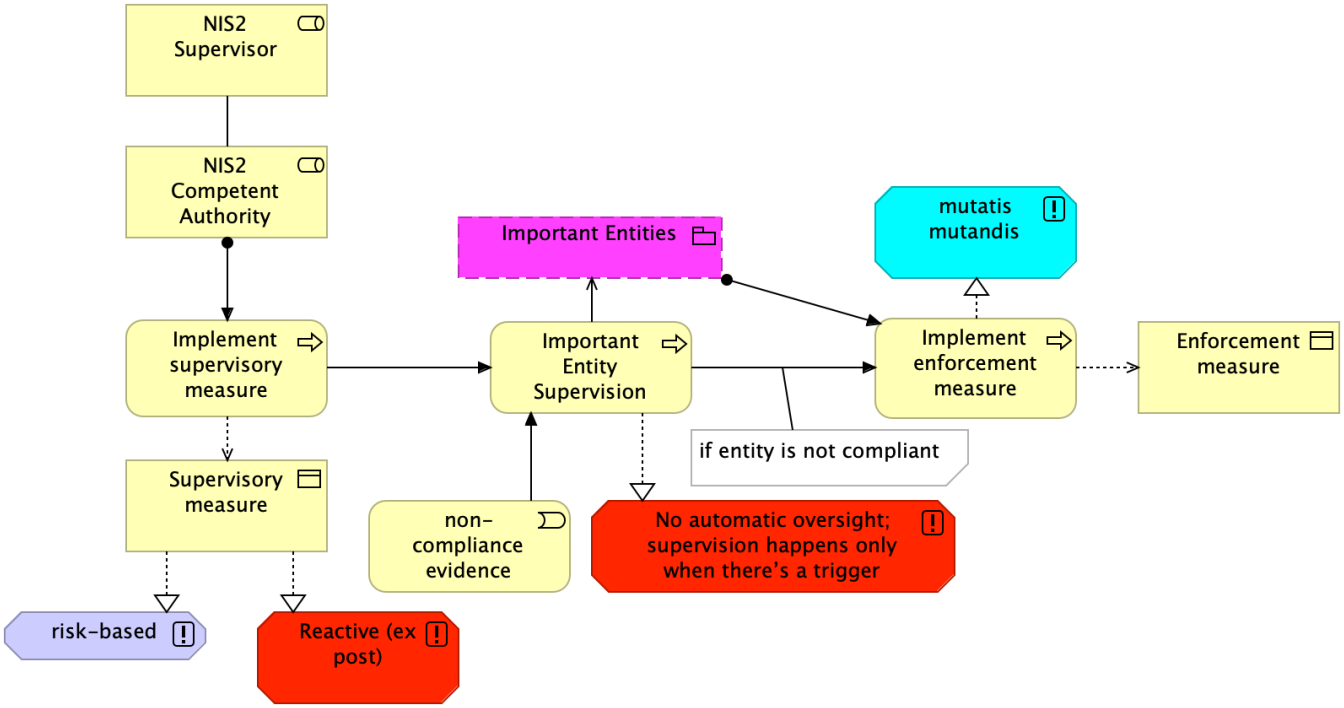
Numbering: 7.32

## Elements

| Element | Type |
|---|---|
| Automatic oversight; ongoing supervision | Principle |
| Enforcement measure | Business Object |
| Essential Entities | Grouping |
| Essential Entity Supervision | Business Process |
| Establish Enforcement Deadline | Business Function |
| Implement enforcement measure | Business Process |
| Implement supervisory measure | Business Process |
| NIS2 Competent Authority | Business Role |
| NIS2 Supervisor | Business Role |
| Notify entities concerned of their preliminary findings | Business Process |
| Proactive (ex ante) | Principle |
| Set out a detailed reasoning | Business Process |
| shall comply with the rights of the defence and take account of the circumstances of each individual case | Requirement |
| Submit observations | Business Process |
| Supervisory and enforcement measures in relation to essential entities Core | Grouping |
| Supervisory measure | Business Object |
| Suspend temporarily a certification or authorisation | Business Process |
| Temporarily prohibit key managers from their duties | Business Process |

# Supervisory and enforcement measures in relation to important entities

*No viewpoint*




## Documentation

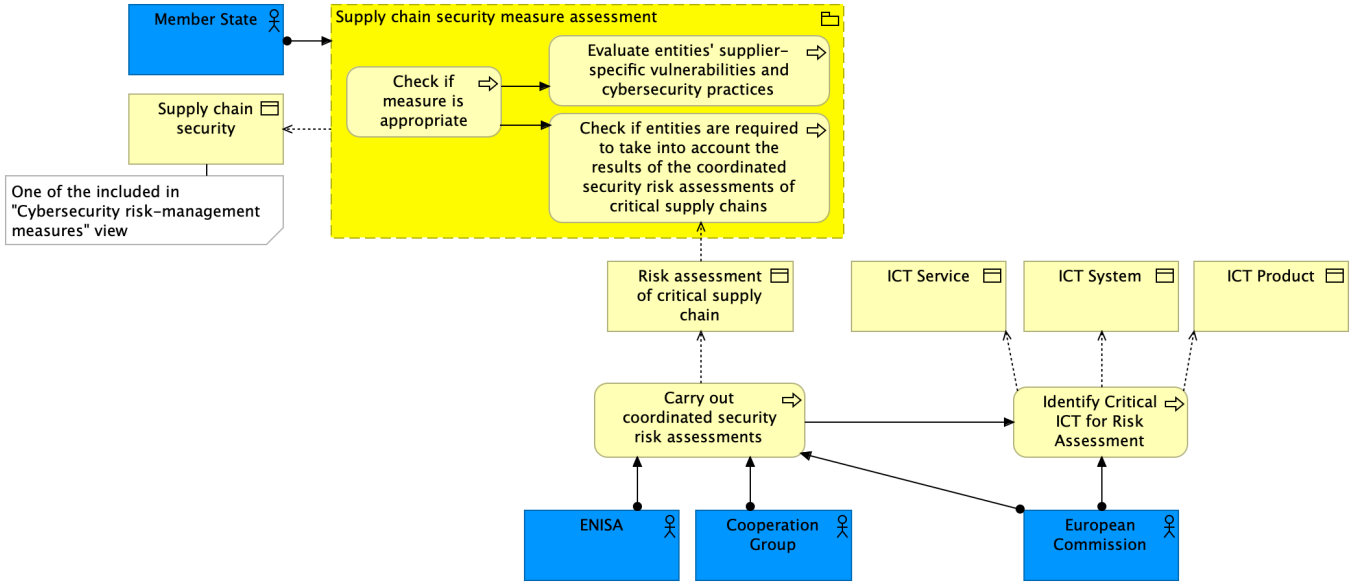
Numbering: 7.33

## Elements

| Element | Type |
|---|---|
| Enforcement measure | Business Object |
| Implement enforcement measure | Business Process |
| Implement supervisory measure | Business Process |
| Important Entities | Grouping |
| Important Entity Supervision | Business Process |
| mutatis mutandis | Principle |
| NIS2 Competent Authority | Business Role |
| NIS2 Supervisor | Business Role |
| No automatic oversight; supervision happens only when there's a trigger | Principle |
| non-compliance evidence | Business Event |
| Reactive (ex post) | Principle |
| risk-based | Principle |
| Supervisory measure | Business Object |

# Union level coordinated security risk assessments of critical supply chains

*No viewpoint*




## Documentation

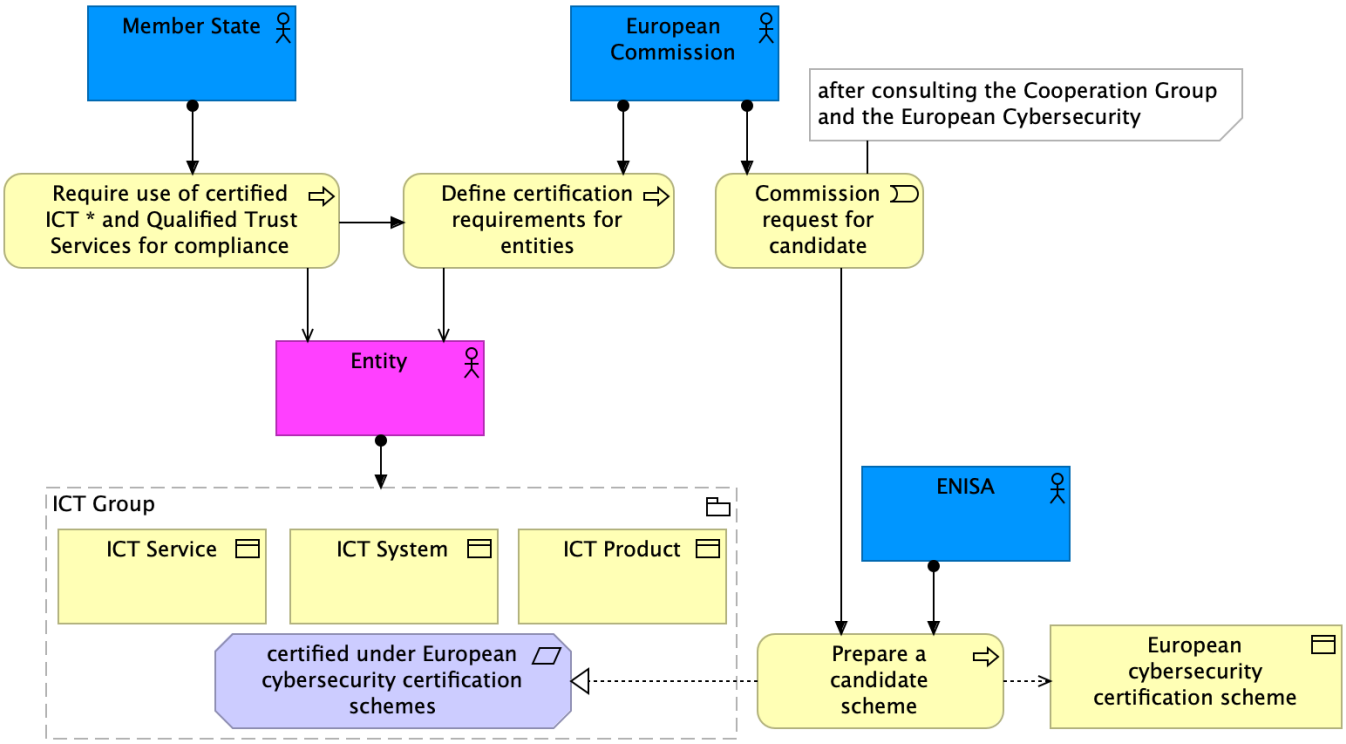
Numbering: 4.22

## Elements

| Element | Type |
|---|---|
| Carry out coordinated security risk assessments | Business Process |
| Check if entities are required to take into account the results of the coordinated security risk assessments of critical supply chains | Business Process |
| Check if measure is appropriate | Business Process |
| Cooperation Group | Business Actor |
| ENISA | Business Actor |
| European Commission | Business Actor |
| Evaluate entities' supplier-specific vulnerabilities and cybersecurity practices | Business Process |
| ICT Product | Business Object |
| ICT Service | Business Object |
| ICT System | Business Object |
| Identify Critical ICT for Risk Assessment | Business Process |
| Member State | Business Actor |
| Risk assessment of critical supply chain | Business Object |
| Supply chain security | Business Object |
| Supply chain security measure assessment | Grouping |

# Use of European cybersecurity certification schemes

*No viewpoint*




## Documentation

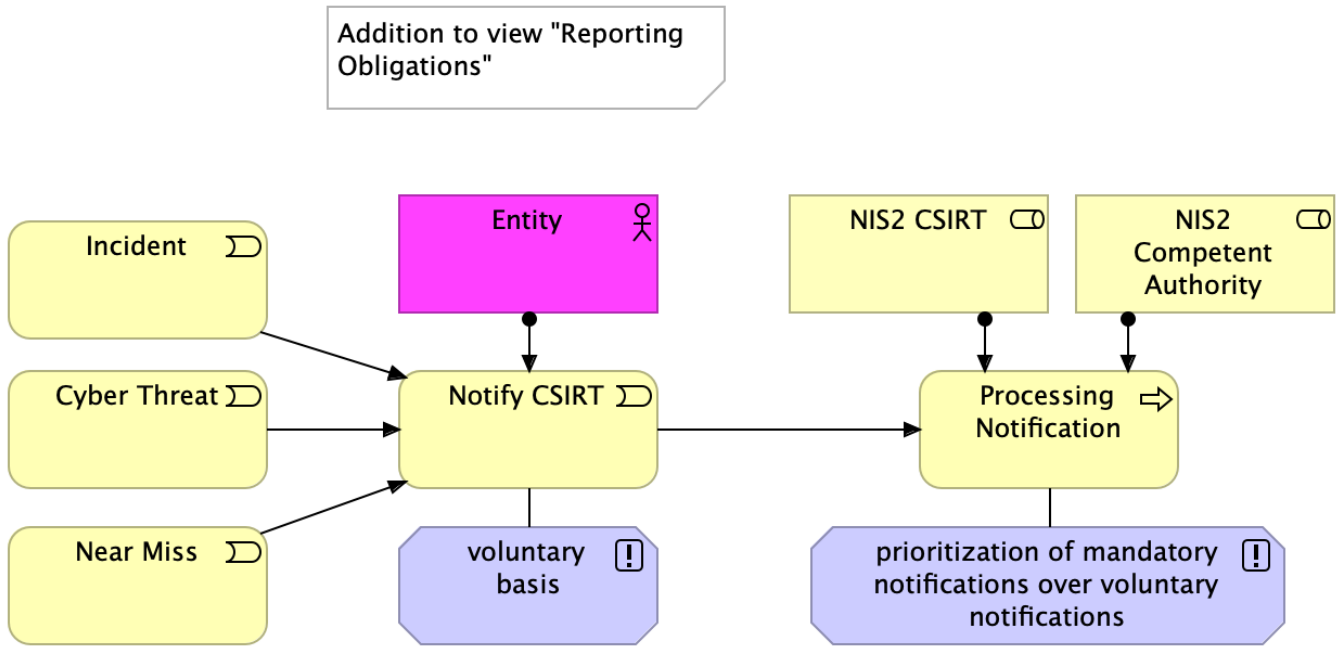
Numbering: 4.24

## Elements

| Element | Type |
|---|---|
| certified under European cybersecurity certification schemes | Requirement |
| Commission request for candidate scheme | Business Event |
| Define certification requirements for entities | Business Process |
| ENISA | Business Actor |
| Entity | Business Actor |
| European Commission | Business Actor |
| European cybersecurity certification scheme | Business Object |
| ICT Group | Grouping |
| ICT Product | Business Object |
| ICT Service | Business Object |
| ICT System | Business Object |
| Member State | Business Actor |
| Prepare a candidate scheme | Business Process |
| Require use of certified ICT * and Qualified Trust Services for compliance | Business Process |

# Voluntary notification of relevant information

*No viewpoint*




## Documentation

Numbering: 6.30

## Elements

| Element | Type |
|---|---|
| Cyber Threat | Business Event |
| Entity | Business Actor |
| Incident | Business Event |
| Near Miss | Business Event |
| NIS2 Competent Authority | Business Role |
| NIS2 CSIRT | Business Role |
| Notify CSIRT | Business Event |
| prioritization of mandatory notifications over voluntary notifications | Principle |
| Processing Notification | Business Process |
| voluntary basis | Principle |

# Business Layer

## 11h30 CNCS  receives notification

| Type | Business Event |
|---|---|

## Address and up-to-date contact details

| Type | Business Object |
|---|---|

Numbering: 1.3.4.2.b

## Address incident

| Type | Business Process |
|---|---|

Numbering: 7.31.3

## Address mobile network operators, demanding explanations for post-blackout voice and data service failures and information on backup power systems at cell towers

| Type | Business Process |
|---|---|

(Vodafone, MEO, NOS, Digi)

## Administrative Contact Information

| Type | Business Object |
|---|---|

Numbering: 5.28.2.4.d

In the event that they are different from those of the registrant.

## Administrative fines

| Type | Business Object |
|---|---|

Numbering: 7.34.2, 7.34.3

## Adopt a report

| Type | Business Process |
|---|---|

Numbering: 3.15.4

## Adopt delegation act

| Type | Business Process |
|---|---|

Numbering: 8.38.1, 8.38.2

## Adopt report

| Type | Business Process |
|---|---|

Numbering: 3.18.1

### Adopt rules of procedure

| Type | Business Process |
|---|---|

Numbering: 3.16.4

### Affected ICT products or ICT services

| Type | Business Object |
|---|---|

Numbering: 2.12.2.2.b

### Aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union

| Type | Business Object |
|---|---|

Numbering: 3.18.1.5.e

### Aggregated assessment of the outcome of peer reviews

| Type | Business Object |
|---|---|

Numbering: 3.18.1.4.d

### Aid CSIRT

| Type | Business Process |
|---|---|

### Aid transposition of NIS2

| Type | Business Process |
|---|---|

Numbering: 3.14.4.1.a

### Allow restrict access

| Type | Business Process |
|---|---|

Numbering: 5.28.5

In the event that they are different from those of the registrant.

### Answer to the notifying entity

| Type | Business Process |
|---|---|

Numbering: 4.23.5

Including initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures.

## Appoint Jurisdiction Representative

| Type | Business Function |
|---|---|

Numbering: 5.26.4

## Appoint main crisis coordinator

| Type | Business Process |
|---|---|

Numbering: 2.9.2

2. Where a Member State designates or establishes more than one cyber crisis management authority pursuant to paragraph 1, it shall clearly indicate which of those authorities is to serve as the coordinator for the management of large- scale cybersecurity incidents and crises.

## Approve cybersecurity risk-management measure

| Type | Business Process |
|---|---|

Numbering: 4.20.1

## April 28

| Type | Business Event |
|---|---|

## April 29

| Type | Business Event |
|---|---|

## April 30

| Type | Business Event |
|---|---|

## Assess compliance with measure

| Type | Business Process |
|---|---|

Numbering: 4.21.4

## Assess NCS

| Type | Business Event |
|---|---|

Numbering: 2.7.4

## Assess the consequences and impact for large-scale cybersecurity incidents and crises

| Type | Business Process |
|---|---|

Numbering: 3.16.3.3.c

## Assess the progress made

| Type | Business Process |
|---|---|

Numbering: 3.15.4

With regard to the operational cooperation

### Assessment of the development of cybersecurity capabilities inthe public and private sectors across the Union

| **Type** | Business Object |
|---|---|

Numbering: 3.18.1.2.b

### Assessment of the general level of cybersecurity awareness andcyber hygiene among citizens and entities

| **Type** | Business Object |
|---|---|

Numbering: 3.18.3.c

### Assist reporter in disclosure process

| **Type** | Business Process |
|---|---|

Numbering: 2.12.1

### Assisting reporting a vulnerability

| **Type** | Business Process |
|---|---|

Numbering: 2.12.1.2.b

### Availability of related patches

| **Type** | Business Object |
|---|---|

Numbering: 2.12.2.3.c

### Basic cyber hygiene practices and cybersecurity training

| **Type** | Business Object |
|---|---|

Numbering: 4.21.2.7.g

### Begin parallel technical investigation with CNCS and REN

| **Type** | Business Process |
|---|---|

### Biennial

| **Type** | Business Event |
|---|---|

Numbering: 3.15.4
Numbering: 3.18.1

### Biennial work programme

| **Type** | Business Event |
|---|---|

Numbering: 3.14.2, 3.14.7

## Business continuity

| Type | Business Object |
|---|---|

Numbering: 4.21.2.3.c

## by 17 October 2027 and every 36 months thereafter

| Type | Business Event |
|---|---|

Numbering: 9.40

## Carry out coordinated security risk assessments

| Type | Business Process |
|---|---|

Numbering: 4.22.1

## Carry out Cybersecurity maturity self-assessment

| Type | Business Process |
|---|---|

## Carry out Peer Review

| Type | Business Process |
|---|---|

Numbering: 3.19.1

Participation is voluntary, with cybersecurity experts designated by at least two different Member States conducting the reviews.

## Carry out Peer review self-assessment

| Type | Business Process |
|---|---|

Numbering: 3.19.5

## Check if entities are required to take into account the results of the coordinated security risk assessments of critical supply chains

| Type | Business Process |
|---|---|

## Check if measure is appropriate

| Type | Business Process |
|---|---|

## Close investigations

| Type | Business Process |
|---|---|

## Collect and maintain accurate and complete domain name registration data

| Type | Business Process |
|---|---|

Numbering: 5.28.1

## Commission request for candidate scheme

| Type | Business Event |
|---|---|

Numbering: 4.24.3

## Committee

| Type | Business Actor |
|---|---|

Shall be a committee within the meaning of Regulation (EU) No 182/2011.

## Committee Procedure

| Type | Business Interaction |
|---|---|

Numbering: 8.39.1

## Compliance Risk Assessment

| Type | Business Function |
|---|---|

Numbering: 4.21.3

Entities must assess the specific vulnerabilities and cybersecurity practices of their direct suppliers and service providers—including secure development procedures—and must also take into account the results of coordinated security risk assessments of critical supply chains under Article 22(1).

## Concludes the blackout resulted from two successive frequency instabilities in the Iberian grid, undetected in time by synchronization systems

| Type | Business Event |
|---|---|

## Confirms coordination with Portuguese authorities and the ENTSO-E to investigate causes and coordinate a gradual power restoration plan

| Type | Business Process |
|---|---|

## Consulte experts designated by each MS

| Type | Business Process |
|---|---|

Numbering: 8.38.4

## Contacts counterparts in Spain, France, and the European Commission

| Type | Business Process |
|---|---|

## Cooperation Group

| Type | Business Actor |
|---|---|

Numbering: 3.14.1, 3.14.3

## Coordinate management for large-scale cybersecurity incidents and crises

| Type | Business Process |
|---|---|

Numbering: 3.16.3.4.d

## Coordinate Procedural Arrangements

| Type | Business Interaction |
|---|---|

Numbering: 3.15.6
Numbering: 3.16.6

## Coordinator CSIRT

| Type | Business Role |
|---|---|

Numbering: 2.12.1

## Cordinate vulnerability disclosure

| Type | Business Process |
|---|---|

Numbering: 2.11.3.7.g

## Council

| Type | Business Actor |
|---|---|

## Create and maintain registry

| Type | Business Process |
|---|---|

Numbering: 5.27.1

## Create Delegation act

| Type | Business Process |
|---|---|

Numbering: 8.38.3

## Critical Entity

| Type | Business Actor |
|---|---|

Entities classified as critical under the Critical Entities Directive (EU) 2022/2557.

## Cross-Border Assistance

| Type | Business Service |
|---|---|

Numbering: 3.15.3.8.h

## Cross-border incident

| Type | Business Event |
|---|---|

## Cyber Awareness Plan

| Type | Business Object |
| --- | --- |

2.7.1.8.h

## Cyber crisis management authority

| Type | Business Role |
| --- | --- |

Numbering: 2.9.1

## Cyber Threat

| Type | Business Event |
| --- | --- |

Means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881.

## Cybersecurity Expert

| Type | Business Role |
| --- | --- |

## Cybersecurity information-sharing arrangement

| Type | Business Interaction |
| --- | --- |

Numbering: 6.29.1

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.

## Cybersecurity maturity self-assessment

| Type | Business Object |
| --- | --- |

## Cybersecurity Measures

| Type | Business Object |
| --- | --- |

Numbering: 2.7.1.5.e

## Cybersecurity risk-management measure

| Type | Business Object |
| --- | --- |

## Database of domain name registration data

| Type | Business Object |
| --- | --- |

Numbering: 5.28.1

## Define certification requirements for entities

| Type | Business Process |
| --- | --- |

Numbering: 4.24.2

## Delegated act

| Type | Business Object |
| --- | --- |

Numbering: 8.38.3

A delegated act adopted pursuant to Article 24(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

## Delegation Act enters into force

| Type | Business Event |
| --- | --- |

Numbering: 8.38.6

## Deployment of secure information-sharing tools

| Type | Business Process |
| --- | --- |

Numbering: 2.11.3.8.h

## Designate CSIRT Coordinator

| Type | Business Process |
| --- | --- |

Numbering: 2.12.1

## Designate Cybersecurity Expert

| Type | Business Process |
| --- | --- |

Numbering: 3.19.7

## Determination of main establishment for cybersecurity oversight

| Type | Business Process |
| --- | --- |

Numbering: 5.26.2

## Determine cross-border or cross-sectoral impact of the incident

| Type | Business Process |
| --- | --- |

Numbering: 4.23.1

## Determine Judisdiction

| Type | Business Function |
|---|---|

Numbering: 5.26.1, 5.26.2

## Develop a shared situational awareness for large-scale cybersecurity incidents and crises

| Type | Business Process |
|---|---|

Numbering: 3.16.3.2.b

## Develop advice and guidelines on technical areas to be considered and existing standards to be used

| Type | Business Interaction |
|---|---|

Numbering: 4.25.2

after consulting relevant stakeholders

## Develop and maintain European Vulnerability DB

| Type | Business Process |
|---|---|

Numbering: 2.12.2

## Develop EU-CyCLONe Work Assessment Report

| Type | Business Process |
|---|---|

Numbering: 3.16.7

## Develop methodology

| Type | Business Interaction |
|---|---|

Numbering: 3.18.3

ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables, such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1, point (e).

## Discuss and identify further forms of operational cooperation

| Type | Business Process |
|---|---|

Numbering: 3.15.3.10.j

in relation to:
(i) categories of cyber threats and incidents;
(ii) early warnings;
(iii) mutual assistance;
(iv) principles and arrangements for coordination in response to cross-border risks and incidents;

(v) contribution to the national large-scale cybersecurity incident and crisis response plan referred to in Article 9(4) at the request of a Member State;

### Discuss capabilities and preparedness

| Type | Business Process |
|---|---|

Numbering: 3.15.3.1.a, 3.15.3.7.g, 3.15.3.13.m

### Discuss mutual assistance

| Type | Business Process |
|---|---|

Numbering: 3.14.4.10.j

### Discuss national large-scale cybersecurity incident and crisis response plans

| Type | Business Process |
|---|---|

Numbering: 3.16.3.5.e

### DNS service provider

| Type | Business Role |
|---|---|

### Domain Name

| Type | Business Object |
|---|---|

Numbering: 5.28.2.1.a

### Domain name registration services Provider

| Type | Business Role |
|---|---|

### Doubles “black start” capacity with additional power plants able to restart autonomously

| Type | Business Process |
|---|---|

### Draft reports on the findings and conclusions

| Type | Business Process |
|---|---|

Numbering: 3.19.9

with Member States able to comment and potentially publish the reports.

### Early warning of potential malicious or cross-border incident

| Type | Business Process |
|---|---|

Numbering: 4.23.4.1.a

### Enforcement measure

| Type | Business Object |
|---|---|

Numbering: 7.32.4
Numbering: 7.33.4
Numbering: 7.37.1.1.a

## Enhanced Cyber Coordination Policy

| **Type** | Contract |
|---|---|

Numbering: 2.7.1.7.g

## ENISA

| **Type** | Business Actor |
|---|---|

## ENISA Cybersecurity Policy Recommendations

| **Type** | Contract |
|---|---|

Numbering: 3.18.2

The report shall include particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union, and a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.

## Entity

| **Type** | Business Actor |
|---|---|

## Entity Name

| **Type** | Business Object |
|---|---|

Numbering: 1.3.4.1.a
Numbering: 5.27.2.1.a

## Entity supervisory and enforcement coordination and cooperation

| **Type** | Business Interaction |
|---|---|

Numbering: 7.37.1

That cooperation shall entail, at least, that:

(a) the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken;
(b) a competent authority may request another competent authority to take supervisory or enforcement measures;
(c) a competent authority shall, upon receipt of a substantiated request from another competent authority, provide the other competent authority with assistance proportionate to its own resources so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent

manner.

## ENTSO-E

| Type | Business Actor |
| --- | --- |

European Network of Transmission System Operators for Electricity

## Essential Entity Supervision

| Type | Business Process |
| --- | --- |

Numbering: 7.32.2

## Establish and publish domain data verification policies

| Type | Business Process |
| --- | --- |

Numbering: 5.28.3

## Establish Competent Authority

| Type | Business Process |
| --- | --- |

Numbering: 2.8.1, 2.8.5

## Establish CSIRT

| Type | Business Process |
| --- | --- |

Numbering: 2.10.1, 2.10.2

## Establish Cyber crisis management authority

| Type | Business Process |
| --- | --- |

Numbering: 2.9.1

## Establish Enforcement Deadline

| Type | Business Function |
| --- | --- |

Numbering: 7.32.5

## Establish KPIs

| Type | Business Process |
| --- | --- |

Numbering: 2.7.4

## Establish NCS

| Type | Business Process |
| --- | --- |

Numbering: 2.7.3

## Establish SPC

| Type | Business Process |
| --- | --- |

Numbering: 2.8.3, 2.8.5

## Establish supervisory methodologies

| Type | Business Process |
| --- | --- |

Numbering: 7.31.2

## Establishments addresses

| Type | Business Object |
| --- | --- |

Numbering: 5.27.2.3.c

## EU CERT-EU

| Type | Business Actor |
| --- | --- |

## EU CSIRTs Coordinator

| Type | Business Role |
| --- | --- |

## EU-CyCLONe

| Type | Business Actor |
| --- | --- |

European cyber crisis liaison organisation network.

## EU-CyCLONe Work Assessment Report

| Type | Business Object |
| --- | --- |

Numbering: 3.16.7

## European Commission

| Type | Business Actor |
| --- | --- |

## European cybersecurity certification scheme

| Type | Business Object |
| --- | --- |

Numbering: 4.24.3

## European External Action Service

| Type | Business Actor |
| --- | --- |

## European Parliament

| Type | Business Actor |
| --- | --- |

## European Union

| Type | Business Actor |
|---|---|

## European Vulnerability Database

| Type | Business Service |
|---|---|

Numbering: 2.12.2

## Evaluate entities' supplier-specific vulnerabilities and cybersecurity practices

| Type | Business Process |
|---|---|

## every 18 months

| Type | Business Event |
|---|---|

Numbering: 3.16.7

## every six months

| Type | Business Event |
|---|---|

Numbering: 4.23.9

## every three months

| Type | Business Event |
|---|---|

Numbering: 4.23.9

## Facilitate establishment

| Type | Business Process |
|---|---|

Numbering: 6.29.3

## failure in the national power grid

| Type | Business Event |
|---|---|

## File a formal complaint with the Public Prosecutor’s Office requesting investigation

| Type | Business Process |
|---|---|

## Final Report

| Type | Business Object |
|---|---|

Numbering: 4.23.4.4.d

Includes:
(i) a detailed description of the incident, including its severity and impact;
(ii) the type of threat or root cause that is likely to have triggeredthe incident;
(iii) applied and ongoing mitigation measures;

(iv) where applicable, the cross-border impact of the incident;

### Forward Notification to SPC

| Type | Business Process |
|---|---|

Numbering: 2.13.3

### forward to ENISA

| Type | Business Event |
|---|---|

Numbering: 5.27.4

### Gather Cooperation Group and CSIRTs Network reports

| Type | Business Process |
|---|---|

Numbering: 9.40

### GDPR Supervisory Authority

| Type | Business Role |
|---|---|

### Governance Framework

| Type | Business Service |
|---|---|

Numbering: 2.7.1.2.b and 2.7.1.3.c

### Guarantee CSIRTs Cooperation

| Type | Business Process |
|---|---|

Numbering: 3.15.3.9.i

### Guidance on the development and implementation of policies on coordinated vulnerability disclosure

| Type | Business Process |
|---|---|

Numbering: 3.14.4.2.b

### Handle and coordinate incident

| Type | Business Process |
|---|---|

Numbering: 2.11.3.3.c

### Human resources security, access control policies and asset management

| Type | Business Object |
|---|---|

Numbering: 4.21.2.9.i

## ICT Product

| Type | Business Object |
|---|---|

## ICT Service

| Type | Business Object |
|---|---|

## ICT System

| Type | Business Object |
|---|---|

## Identify and contact the entities concerned

| Type | Business Process |
|---|---|

Numbering: 2.12.1.1.a

## Identify Critical ICT for Risk Assessment

| Type | Business Process |
|---|---|

Numbering: 4.22.2

## Implement enforcement measure

| Type | Business Process |
|---|---|

Numbering: 7.32.4
Numbering: 7.33.4

## Implement plan

| Type | Business Function |
|---|---|

Numbering: 2.9.4

## Implement supervisory measure

| Type | Business Process |
|---|---|

Numbering: 7.32.2
Numbering: 7.33.2

## Important Entity

| Type | Business Actor |
|---|---|

Entities designated as important by Member States under Article 2(2), points (b) to (e).

## Important Entity Supervision

| Type | Business Process |
|---|---|

Numbering: 7.33.2

## Incident

| Type | Business Event |
|---|---|

## Incident Coordination Service

| Type | Business Service |
|---|---|

Numbering: 2.7.1.3.c

## Incident handling

| Type | Business Object |
|---|---|

Numbering: 4.21.2.2.b

## Incident notification (update)

| Type | Business Event |
|---|---|

Numbering: 4.23.4.2.b

## Increase the level of preparedness of the management of large-scale cybersecurity incidents and crises

| Type | Business Process |
|---|---|

Numbering: 3.16.3.1.a

## Inform findings on notifications

| Type | Business Process |
|---|---|

Numbering: 4.23.9

## inform relevant GDPR Supervisory Authority

| Type | Business Event |
|---|---|

Numbering: 7.35.1, 7.35.3

## Information from SPC

| Type | Business Event |
|---|---|

Numbering: 5.27.1

## Intermediate Report

| Type | Business Object |
|---|---|

Numbering: 4.23.4.3.c

## International Agreement

| Type | Contract |
|---|---|

Numbering: 3.17

## International Agreements Conclusion

| Type | Business Service |
|---|---|

Numbering: 3.17

## International Cybersecurity Assistance

| Type | Business Service |
|---|---|

Numbering: 2.10.7, 2.10.8

## International/Third Country Organization

| Type | Business Actor |
|---|---|

## IP ranges

| Type | Business Object |
|---|---|

Numbering: 5.27.2.6.f

## Issue renewed statements reaffirming no evidence of cyberattacks and urges media outlets to rely only on official sources

| Type | Business Process |
|---|---|

## Issues fine on Entity

| Type | Business Process |
|---|---|

## Issues statements denying signs of cyberattacks and warning against misinformation on social media

| Type | Business Process |
|---|---|

## June 25

| Type | Business Event |
|---|---|

## Jurisdiction Representative

| Type | Business Role |
|---|---|

## Keep updated a list of SPCs publicly available

| Type | Business Process |
|---|---|

Numbering: 2.8.6

## Large-scale cybersecurity incident or crise

| Type | Business Event |
|---|---|

## Large-scale cybersecurity incident or crise MS request

| Type | Business Event |
|---|---|

Numbering: 3.16.3.5.e

### lawful and duly substantiated request

| Type | Business Event |
|---|---|

Numbering: 5.28.5

### Lay down rules and compliance to fines

| Type | Business Process |
|---|---|

Numbering: 7.34.7, 7.34.8

### Lay down rules and take measures

| Type | Business Process |
|---|---|

Numbering: 7.36

### Legitimate access seeker

| Type | Business Role |
|---|---|

### Liason Function

| Type | Business Role |
|---|---|

Numbering: 2.8.4

Each single point of contact shall 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.

### List of involved actors

| Type | Business Object |
|---|---|

Numbering: 2.7.1.6.f

### List of the Member States where they provide services

| Type | Business Object |
|---|---|

Numbering: 1.3.4.4.d

Where applicable, a list of the Member States where they provide services falling within the scope of this Directive.

### Make the identity of the Competent Authority public

| Type | Business Event |
|---|---|

Numbering: 2.8.6

## Management Body

| Type | Business Role |
|---|---|

## May 1

| Type | Business Event |
|---|---|

## May 9

| Type | Business Event |
|---|---|

## Medium-sized enterprise

| Type | Business Actor |
|---|---|

Medium-sized enterprises in Annex I and II sectors.

## Member State

| Type | Business Actor |
|---|---|

## Member State Representative

| Type | Business Actor |
|---|---|

## Monitor cyber threats and incidents

| Type | Business Function |
|---|---|

Numbering: 2.11.3.1.a

## MS participation notification

| Type | Business Event |
|---|---|

Numbering: 3.19.4

## MS request

| Type | Business Event |
|---|---|

Numbering: 5.28.2

## MSs where provides services

| Type | Business Object |
|---|---|

Numbering: 5.27.2.5.e

## National Cybersecurity Strategy

| Type | Product |
|---|---|

Numbering: 2.7.1

## National large-scale cybersecurity incident and crisis response plan

| Type | Business Object |
|---|---|

Numbering: 2.9.4

## Natural or legal person

| Type | Business Actor |
|---|---|

## NCS Assessment

| Type | Business Function |
|---|---|

Numbering: 2.7.4

## Near Miss

| Type | Business Event |
|---|---|

Means 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

## Negotiate disclosure timelines and managing vulnerabilities that affect multiple entities

| Type | Business Process |
|---|---|

Numbering: 2.12.1.3.c

## NIS2 Competent Authority

| Type | Business Role |
|---|---|

## NIS2 CSIRT

| Type | Business Role |
|---|---|

## NIS2 CSIRTs Network

| Type | Business Role |
|---|---|

## NIS2 Review Report

| Type | Business Object |
|---|---|

Numbering: 9.40

## NIS2 Single Point of Contact

| Type | Business Role |
|---|---|

Numbering: 2.8.3

An entity (can be the same as the Competent Authority) that facilitates cooperation between:
- Authorities in different Member States
- National authorities across sectors
- The European Commission and ENISA

## NIS2 Supervisor

| Type | Business Role |
|---|---|

Numbering: 2.8.1
Numbering: 7.31.1

Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive.

Supervisory tasks referred to in Chapter VII

## non-compliance evidence

| Type | Business Event |
|---|---|

Numbering: 7.33.2

## Notification of significant incidents, incidents, cyber threats or near misses

| Type | Business Event |
|---|---|

Numbering: 2.13.2

## Notify changes to Competent Authority

| Type | Business Event |
|---|---|

Numbering: 5.27.3

## Notify Commission of CSIRT

| Type | Business Event |
|---|---|

Numbering: 2.10.9

## Notify Commission of measures

| Type | Business Event |
|---|---|

Numbering: 7.36

## Notify Commission of NCS

| Type | Business Event |
|---|---|

Numbering: 2.7.3

### Notify Commission of SPC

| Type | Business Event |
|---|---|

Numbering: 2.8.6

### Notify competent authority of participation or withdrawal

| Type | Business Event |
|---|---|

Numbering: 6.29.4

### Notify Cooperation Group

| Type | Business Event |
|---|---|

Numbering: 3.15.4

### Notify CSIRT

| Type | Business Event |
|---|---|

Numbering: 4.23.1
Numbering: 6.30.1

### Notify entities concerned of their preliminary findings

| Type | Business Process |
|---|---|

Numbering: 7.32.8

### Notify of coordinator and plan

| Type | Business Event |
|---|---|

Numbering: 2.9.5

### Notify other MSs and ENISA

| Type | Business Event |
|---|---|

Numbering: 4.23.6

### Notify Parliament and Council of delegated act

| Type | Business Event |
|---|---|

Numbering: 8.38.5

### Notify recipients of service

| Type | Business Event |
|---|---|

Numbering: 4.23.2

### Notify report to Parliament and Council

| Type | Business Event |
|---|---|

Numbering: 9.40

### Notify SPC of cross-* incident

| Type | Business Event |
|---|---|

Numbering: 4.23.1

### Operational Cooperation Information

| Type | Business Object |
|---|---|

### Order a technical-strategic review to urgently modernize the SIRESP emergency communications system

| Type | Business Process |
|---|---|

### Oversee implementation

| Type | Business Process |
|---|---|

Numbering: 4.20.1

### Participate in peer reviews

| Type | Business Process |
|---|---|

Numbering: 2.10.5

### Peer review

| Type | Business Interaction |
|---|---|

Numbering: 3.19.1

The peer reviews shall cover at least one of the following:
(a) the level of implementation of the cybersecurity risk-management measures and reporting obligations laid down in Articles 21 and 23;
(b) 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;
(c) the operational capabilities of the CSIRTs;
(d) the level of implementation of mutual assistance referred to in Article 37;
(e) the level of implementation of the cybersecurity information-sharing arrangements referred to in Article 29;
(f) specific issues of cross-border or cross-sector nature.

It involves multiple MSs working together to evaluate and enhance cybersecurity measures.

### Peer review self-assessment

| Type | Business Object |
|---|---|

Numbering: 3.19.5

## Penalty by infringements of national measures

| Type | Business Event |
| --- | --- |

Numbering: 7.36

## People Training

| Type | Business Function |
| --- | --- |

Numbering: 4.20.2

## Perform forensic and risk analysis

| Type | Business Process |
| --- | --- |

Numbering: 2.11.3.4.d

## Periodic penalty payments

| Type | Business Object |
| --- | --- |

Numbering: 7.34.6

## personal data breach incident

| Type | Business Event |
| --- | --- |

Numbering: 7.31.3
Numbering: 7.35.1

## Policies and procedures regarding the use of cryptography and, where appropriate, encryption

| Type | Business Object |
| --- | --- |

Numbering: 4.21.2.8.h

## Policies and procedures to assess the effectiveness of cybersecurity risk-management measures

| Type | Business Object |
| --- | --- |

Numbering: 4.21.2.6.f

## Policies on risk analysis and information system security

| Type | Business Object |
| --- | --- |

Numbering: 4.21.2.1.a

## Preliminary report

| Type | Business Object |
| --- | --- |

Recommending:

- Improvement of public alert systems (SMS, Cell Broadcast).
- Diversification of emergency call routing (112).
- Assessment of battery and generator autonomy in cell sites.
- Adoption of renewable energy sources in critical infrastructure.

### Prepare a candidate scheme

| Type | Business Process |
|---|---|

Numbering: 4.24.3

### Processing Notification

| Type | Business Process |
|---|---|

Numbering: 6.30.2

### Progress Report

| Type | Business Object |
|---|---|

Numbering: 3.15.4

### Promote standards and relevant technical specifications usage

| Type | Business Process |
|---|---|

Numbering: 4.25.1

### Propose possible mitigation measures

| Type | Business Process |
|---|---|

Numbering: 3.16.3.3.c

### Provide alerts and incident response

| Type | Business Process |
|---|---|

Numbering: 2.11.3.2.b

### Provider of public electronic communications network/service

| Type | Business Role |
|---|---|

### Provider or Manufacturer

| Type | Business Role |
|---|---|

### PT Anacom

| Type | Business Actor |
|---|---|

May 1

## PT CERT.PT

| Type | Business Actor |
|---|---|

## PT Citizens for Cybersecurity (CpC)

| Type | Business Actor |
|---|---|

## PT CNCS

| Type | Business Actor |
|---|---|

## PT GNS

| Type | Business Actor |
|---|---|

## PT Government

| Type | Business Actor |
|---|---|

## PT RNCSIRT

| Type | Business Actor |
|---|---|

## Public administration entity

| Type | Business Actor |
|---|---|

## Publication in the Official Journal

| Type | Business Process |
|---|---|

Numbering: 8.38.3

## Publish a preliminary report

| Type | Business Process |
|---|---|

## QTS Provider

| Type | Business Role |
|---|---|

## Raise objection

| Type | Business Event |
|---|---|

Numbering: 8.38.6

Parliament and Council have 2 months to raise objections

## Registrant Contact Information

| Type | Business Object |
|---|---|

Numbering: 5.28.2.3.c

## Registration Date

| Type | Business Object |
| --- | --- |

Numbering: 5.28.2.2.b

## Registry of entities

| Type | Business Object |
| --- | --- |

Numbering: 5.27.1

## Relevant assets

| Type | Business Object |
| --- | --- |

Numbering: 2.7.1.4.d

## Relevant Information

| Type | Business Event |
| --- | --- |

## Relevant sector and subsector

| Type | Business Object |
| --- | --- |

Numbering: 1.3.4.3.c

Where applicable, the relevant sector and subsector referred to in Annex I or II;

## Relevant sector, subsector and type

| Type | Business Object |
| --- | --- |

Numbering: 5.27.2.2.b

## Relevant Secure Information Exchange

| Type | Business Process |
| --- | --- |

Numbering: 3.14.4.3.c, 3.14.4.4.d, 3.14.4.5.e, 3.14.4.6.f, 3.14.4.13.m, 3.14.4.14.n
Numbering: 3.15.3.2.b, 3.15.3.3.c, 3.15.3.4.d, 3.15.3.14.n
Numbering: 3.16.3

## Report incident impact information

| Type | Business Process |
| --- | --- |

Numbering: 4.23.4.3.c, 4.23.4.5.e

## Report management and trends

| Type | Business Process |
| --- | --- |

Numbering: 3.16.5

## Report of an alleged sale of privileged access to energy infrastructures on the dark web, highlighting a possible link to the blackout

| Type | Business Event |
| --- | --- |

(advertised for $30,000 by “DarkWebInformer”)

## Report on the state of cybersecurity

| Type | Business Object |
| --- | --- |

Numbering: 3.18.1

## Report operations and activities

| Type | Business Process |
| --- | --- |

Numbering: 3.15.3.11.k

## Report request

| Type | Business Event |
| --- | --- |

Numbering: 4.23.4.3.c

## Reported potential vulnerability on ICT products or ICT services

| Type | Business Event |
| --- | --- |

Numbering: 2.12.1

## Reported vulnerability

| Type | Business Event |
| --- | --- |

Numbering: 2.12.1

## Representative of relevant stakeholder

| Type | Business Role |
| --- | --- |

## Request

| Type | Business Event |
| --- | --- |

Numbering: 4.20.2

## Request for mutual assistance

| Type | Business Event |
| --- | --- |

Numbering: 5.26.5

## Request for written procedure

| Type | Business Event |
| --- | --- |

Numbering: 8.39.1

## Request of an individual CSIRT

| Type | Business Event |
|---|---|

Numbering: 3.15.3.6.f, 3.15.3.13.m

## Request technical report on selected topics

| Type | Business Event |
|---|---|

Numbering: 3.14.6

## Require use of certified ICT * and Qualified Trust Services for compliance

| Type | Business Process |
|---|---|

Numbering: 4.24.1

## Responsible Disclosure Management

| Type | Business Service |
|---|---|

Numbering: 2.12.1

Diligent follow-up action.

## Review NIS2 functioning

| Type | Business Process |
|---|---|

Numbering: 9.40

## Revoke Delegation act

| Type | Business Event |
|---|---|

Numbering: 8.38.3

A decision to revoke shall put an end to the delegation of the power specified in that decision.

## Risk

| Type | Business Event |
|---|---|

## Risk Assessment

| Type | Business Object |
|---|---|

Numbering: 2.7.1.4.d

## Risk assessment of critical supply chain

| Type | Business Object |
|---|---|

Numbering: 4.22.1

## Secretariat Provider

| Type | Business Role |
|---|---|

Numbering: 3.14.3
Numbering: 3.15.2
Numbering: 3.16.2

## Secure and authenticated communications

| Type | Business Object |
|---|---|

Numbering: 4.21.2.10.j

## Secure network and information system development and vulnerability management

| Type | Business Object |
|---|---|

Numbering: 4.21.2.5.e

## Security Incident

| Type | Business Event |
|---|---|

## Security Operations Centre

| Type | Business Role |
|---|---|

SOC

## Set out a detailed reasoning

| Type | Business Process |
|---|---|

Numbering: 7.32.8

## Severity

| Type | Business Object |
|---|---|

Numbering: 2.12.2.12.b

## Significant Cyber Threat

| Type | Business Event |
|---|---|

Means 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.

## Significant Incident

| Type | Business Event |
|---|---|

## SP INCIBE

| Type | Business Actor |
| --- | --- |

Spain’s National Cybersecurity Institute

## Starts installation of battery systems in critical infrastructure (hospitals, communication stations)

| Type | Business Process |
| --- | --- |

## Strategic Guidance Provision

| Type | Business Service |
| --- | --- |

Numbering: 3.14.4.12.l

## Strategic Level Experience Report

| Type | Business Object |
| --- | --- |

Numbering: 3.14.4.18.r

## Submit and present report

| Type | Business Process |
| --- | --- |

Numbering: 3.18.1

## Submit Entity information

| Type | Business Process |
| --- | --- |

Numbering: 5.27.3

## Submit observations

| Type | Business Process |
| --- | --- |

Numbering: 7.32.5

## Submit Summary Report

| Type | Business Process |
| --- | --- |

Numbering: 4.23.9

## Summary Report

| Type | Business Object |
| --- | --- |

Numbering: 4.23.9

Including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses.

## Supervise compliance and enforce measures on public administration entities

| Type | Business Process |
| --- | --- |

Numbering: 7.31.4

## Supervisory measure

| Type | Business Object |
| --- | --- |

Numbering: 7.32.2
Numbering: 7.33.2
Numbering: 7.37.1.1.a

## supervisory task

| Type | Business Event |
| --- | --- |

Numbering: 7.31.2

## Supply chain security

| Type | Business Object |
| --- | --- |

Numbering: 4.21.2.4.d

## Support decision-making at political level

| Type | Business Process |
| --- | --- |

Numbering: 3.16.3.4.d

## Suspend temporarily a certification or authorisation

| Type | Business Process |
| --- | --- |

Numbering: 7.32.5.1.a

## Take appropriate and proportionate corrective measures

| Type | Business Process |
| --- | --- |

Numbering: 4.21.4

## Take cybersecurity risk-management measure

| Type | Business Process |
| --- | --- |

Numbering: 4.20.1
Numbering: 4.21.1

## Take security risk assessments

| Type | Business Process |
| --- | --- |

Numbering: 3.14.4.9.i

## Take Standardised Practices for Cooperation

| Type | Business Process |
|---|---|

Numbering: 2.11.5

2.11.5.1.a - incident-handling procedures;
2.11.5.2 .b - crisis management; and
2.11.5.3 .c - coordinated vulnerability disclosure under Article 12(1).

## Take supervisory and enforcement measures

| Type | Business Process |
|---|---|

Numbering: 5.26.5

## Technical report request

| Type | Business Process |
|---|---|

Numbering: 3.14.6

## Temporarily prohibit key managers from their duties

| Type | Business Process |
|---|---|

Numbering: 7.32.5.2.b

## Terminate procedure

| Type | Business Event |
|---|---|

Numbering: 8.39.3

Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of th committee so decides or a committee member so requests.

## Third countries’ national CSIRT

| Type | Business Role |
|---|---|

## Third country security incident

| Type | Business Event |
|---|---|

Numbering: 2.10.7

## TLD name registry

| Type | Business Role |
|---|---|

## Top-level domain name registry

| Type | Business Role |
|---|---|

## Trusted User Guidance

| Type | Business Object |
| --- | --- |

Numbering: 2.12.2.3.c

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.

## Union-level cybersecurity risk assessment

| Type | Business Object |
| --- | --- |

Numbering: 3.18.1.1.a

## Up-to-date contact details

| Type | Business Object |
| --- | --- |

Numbering: 5.27.2.4.d

## Update NCS

| Type | Business Process |
| --- | --- |

Numbering: 2.7.4

## Vulnerability Information

| Type | Business Object |
| --- | --- |

Numbering: 2.12.2.1.a

# Motivation

## achieve cybersecurity strategy

| Type | Goal |
| --- | --- |

Numbering: 2.7.1

## Active Cyber Protection Policy

| Type | Requirement |
| --- | --- |

Numbering: 2.7.2.10.j

## Adequate and Trained Staffing

| Type | Requirement |
| --- | --- |

Numbering: 2.11.1.5.e

## adopt the necessary technical and organisational measures to ensure the security and integrity of the European DB

| Type | Requirement |
| --- | --- |

Numbering: 2.12.2

## aims to prevent, detect, respond to or recover from incidents or to mitigate their impact

| Type | Goal |
| --- | --- |

Numbering: 6.29.1.1.a

## all-hazards approach

| Type | Requirement |
| --- | --- |

Numbering: 4.21.2

## anonymity

| Type | Requirement |
| --- | --- |

## appropriate cooperation

| Type | Requirement |
| --- | --- |

Numbering: 2.13.1, 2.13.4

## Automatic oversight; ongoing supervision

| Type | Principle |
| --- | --- |

certified under European cybersecurity certification schemes

| Type | Requirement |
| --- | --- |

Numbering: 4.24.2

contribute to the development of confidence and trust and to promote swift and effective operational cooperation among MSs

| Type | Goal |
| --- | --- |

Numbering: 3.15.1

contribute to the security, stability, and resilience of the DNS

| Type | Goal |
| --- | --- |

Numbering: 5.28.1

contributes to the deployment of secure information-sharing tools

| Type | Requirement |
| --- | --- |

Numbering: 2.10.3

cooperation with eIDAS2 authorities

| Type | Requirement |
| --- | --- |

Numbering: 2.13.4

coordinated vulnerability disclosure

| Type | Goal |
| --- | --- |

Numbering: 2.12

cross-border cooperation

| Type | Value |
| --- | --- |

Numbering: 2.8.4

cross-sectoral cooperation

| Type | Value |
| --- | --- |

Numbering: 2.8.4

cyber crisis management procedures

| Type | Value |
| --- | --- |

Numbering: 2.9.4.3.c

Cyber Education & Awareness Program

| Type | Requirement |
| --- | --- |

Numbering: 2.7.2.6.f

### Cybersecurity

| Type | Value |
|---|---|

Numbering: 1.1.1

### Cybersecurity  in Portugal

| Type | Value |
|---|---|

### Cybersecurity Research & Innovation

| Type | Requirement |
|---|---|

Numbering: 2.7.2.7.g

### do on regular basis and at least every five years

| Type | Requirement |
|---|---|

Numbering: 2.7.4

### effective, proportionate and dissuasive

| Type | Principle |
|---|---|

Numbering: 7.34.1

### enabling entities and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services

| Type | Goal |
|---|---|

Numbering: 2.12.2

### Enhance cybersecurity trust and capabilities across MSs

| Type | Goal |
|---|---|

Numbering: 3.19.1

### enhance the level of cybersecurity

| Type | Driver |
|---|---|

Numbering: 6.29.1.2.b

### Enhance the overall level of cybersecurity across the European Union

| Type | Driver |
|---|---|

Numbering: 1.1.1

Ensure a proportional level of security based on risk exposure, entity size, and potential impact

| Type | Principle |
| --- | --- |

Numbering: 4.21.1

ensure effective, efficient and secure cooperation of their representatives in the Cooperation Group

| Type | Requirement |
| --- | --- |

Numbering: 3.14.5

ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network

| Type | Goal |
| --- | --- |

Numbering: 2.10.6

Entities already covered by equivalent EU cybersecurity laws are exempt, while others remain under this Directive

| Type | Constraint |
| --- | --- |

Numbering: 1.4

Entities and authorities must share cybersecurity threat intelligence

| Type | Requirement |
| --- | --- |

Entities must comply with reporting obligations on security incidents

| Type | Requirement |
| --- | --- |

Entities must implement cybersecurity risk-management measures

| Type | Requirement |
| --- | --- |

exceptions from Article 26 1.

| Type | Constraint |
| --- | --- |

Numbering: 5.26.1

exchange on a voluntary basis relevant cybersecurity information

| Type | Principle |
| --- | --- |

Numbering: 6.29.2

For significant cross-border or cross-sector incidents, Member States must promptly notify their single points of contact

| Type | Requirement |
| --- | --- |

## GDPR

| Type | Requirement |
|---|---|

Numbering: 3.17
Numbering: 5.28.1

## ICT Cybersecurity Procurement Standards

| Type | Requirement |
|---|---|

Numbering: 2.7.2.2.b

## ICT Supply Chain Security Policy

| Type | Requirement |
|---|---|

Numbering: 2.7.2.1.a

## If the GDPR supervisory authority has already fined the entity for the same incident, the competent authority cannot also impose a fine under NIS2 for the same conduct. However, it can still apply other enforcement measures (like warnings, orders, audits).

| Type | Constraint |
|---|---|

Numbering: 7.35.2

## If the relevant GDPR supervisory authority is in another country, the competent authority must notify its own national GDPR authority about the potential data breach

| Type | Requirement |
|---|---|

Numbering: 7.35.3

## information exchange

| Type | Requirement |
|---|---|

Numbering: 2.13.5

## Information Sharing

| Type | Goal |
|---|---|

Numbering: 1.1.2.c

## Joint supervisory actions

| Type | Principle |
|---|---|

Numbering: 7.37.2

## Manage the risks posed to the security of network and information systems

| Type | Goal |
|---|---|

Numbering: 4.21.2

### Management of large-scale cybersecurity incidents and crises

| Type | Value |
|---|---|

Numbering: 2.9.1

### Maturity Level 1 - Initial / Ad-hoc

| Type | Value |
|---|---|

### Maturity Level 2 - Developing

| Type | Value |
|---|---|

### Maturity Level 3 - Defined

| Type | Value |
|---|---|

### Maturity Level 4 - Managed

| Type | Value |
|---|---|

### Maturity Level 5 - Optimized

| Type | Value |
|---|---|

### Member States may allow their competent authorities to prioritise supervisory tasks

| Type | Requirement |
|---|---|

### Member States shall adopt a national cybersecurity strategy outlining objectives, resources, and measures to ensure high cybersecurity levels

| Type | Requirement |
|---|---|

### Member States shall enable relevant entities to voluntarily share cybersecurity information, including threats, vulnerabilities, and attack indicators

| Type | Requirement |
|---|---|

### Member States shall ensure entities implement measures to manage cybersecurity risks and minimize incident impact

| Type | Requirement |
|---|---|

### Member States shall ensure entities promptly notify CSIRTs or authorities of significant incidents

| Type | Requirement |
|---|---|

## Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive

| Type | Requirement |
|---|---|

## Minimum harmonisation

| Type | Principle |
|---|---|

> Numbering: 1.5
>
> Article 5 - Minimum harmonisation
>
> This Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.

## monitor the implementation NIS2 at national level

| Type | Goal |
|---|---|

> Numbering: 2.8.2

## MSs must designate competent authorities, CSIRTs, and single points of contact

| Type | Requirement |
|---|---|

## MSs must establish national cybersecurity strategies

| Type | Requirement |
|---|---|

## mutatis mutandis

| Type | Principle |
|---|---|

> Numbering: 7.33.5
>
> The same rules for liability, safeguards, and proportionality as for essential entities (Article 32) also apply here.

## Mutual assistance

| Type | Principle |
|---|---|

> Numbering: 7.37

## National Cybersecurity Strategy

| Type | Goal |
|---|---|

> Numbering: 1.1.2.a

## national preparedness measures

| Type | Value |
|---|---|

Numbering: 2.9.4.4.d

national procedures and arrangements between relevant national authorities and bodies

| Type | Value |
|---|---|

Numbering: 2.9.4.6.f

NIS2 cross-sector coordination

| Type | Requirement |
|---|---|

Numbering: 2.13.5, 2.13.4

Between authorities under NIS2 and under the CER Directive (2022/2557).

No automatic oversight; supervision happens only when there’s a trigger

| Type | Principle |
|---|---|

not later than one month

| Type | Requirement |
|---|---|

Numbering: 4.23.4.4.d

objectives of national preparedness measures and activities

| Type | Value |
|---|---|

Numbering: 2.9.4.1.a

Once subject to a peer review, the same aspects reviewed in a MS shall not be subject to a further peer review in that MS for two years following the conclusion of the peer review

| Type | Constraint |
|---|---|

Numbering: 3.19.7

Open Internet Public Core AIC

| Type | Requirement |
|---|---|

Numbering: 2.7.2.4.d

Operational Confidentiality

| Type | Requirement |
|---|---|

Numbering: 2.11.1.4.d

period of five years

| Type | Requirement |
|---|---|

## Prevent or minimise the impact of incidents on recipients of their services and on other services

| Type | Goal |
|---|---|

Numbering: 4.21.1

## prioritisation of tasks following a risk-based approach

| Type | Principle |
|---|---|

Numbering: 7.31.2

## prioritization of mandatory notifications over voluntary notifications

| Type | Principle |
|---|---|

Numbering: 6.30.2

## Proactive (ex ante)

| Type | Principle |
|---|---|

## Provide services

| Type | Value |
|---|---|

Numbering: 1.2, 1.3

## public awareness principle

| Type | Principle |
|---|---|

Numbering: 4.23.7

Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, a Member State’s CSIRT or, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned, may, after consulting the entity concerned, inform the public about the significant incident or require the entity to do so.

## publicly available

| Type | Requirement |
|---|---|

Numbering: 5.28.4

4. Member States shall require the TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.

Member States shall require policies and procedures with regard to the disclosure of such data to be made publicly available.

### Reactive (ex post)

| Type | Principle |
|---|---|

### Redundant Communication Channels

| Type | Requirement |
|---|---|

Numbering: 2.11.1.1.a

### relevant public and private stakeholders and infrastructure involved

| Type | Value |
|---|---|

Numbering: 2.9.4.5.e

### relevant to the security of network and information systems

| Type | Requirement |
|---|---|

Numbering: 4.25.1

### Reporting Obligations

| Type | Goal |
|---|---|

Numbering: 1.1.2.b

### Request Management System

| Type | Requirement |
|---|---|

Numbering: 2.11.1.3.c

### Risk Management

| Type | Goal |
|---|---|

Numbering: 1.1.2.b

### risk-based

| Type | Principle |
|---|---|

### Risk-based approach

| Type | Principle |
|---|---|

Numbering: 2.11.3

### Secure Infrastructure

| Type | Requirement |
|---|---|

Numbering: 2.11.1.2.b

### Service Continuity and Backup

| Type | Requirement |
|---|---|

Numbering: 2.11.1.6.f

### shall comply with the rights of the defence and take account of the circumstances of each individual case

| Type | Requirement |
|---|---|

Numbering: 7.32.7

### shall ensure coherence with the existing frameworks for general national crisis management

| Type | Requirement |
|---|---|

Numbering: 2.9.1

### shall identify capabilities, assets and procedures that can be deployed in the case of a crisis

| Type | Requirement |
|---|---|

Numbering: 2.9.3

### shall meet on a regular basis and in any event at least once a year with the Critical Entities Resilience Group

| Type | Requirement |
|---|---|

Numbering: 3.14.9

### simplified reporting

| Type | Principle |
|---|---|

Numbering: 2.13.6

### SME Cyber Resilience Program

| Type | Requirement |
|---|---|

Numbering: 2.7.2.8.i

### Stakeholder

| Type | Stakeholder |
|---|---|

### State-of-the-art Cybersecurity Risk Management

| Type | Requirement |
|---|---|

Numbering: 2.7.2.5.e

### Supervision and Enforcement

| Type | Goal |
|---|---|

Numbering: 1.1.2.d

### support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence

| Type | Goal |
|---|---|

Numbering: 3.14.9

### Support coordinated management of major cybersecurity incidents and enable regular information exchange across Member States and EU bodies

| Type | Goal |
|---|---|

Numbering: 3.16.1

### tasks and responsibilities of the cyber crisis management authorities

| Type | Value |
|---|---|

Numbering: 2.9.4.2.b

### The competent authorities shall work in close cooperation with supervisory authorities

| Type | Requirement |
|---|---|

### Trusted intermediary

| Type | Value |
|---|---|

Numbering: 2.12.1

### voluntary basis

| Type | Principle |
|---|---|

Numbering: 6.30.1

### Voluntary Cyber Information Sharing

| Type | Requirement |
|---|---|

Numbering: 2.7.2.8.h

### Vulnerability Management & Disclosure

| Type | Requirement |
|---|---|

Numbering: 2.7.2.3.c

## within 2 months

| Type | Requirement |
| --- | --- |

Numbering: 8.38.6

## within 24 hours

| Type | Requirement |
| --- | --- |

Numbering: 4.23.4.1.a

## within 72 hours

| Type | Requirement |
| --- | --- |

Numbering: 4.23.4.2.b
Numbering: 5.28.5

## within three months of NCS adoption

| Type | Requirement |
| --- | --- |

Numbering: 2.7.3

# Other

## CNCS in action

| Type | Grouping |
|---|---|

## Cooperation Group Core Behavior

| Type | Grouping |
|---|---|

Numbering: 3.14.4, 3.14.6

## Core CSIRTs Network Behavior

| Type | Grouping |
|---|---|

Numbering: 3.15.3

## CpC actions

| Type | Grouping |
|---|---|

## CSIRTs Core Processes

| Type | Grouping |
|---|---|

## CSIRTs Core Requirements

| Type | Grouping |
|---|---|

## Cybersecurity risk-management measures

| Type | Grouping |
|---|---|

Numbering: 4.21.2

## Database of domain name registration data inclusions

| Type | Grouping |
|---|---|

## Entity Information

| Type | Grouping |
|---|---|

Numbering: 5.27.2

## Essential Entities

| Type | Grouping |
|---|---|

Numbering: 1.3.1

## EU-CyCLONe Core Behavior

| Type | Grouping |
|---|---|

## Government actions

| Type | Grouping |
|---|---|

## ICT Group

| Type | Grouping |
|---|---|

## Important Entities

| Type | Grouping |
|---|---|

Numbering: 1.3.2

## Junction

| Type | Junction |
|---|---|

Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.

## Junction

| Type | Junction |
|---|---|

## Large-scale cybersecurity incidents or crises handling

| Type | Grouping |
|---|---|

Numbering: 3.16.3, 3.16.5

## Major Required Information

| Type | Grouping |
|---|---|

Numbering: 1.3.4

## Maturity Levels

| Type | Grouping |
|---|---|

## National Cooperation

| Type | Grouping |
|---|---|

## National large-scale cybersecurity incident and crisis response plan content

| Type | Grouping |
|---|---|

Numbering: 2.9.4

## NCS Lifecycle

| Type | Grouping |
|---|---|

## Operational cooperation information handling

| Type | Grouping |
|---|---|

## Policies to adopt

| Type | Grouping |
|---|---|

Numbering: 2.7.2

## Portugal

| Type | Location |
|---|---|

## Report on the state of cybersecurity inclusions

| Type | Grouping |
|---|---|

Numbering: 3.18.1

## Supervisory and enforcement measures in relation to essential entities Core

| Type | Grouping |
|---|---|

Numbering: 7.32.1

## Supply chain security measure assessment

| Type | Grouping |
|---|---|

# Relations

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Important Entities |
| **Target** | Medium-sized enterprise |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Important Entities |
| **Target** | Important Entity |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Major Required Information |
| **Target** | Entity Name |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Major Required Information |
| **Target** | Address and up-to-date contact details |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Major Required Information |
| **Target** | Relevant sector and subsector |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Major Required Information |
| **Target** | List of the Member States where they provide services |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Important Entities |
| **Target** | Major Required Information |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Essential Entities |
| **Target** | Major Required Information |

## Association relation

| | |
|---|---|
| **Type** | Association relation |

| | |
|---|---|
| **Source** | Enhance the overall level of cybersecurity across the European Union |
| **Target** | Provide services |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Enhance the overall level of cybersecurity across the European Union |
| **Target** | Minimum harmonisation |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Enhance the overall level of cybersecurity across the European Union |
| | Entities already covered by equivalent EU cybersecurity laws are exempt, while others remain under this Directive |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | National Cybersecurity Strategy |
| **Target** | achieve cybersecurity strategy |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Governance Framework |
| **Target** | achieve cybersecurity strategy |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Member State |
| **Target** | achieve cybersecurity strategy |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cybersecurity Strategy |
| **Target** | Risk Assessment |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cybersecurity Strategy |
| **Target** | Governance Framework |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cybersecurity Strategy |
| **Target** | Cybersecurity Measures |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cybersecurity Strategy |
| **Target** | List of involved actors |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cybersecurity Strategy |
| **Target** | Enhanced Cyber Coordination Policy |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cybersecurity Strategy |
| **Target** | Cyber Awareness Plan |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Policies to adopt |
| **Target** | State-of-the-art Cybersecurity Risk Management |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Policies to adopt |
| **Target** | ICT Supply Chain Security Policy |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Policies to adopt |
| **Target** | Cyber Education & Awareness Program |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Policies to adopt |
| **Target** | ICT Cybersecurity Procurement Standards |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Policies to adopt |
| **Target** | Cybersecurity Research & Innovation |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Policies to adopt |
| **Target** | Voluntary Cyber Information Sharing |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Policies to adopt |
| **Target** | Vulnerability Management & Disclosure |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Policies to adopt |
| **Target** | Open Internet Public Core AIC |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Policies to adopt |
| **Target** | SME Cyber Resilience Program |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | National Cybersecurity Strategy |
| **Target** | Policies to adopt |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Policies to adopt |
| **Target** | Active Cyber Protection Policy |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | National Cybersecurity Strategy |
| **Target** | Establish NCS |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Establish NCS |
| **Target** | Notify Commission of NCS |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notify Commission of NCS |
| **Target** | European Commission |

## Association relation

| | |
|---|---|
| **Type** | Association relation |

| | |
|---|---|
| **Source** | Governance Framework |
| **Target** | NIS2 Competent Authority |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Governance Framework |
| **Target** | NIS2 Single Point of Contact |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Governance Framework |
| **Target** | NIS2 CSIRT |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | NCS Lifecycle |
| **Target** | Establish NCS |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | NCS Lifecycle |
| **Target** | NCS Assessment |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | NCS Lifecycle |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | NCS Lifecycle |
| **Target** | Establish KPIs |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | NCS Assessment |
| **Target** | Establish KPIs |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | NCS Lifecycle |
| **Target** | Update NCS |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | NCS Assessment |
| **Target** | Update NCS |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cybersecurity Strategy |
| **Target** | Relevant assets |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Important Entities |
| **Target** | Provide services |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Essential Entities |
| **Target** | Provide services |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Assess NCS |
| **Target** | NCS Assessment |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Assess NCS |
| **Target** | do on regular basis and at least every five years |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Notify Commission of NCS |
| **Target** | within three months of NCS adoption |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Liason Function |
| **Target** | cross-sectoral cooperation |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Liason Function |
| **Target** | cross-border cooperation |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | NIS2 Competent Authority |
| **Target** | monitor the implementation NIS2 at national level |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Member State |
| | ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Cyber crisis management authority |
| | shall ensure coherence with the existing frameworks for general national crisis management |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | National large-scale cybersecurity incident and crisis response plan |
| | National large-scale cybersecurity incident and crisis response plan content |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National large-scale cybersecurity incident and crisis response plan content |
| | cyber crisis management procedures |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National large-scale cybersecurity incident and crisis response plan content |
| | national preparedness measures |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National large-scale cybersecurity incident and crisis response plan content |
| | national procedures and arrangements between relevant national authorities and bodies |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | National large-scale cybersecurity incident and crisis response plan content |
| | relevant public and private stakeholders and infrastructure involved |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National large-scale cybersecurity incident and crisis response plan content |
| | objectives of national preparedness measures and activities |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National large-scale cybersecurity incident and crisis response plan content |
| | tasks and responsibilities of the cyber crisis management authorities |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Establish Competent Authority |
| **Target** | Establish SPC |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Establish SPC |
| **Target** | Notify Commission of SPC |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notify Commission of SPC |
| **Target** | European Commission |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Notify Commission of SPC |
| **Target** | Keep updated a list of SPCs publicly available |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Keep updated a list of SPCs publicly available |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Establish Competent Authority |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Establish SPC |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notify of coordinator and plan |
| **Target** | EU-CyCLONe |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notify of coordinator and plan |
| **Target** | European Commission |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Implement plan |
| **Target** | National large-scale cybersecurity incident and crisis response plan |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Establish Cyber crisis management authority |
| **Target** | Appoint main crisis coordinator |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Cyber crisis management authority |
| | shall identify capabilities, assets and procedures that can be deployed in the case of a crisis |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Establish CSIRT |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Establish CSIRT |
| **Target** | contributes to the deployment of secure information-sharing tools |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |

| | |
|---|---|
| **Source** | Member State |
| **Target** | Designate CSIRT Coordinator |

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Reported vulnerability |
| **Target** | Responsible Disclosure Management |

### Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Responsible Disclosure Management |
| **Target** | anonymity |

### Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Coordinator CSIRT |
| **Target** | Responsible Disclosure Management |

### Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Natural or legal person |
| **Target** | Reported vulnerability |

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Reported potential vulnerability on ICT products or ICT services |
| **Target** | Responsible Disclosure Management |

### Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Provider or Manufacturer |
| **Target** | Reported potential vulnerability on ICT products or ICT services |

### Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | European Vulnerability Database |
| **Target** | Trusted User Guidance |

### Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | European Vulnerability Database |
| **Target** | Availability of related patches |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | European Vulnerability Database |
| **Target** | Severity |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | European Vulnerability Database |
| **Target** | Affected ICT products or ICT services |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | European Vulnerability Database |
| **Target** | Vulnerability Information |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notification of significant incidents, incidents, cyber threats or near misses |
| | NIS2 CSIRT |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notification of significant incidents, incidents, cyber threats or near misses |
| | NIS2 Competent Authority |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Notification of significant incidents, incidents, cyber threats or near misses |
| | Forward Notification to SPC |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Forward Notification to SPC |
| **Target** | NIS2 Single Point of Contact |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRT |
| **Target** | Forward Notification to SPC |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |

| | |
|---|---|
| **Source** | NIS2 Competent Authority |
| **Target** | Forward Notification to SPC |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| | Notification of significant incidents, incidents, cyber threats or near misses |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | NIS2 Single Point of Contact |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | Forward Notification to SPC |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | NIS2 Competent Authority |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | NIS2 CSIRT |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | appropriate cooperation |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | information exchange |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | simplified reporting |

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Establish Competent Authority |
| **Target** | Make the identity of the Competent Authority public |

### Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cooperation Group Core Behavior |
| **Target** | Strategic Level Experience Report |

### Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENISA |
| **Target** | Establish CSIRT |

Numbering: 2.10.10

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Relevant Information |
| **Target** | Relevant Secure Information Exchange |

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Cross-border incident |
| **Target** | Cross-Border Assistance |

### Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Cross-Border Assistance |
| **Target** | Member State |

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Third country security incident |
| **Target** | International Cybersecurity Assistance |

### Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | International Cybersecurity Assistance |
| **Target** | Third countries’ national CSIRT |

### Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | CSIRTs Core Processes |
| **Target** | International Cybersecurity Assistance |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Processes |
| **Target** | Handle and coordinate incident |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRT |
| **Target** | Monitor cyber threats and incidents |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Cross-Border Assistance |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Relevant Secure Information Exchange |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Guarantee CSIRTs Cooperation |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRTs Network |
| **Target** | Core CSIRTs Network Behavior |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Processes |
| **Target** | Participate in peer reviews |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Report operations and activities |
| **Target** | Cooperation Group |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Discuss capabilities and preparedness |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Request of an individual CSIRT |
| **Target** | Discuss capabilities and preparedness |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Biennial |
| **Target** | Assess the progress made |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Assess the progress made |
| **Target** | Adopt a report |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Adopt a report |
| **Target** | Notify Cooperation Group |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notify Cooperation Group |
| **Target** | Cooperation Group |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Assess the progress made |
| **Target** | Operational Cooperation Information |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Report operations and activities |
| **Target** | Operational Cooperation Information |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Discuss and identify further forms of operational cooperation |
| **Target** | Operational Cooperation Information |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Aid CSIRT |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Designate CSIRT Coordinator |
| **Target** | Coordinator CSIRT |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Establish Competent Authority |
| **Target** | NIS2 Competent Authority |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Establish SPC |
| **Target** | NIS2 Single Point of Contact |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Establish Cyber crisis management authority |
| **Target** | Cyber crisis management authority |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Assisting reporting a vulnerability |
| **Target** | Reported vulnerability |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Assisting reporting a vulnerability |
| **Target** | Natural or legal person |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Coordinator CSIRT |
| **Target** | Assisting reporting a vulnerability |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | Cooperation Group Core Behavior |
| **Target** | Strategic Guidance Provision |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Strategic Guidance Provision |
| **Target** | NIS2 CSIRTs Network |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Strategic Guidance Provision |
| **Target** | EU-CyCLONe |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cooperation Group Core Behavior |
| **Target** | Technical report request |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Request technical report on selected topics |
| **Target** | Technical report request |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Technical report request |
| **Target** | NIS2 CSIRTs Network |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cooperation Group Core Behavior |
| **Target** | Discuss mutual assistance |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Large-scale cybersecurity incident or crise MS request |
| **Target** | Discuss mutual assistance |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cooperation Group Core Behavior |
| **Target** | Aid transposition of NIS2 |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Aid transposition of NIS2 |
| **Target** | NIS2 Competent Authority |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cooperation Group Core Behavior |
| | Guidance on the development and implementation of policies on coordinated vulnerability disclosure |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Guidance on the development and implementation of policies on coordinated vulnerability disclosure |
| | NIS2 Competent Authority |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Processes |
| **Target** | Provide alerts and incident response |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Security Incident |
| **Target** | Provide alerts and incident response |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Provide alerts and incident response |
| **Target** | Handle and coordinate incident |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Monitor cyber threats and incidents |
| **Target** | Security Incident |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Monitor cyber threats and incidents |
| **Target** | Third country security incident |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | CSIRTs Core Processes |
| **Target** | Perform forensic and risk analysis |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | Monitor cyber threats and incidents |
| **Target** | Perform forensic and risk analysis |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | NIS2 CSIRTs Network |
| | contribute to the development of confidence and trust and to promote swift and effective operational cooperation among MSs |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | EU-CyCLONe |
| | Support coordinated management of major cybersecurity incidents and enable regular information exchange across Member States and EU bodies |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | EU-CyCLONe |
| **Target** | European Commission |

Numbering: 3.16.2

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Assess the consequences and impact for large-scale cybersecurity incidents and crises |
| | Propose possible mitigation measures |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Aid CSIRT |
| **Target** | Discuss capabilities and preparedness |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Large-scale cybersecurity incident or crise |
| | Coordinate management for large-scale cybersecurity incidents and crises |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Large-scale cybersecurity incident or crise |
| | Assess the consequences and impact for large-scale cybersecurity incidents and crises |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Coordinate management for large-scale cybersecurity incidents and crises |
| | Support decision-making at political level |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | EU-CyCLONe |
| **Target** | EU-CyCLONe Core Behavior |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Large-scale cybersecurity incident or crise MS request |
| | Discuss national large-scale cybersecurity incident and crisis response plans |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Coordinate management for large-scale cybersecurity incidents and crises |
| | Report management and trends |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Report management and trends |
| **Target** | Cooperation Group |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Coordinate Procedural Arrangements |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | EU-CyCLONe Core Behavior |
| **Target** | Coordinate Procedural Arrangements |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | International/Third Country Organization |
| **Target** | International Agreement |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Union |
| **Target** | International Agreements Conclusion |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | International Agreement |
| **Target** | GDPR |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | International Agreement |
| **Target** | Cooperation Group |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | International Agreement |
| **Target** | NIS2 CSIRTs Network |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | International Agreements Conclusion |
| **Target** | International/Third Country Organization |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | International Agreement |
| **Target** | EU-CyCLONe |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | EU-CyCLONe Core Behavior |
| **Target** | EU-CyCLONe Work Assessment Report |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Council |
| **Target** | EU-CyCLONe Work Assessment Report |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | European Parliament |
| **Target** | EU-CyCLONe Work Assessment Report |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | European Commission |
| **Target** | Strategic Level Experience Report |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Council |
| **Target** | Strategic Level Experience Report |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | European Parliament |
| **Target** | Strategic Level Experience Report |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Adopt a report |
| **Target** | Progress Report |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Cooperation Group |
| **Target** | Progress Report |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Progress Report |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | EU-CyCLONe |
| **Target** | Discuss mutual assistance |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |

| | |
|---|---|
| **Source** | NIS2 CSIRTs Network |
| **Target** | Discuss mutual assistance |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Adopt report |
| **Target** | Report on the state of cybersecurity |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Cooperation Group |
| **Target** | Adopt report |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENISA |
| **Target** | Adopt report |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Submit and present report |
| **Target** | Report on the state of cybersecurity |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Submit and present report |
| **Target** | European Parliament |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Adopt report |
| **Target** | Submit and present report |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Report on the state of cybersecurity inclusions |
| | Aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Report on the state of cybersecurity inclusions |
| **Target** | Union-level cybersecurity risk assessment |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Report on the state of cybersecurity inclusions |
| **Target** | Aggregated assessment of the outcome of peer reviews |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Report on the state of cybersecurity inclusions |
| | Assessment of the general level of cybersecurity awareness andcyber hygiene among citizens and entities |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Report on the state of cybersecurity inclusions |
| | Assessment of the development of cybersecurity capabilities inthe public and private sectors across the Union |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Report on the state of cybersecurity |
| **Target** | Report on the state of cybersecurity inclusions |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Report on the state of cybersecurity inclusions |
| **Target** | ENISA Cybersecurity Policy Recommendations |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | ENISA |
| **Target** | ENISA Cybersecurity Policy Recommendations |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Develop methodology |
| | Aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENISA |
| **Target** | Peer review |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |

| | |
|---|---|
| **Source** | European Commission |
| **Target** | Peer review |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Cooperation Group |
| **Target** | Peer review |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRTs Network |
| **Target** | Peer review |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Peer review |
| **Target** | Enhance cybersecurity trust and capabilities across MSs |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Peer review |
| **Target** | Carry out Peer Review |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Cybersecurity Expert |
| **Target** | Carry out Peer Review |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Cybersecurity Expert |
| **Target** | Draft reports on the findings and conclusions |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Peer review |
| | Once subject to a peer review, the same aspects reviewed in a MS shall not be subject to a further peer review in that MS for two years following the conclusion of the peer review |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | MS participation notification |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Carry out Peer review self-assessment |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Carry out Peer review self-assessment |
| **Target** | Peer review self-assessment |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | MS participation notification |
| **Target** | Peer review |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Carry out Peer review self-assessment |
| **Target** | Peer review |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Peer review |
| **Target** | Member State |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cybersecurity risk-management measures |
| **Target** | Policies on risk analysis and information system security |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cybersecurity risk-management measures |
| **Target** | Incident handling |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cybersecurity risk-management measures |
| **Target** | Supply chain security |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cybersecurity risk-management measures |
| | Secure network and information system development and vulnerability |

| | |
|---|---|
| | management |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cybersecurity risk-management measures |
| | Policies and procedures to assess the effectiveness of cybersecurity risk-management measures |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cybersecurity risk-management measures |
| **Target** | Basic cyber hygiene practices and cybersecurity training |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cybersecurity risk-management measures |
| | Policies and procedures regarding the use of cryptography and, where appropriate, encryption |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cybersecurity risk-management measures |
| | Human resources security, access control policies and asset management |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cybersecurity risk-management measures |
| **Target** | Secure and authenticated communications |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Cybersecurity risk-management measure |
| | Manage the risks posed to the security of network and information systems |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Cybersecurity risk-management measure |
| | Prevent or minimise the impact of incidents on recipients of their services and on other services |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Ensure a proportional level of security based on risk exposure, entity size, and potential impact |

| | |
|---|---|
| | Cybersecurity risk-management measure |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Cybersecurity risk-management measure |
| **Target** | all-hazards approach |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Check if measure is appropriate |
| | Evaluate entities' supplier-specific vulnerabilities and cybersecurity practices |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Supply chain security measure assessment |
| **Target** | Supply chain security |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Supply chain security measure assessment |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supply chain security measure assessment |
| | Evaluate entities' supplier-specific vulnerabilities and cybersecurity practices |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Assess compliance with measure |
| **Target** | Junction |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Assess compliance with measure |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Take appropriate and proportionate corrective measures |
| **Target** | Entity |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Take cybersecurity risk-management measure |
| **Target** | Cybersecurity risk-management measure |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Take appropriate and proportionate corrective measures |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Take cybersecurity risk-management measure |
| **Target** | Compliance Risk Assessment |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Take cybersecurity risk-management measure |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENISA |
| **Target** | Carry out coordinated security risk assessments |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Carry out coordinated security risk assessments |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Cooperation Group |
| **Target** | Carry out coordinated security risk assessments |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Carry out coordinated security risk assessments |
| **Target** | Identify Critical ICT for Risk Assessment |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Identify Critical ICT for Risk Assessment |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Carry out coordinated security risk assessments |
| **Target** | Risk assessment of critical supply chain |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Identify Critical ICT for Risk Assessment |
| **Target** | ICT Service |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Identify Critical ICT for Risk Assessment |
| **Target** | ICT System |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Identify Critical ICT for Risk Assessment |
| **Target** | ICT Product |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supply chain security measure assessment |
| **Target** | Check if measure is appropriate |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supply chain security measure assessment |
| | Check if entities are required to take into account the results of the coordinated security risk assessments of critical supply chains |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Check if measure is appropriate |
| | Check if entities are required to take into account the results of the coordinated security risk assessments of critical supply chains |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Check if entities are required to take into account the results of the coordinated security risk assessments of critical supply chains |
| | Risk assessment of critical supply chain |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Take cybersecurity risk-management measure |
| **Target** | Approve cybersecurity risk-management measure |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Management Body |
| **Target** | Approve cybersecurity risk-management measure |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Approve cybersecurity risk-management measure |
| **Target** | Oversee implementation |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Management Body |
| **Target** | People Training |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Request |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Request |
| **Target** | People Training |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Management Body |
| **Target** | Oversee implementation |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Significant Incident |
| **Target** | Notify CSIRT |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRT |
| **Target** | Determine cross-border or cross-sectoral impact of the incident |

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Incident |
| **Target** | Significant Incident |

> Numbering: 4.23.3.1.a, 4.23.3.1.b
>
> a - severe service disruption or financial loss to the entity
>
> or
>
> b - significant harm to others (material or non-material)

### Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Early warning of potential malicious or cross-border incident |
| **Target** | NIS2 CSIRT |

### Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Early warning of potential malicious or cross-border incident |
| **Target** | within 24 hours |

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Early warning of potential malicious or cross-border incident |
| **Target** | Incident notification (update) |

### Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | within 72 hours |
| **Target** | Incident notification (update) |

### Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Incident notification (update) |
| **Target** | NIS2 CSIRT |

### Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Report incident impact information |
| **Target** | Intermediate Report |

### Access relation

| | |
|---|---|
| **Type** | Access relation |

| | |
|---|---|
| **Source** | Report incident impact information |
| **Target** | Final Report |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRT |
| **Target** | Answer to the notifying entity |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Answer to the notifying entity |
| **Target** | Early warning of potential malicious or cross-border incident |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notify SPC of cross-* incident |
| **Target** | NIS2 Single Point of Contact |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRT |
| **Target** | Notify SPC of cross-* incident |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notify other MSs and ENISA |
| **Target** | ENISA |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Single Point of Contact |
| **Target** | Notify other MSs and ENISA |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | public awareness principle |
| **Target** | Incident notification (update) |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Submit Summary Report |
| **Target** | Summary Report |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Single Point of Contact |
| **Target** | Submit Summary Report |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Submit Summary Report |
| **Target** | ENISA |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | every three months |
| **Target** | Submit Summary Report |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | Assist reporter in disclosure process |
| | Negotiate disclosure timelines and managing vulnerabilities that affect multiple entities |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRTs Network |
| **Target** | Coordinate Procedural Arrangements |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | EU-CyCLONe |
| **Target** | Coordinate Procedural Arrangements |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| | Require use of certified ICT * and Qualified Trust Services for compliance |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Require use of certified ICT * and Qualified Trust Services for compliance |
| | Entity |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | ICT Group |
| **Target** | ICT Product |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | ICT Group |
| **Target** | ICT System |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | ICT Group |
| **Target** | ICT Service |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | ICT Group |
| **Target** | certified under European cybersecurity certification schemes |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Define certification requirements for entities |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Define certification requirements for entities |
| **Target** | Entity |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Commission request for candidate scheme |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Commission request for candidate scheme |
| **Target** | Prepare a candidate scheme |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENISA |
| **Target** | Prepare a candidate scheme |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Prepare a candidate scheme |
| **Target** | certified under European cybersecurity certification schemes |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Prepare a candidate scheme |
| **Target** | European cybersecurity certification scheme |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENISA |
| | Develop advice and guidelines on technical areas to be considered and existing standards to be used |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| | Develop advice and guidelines on technical areas to be considered and existing standards to be used |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Develop advice and guidelines on technical areas to be considered and existing standards to be used |
| | Promote standards and relevant technical specifications usage |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Promote standards and relevant technical specifications usage |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Create and maintain registry |
| **Target** | Registry of entities |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Single Point of Contact |
| **Target** | Information from SPC |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |

| | |
|---|---|
| **Source** | ENISA |
| **Target** | Create and maintain registry |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Information from SPC |
| **Target** | Create and maintain registry |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notify changes to Competent Authority |
| **Target** | NIS2 Competent Authority |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Submit Entity information |
| **Target** | NIS2 Competent Authority |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Submit Entity information |
| **Target** | Notify changes to Competent Authority |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Entity Information |
| **Target** | Establishments addresses |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Entity Information |
| **Target** | IP ranges |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Entity Information |
| **Target** | Relevant sector, subsector and type |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Entity Information |
| **Target** | MSs where provides services |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Entity Information |
| **Target** | Up-to-date contact details |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Submit Entity information |
| **Target** | Entity Information |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Single Point of Contact |
| **Target** | forward to ENISA |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | forward to ENISA |
| **Target** | ENISA |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Notify changes to Competent Authority |
| **Target** | forward to ENISA |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Database of domain name registration data |
| **Target** | contribute to the security, stability, and resilience of the DNS |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Database of domain name registration data inclusions |
| **Target** | Administrative Contact Information |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Database of domain name registration data inclusions |
| **Target** | Registration Date |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Database of domain name registration data inclusions |
| **Target** | Registrant Contact Information |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Database of domain name registration data inclusions |
| **Target** | Domain Name |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | Database of domain name registration data |
| **Target** | Database of domain name registration data inclusions |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Domain name registration services Provider |
| | Collect and maintain accurate and complete domain name registration data |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | TLD name registry |
| | Collect and maintain accurate and complete domain name registration data |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | MS request |
| | Collect and maintain accurate and complete domain name registration data |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | TLD name registry |
| **Target** | Establish and publish domain data verification policies |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Domain name registration services Provider |
| **Target** | Establish and publish domain data verification policies |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Collect and maintain accurate and complete domain name registration data |
| | Establish and publish domain data verification policies |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Collect and maintain accurate and complete domain name registration data |
| | publicly available |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Legitimate access seeker |
| **Target** | lawful and duly substantiated request |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | lawful and duly substantiated request |
| **Target** | Allow restrict access |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Allow restrict access |
| **Target** | Database of domain name registration data |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Domain name registration services Provider |
| **Target** | Allow restrict access |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | TLD name registry |
| **Target** | Allow restrict access |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Appoint Jurisdiction Representative |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Appoint Jurisdiction Representative |
| **Target** | Jurisdiction Representative |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |

| | |
|---|---|
| **Source** | Jurisdiction Representative |
| **Target** | Determine Judisdiction |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Determine Judisdiction |
| **Target** | exceptions from Article 26 1. |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Request for mutual assistance |
| **Target** | Take supervisory and enforcement measures |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Request for mutual assistance |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Cybersecurity information-sharing arrangement |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Cybersecurity information-sharing arrangement |
| | aims to prevent, detect, respond to or recover from incidents or to mitigate their impact |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | exchange on a voluntary basis relevant cybersecurity information |
| **Target** | Cybersecurity information-sharing arrangement |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Notify competent authority of participation or withdrawal |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Cybersecurity information-sharing arrangement |
| **Target** | Notify competent authority of participation or withdrawal |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Facilitate establishment |
| **Target** | Cybersecurity information-sharing arrangement |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Incident |
| **Target** | Notify CSIRT |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Notify CSIRT |
| **Target** | voluntary basis |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Notify CSIRT |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Notify recipients of service |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Early warning of potential malicious or cross-border incident |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Incident notification (update) |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Report incident impact information |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Processing Notification |
| **Target** | prioritization of mandatory notifications over voluntary notifications |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Notify CSIRT |
| **Target** | Processing Notification |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Report request |
| **Target** | Report incident impact information |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRT |
| **Target** | Report request |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Final Report |
| **Target** | not later than one month |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Incident notification (update) |
| **Target** | Determine cross-border or cross-sectoral impact of the incident |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Inform findings on notifications |
| **Target** | Cooperation Group |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Inform findings on notifications |
| **Target** | NIS2 CSIRTs Network |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | every six months |
| **Target** | Inform findings on notifications |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |

| | |
|---|---|
| **Source** | ENISA |
| **Target** | Inform findings on notifications |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRT |
| **Target** | Processing Notification |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | publicly available |
| **Target** | Establish and publish domain data verification policies |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Establish supervisory methodologies |
| **Target** | prioritisation of tasks following a risk-based approach |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | supervisory task |
| **Target** | Establish supervisory methodologies |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Supervisor |
| **Target** | Establish supervisory methodologies |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Supervisor |
| | Supervise compliance and enforce measures on public administration entities |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | GDPR Supervisory Authority |
| **Target** | Address incident |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Supervisor |
| **Target** | Address incident |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Implement enforcement measure |
| **Target** | Junction |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | Establish Enforcement Deadline |
| **Target** | Suspend temporarily a certification or authorisation |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | Establish Enforcement Deadline |
| **Target** | Temporarily prohibit key managers from their duties |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Set out a detailed reasoning |
| **Target** | Notify entities concerned of their preliminary findings |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Essential Entities |
| **Target** | Submit observations |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Submit observations |
| **Target** | NIS2 Competent Authority |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Notify entities concerned of their preliminary findings |
| **Target** | Submit observations |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Entity |
| **Target** | Administrative fines |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Administrative fines |
| **Target** | effective, proportionate and dissuasive |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Entity |
| **Target** | Periodic penalty payments |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | NIS2 Competent Authority |
| **Target** | Administrative fines |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | NIS2 Competent Authority |
| **Target** | Periodic penalty payments |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Competent Authority |
| **Target** | inform relevant GDPR Supervisory Authority |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | GDPR Supervisory Authority |
| **Target** | inform relevant GDPR Supervisory Authority |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Competent Authority |
| **Target** | Issues fine on Entity |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | GDPR Supervisory Authority |
| **Target** | Issues fine on Entity |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Issues fine on Entity |
| | If the GDPR supervisory authority has already fined the entity for the same incident, the competent authority cannot also impose a fine under NIS2 for the same conduct. However, it can still apply other enforcement measures (like warnings, orders, audits). |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | inform relevant GDPR Supervisory Authority |
| **Target** | Issues fine on Entity |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | inform relevant GDPR Supervisory Authority |
| | If the relevant GDPR supervisory authority is in another country, the competent authority must notify its own national GDPR authority about the potential data breach |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notify Commission of measures |
| **Target** | European Commission |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Notify Commission of measures |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Penalty by infringements of national measures |
| **Target** | Lay down rules and take measures |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Lay down rules and take measures |
| **Target** | Notify Commission of measures |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Lay down rules and take measures |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Competent Authority |
| **Target** | Entity supervisory and enforcement coordination and cooperation |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |

| | |
|---|---|
| **Source** | Entity supervisory and enforcement coordination and cooperation |
| **Target** | Entity |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Entity supervisory and enforcement coordination and cooperation |
| **Target** | Mutual assistance |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Implement supervisory measure |
| **Target** | Supervisory measure |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Implement enforcement measure |
| **Target** | Enforcement measure |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Implement supervisory measure |
| **Target** | Essential Entity Supervision |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Implement enforcement measure |
| **Target** | Set out a detailed reasoning |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | shall comply with the rights of the defence and take account of the circumstances of each individual case |
| | Implement enforcement measure |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Competent Authority |
| **Target** | Implement supervisory measure |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Essential Entities |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Supervisory measure |
| **Target** | risk-based |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Implement enforcement measure |
| **Target** | mutatis mutandis |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Important Entities |
| **Target** | Implement enforcement measure |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Important Entity Supervision |
| **Target** | Important Entities |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Important Entity Supervision |
| **Target** | Implement enforcement measure |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | non-compliance evidence |
| **Target** | Important Entity Supervision |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Supervisory measure |
| **Target** | Proactive (ex ante) |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Essential Entity Supervision |
| **Target** | Automatic oversight; ongoing supervision |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Supervisory measure |
| **Target** | Reactive (ex post) |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Important Entity Supervision |
| | No automatic oversight; supervision happens only when there’s a trigger |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Entity supervisory and enforcement coordination and cooperation |
| **Target** | Enforcement measure |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Entity supervisory and enforcement coordination and cooperation |
| **Target** | Supervisory measure |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Council |
| **Target** | Create Delegation act |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Parliament |
| **Target** | Create Delegation act |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Adopt delegation act |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Create Delegation act |
| **Target** | Delegated act |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Adopt delegation act |
| **Target** | period of five years |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |

| | |
|---|---|
| **Source** | Council |
| **Target** | Revoke Delegation act |

### Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Parliament |
| **Target** | Revoke Delegation act |

### Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Revoke Delegation act |
| **Target** | Delegated act |

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Create Delegation act |
| **Target** | Consulte experts designated by each MS |

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Consulte experts designated by each MS |
| **Target** | Adopt delegation act |

### Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Consulte experts designated by each MS |

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Adopt delegation act |
| **Target** | Notify Parliament and Council of delegated act |

### Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Request for written procedure |

### Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Request for written procedure |
| **Target** | Committee |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Committee |
| **Target** | Terminate procedure |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Review NIS2 functioning |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notify report to Parliament and Council |
| **Target** | European Parliament |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Notify report to Parliament and Council |
| **Target** | Council |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Review NIS2 functioning |
| **Target** | NIS2 Review Report |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Review NIS2 functioning |
| **Target** | Notify report to Parliament and Council |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | European Parliament |
| **Target** | NIS2 Review Report |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Council |
| **Target** | NIS2 Review Report |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | Review NIS2 functioning |
| **Target** | Gather Cooperation Group and CSIRTs Network reports |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Processes |
| **Target** | Security Incident |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Processes |
| **Target** | Third country security incident |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | NCS Lifecycle |
| **Target** | Notify Commission of NCS |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | NCS Lifecycle |
| **Target** | Assess NCS |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | EU-CyCLONe Core Behavior |
| **Target** | every 18 months |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Relevant Information |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Cross-border incident |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Request of an individual CSIRT |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | Cooperation Group Core Behavior |
| **Target** | Biennial work programme |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cooperation Group Core Behavior |
| **Target** | Large-scale cybersecurity incident or crise MS request |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Essential Entities |
| **Target** | QTS Provider |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Essential Entities |
| **Target** | Top-level domain name registry |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Essential Entities |
| **Target** | DNS service provider |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Essential Entities |
| **Target** | Public administration entity |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Essential Entities |
| **Target** | Provider of public electronic communications network/service |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Essential Entities |
| **Target** | Critical Entity |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cooperation Group Core Behavior |
| **Target** | Request technical report on selected topics |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Secretariat Provider |

Numbering: 3.14.3

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cooperation Group Core Behavior |
| **Target** | Secretariat Provider |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Facilitate establishment |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | MS request |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Take supervisory and enforcement measures |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Determine Judisdiction |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cooperation Group |
| **Target** | Member State Representative |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cooperation Group |
| **Target** | European Commission |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | Cooperation Group |
| **Target** | ENISA |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Cooperation Group |
| | support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Cooperation Group |
| **Target** | Cooperation Group Core Behavior |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Cooperation Group |
| | shall meet on a regular basis and in any event at least once a year with the Critical Entities Resilience Group |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Secretariat Provider |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENISA |
| **Target** | Secretariat Provider |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | EU-CyCLONe Core Behavior |
| **Target** | Secretariat Provider |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Database of domain name registration data |
| **Target** | GDPR |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Allow restrict access |
| **Target** | within 72 hours |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Appoint main crisis coordinator |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Establish Cyber crisis management authority |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | personal data breach incident |
| **Target** | inform relevant GDPR Supervisory Authority |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | personal data breach incident |
| **Target** | Address incident |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cybersecurity risk-management measures |
| **Target** | Business continuity |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | ENISA |
| | adopt the necessary technical and organisational measures to ensure the security and integrity of the European DB |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Designate CSIRT Coordinator |
| **Target** | coordinated vulnerability disclosure |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | European Vulnerability Database |
| | enabling entities and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Notify CSIRT |
| **Target** | Early warning of potential malicious or cross-border incident |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | NIS2 Competent Authority |
| **Target** | NIS2 Supervisor |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | PT CNCS |
| **Target** | NIS2 Competent Authority |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | PT CNCS |
| **Target** | NIS2 Single Point of Contact |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | PT CERT.PT |
| **Target** | NIS2 CSIRT |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | PT CNCS |
| **Target** | PT CERT.PT |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | NIS2 CSIRTs Network |
| **Target** | Coordinator CSIRT |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | EU CERT-EU |
| **Target** | EU CSIRTs Coordinator |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | PT RNCSIRT |
| **Target** | NIS2 CSIRTs Network |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Promote standards and relevant technical specifications usage |
| **Target** | relevant to the security of network and information systems |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Risk |
| **Target** | Take cybersecurity risk-management measure |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Near Miss |
| **Target** | Notify CSIRT |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Cyber Threat |
| **Target** | Notify CSIRT |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Significant Incident |
| | Notification of significant incidents, incidents, cyber threats or near misses |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Incident |
| | Notification of significant incidents, incidents, cyber threats or near misses |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Cyber Threat |
| | Notification of significant incidents, incidents, cyber threats or near misses |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Near Miss |
| | Notification of significant incidents, incidents, cyber threats or near misses |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Significant Cyber Threat |
| **Target** | Notify recipients of service |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | PT GNS |
| **Target** | PT CNCS |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | PT RNCSIRT |
| **Target** | PT CERT.PT |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | EU CERT-EU |
| **Target** | PT CERT.PT |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | EU CERT-EU |
| **Target** | NIS2 CSIRTs Network |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | PT CNCS |
| **Target** | Cybersecurity  in Portugal |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Member States may allow their competent authorities to prioritise supervisory tasks |
| | Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | The competent authorities shall work in close cooperation with supervisory authorities |
| | Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Entities must comply with reporting obligations on security incidents |
| | Member States shall ensure entities promptly notify CSIRTs or authorities of significant incidents |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | For significant cross-border or cross-sector incidents, Member States must promptly notify their single points of contact |
| | Member States shall ensure entities promptly notify CSIRTs or authorities of significant incidents |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Entities must implement cybersecurity risk-management measures |
| | Member States shall ensure entities implement measures to manage cybersecurity risks and minimize incident impact |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Entities and authorities must share cybersecurity threat intelligence |
| | Member States shall enable relevant entities to voluntarily share cybersecurity information, including threats, vulnerabilities, and attack indicators |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | MSs must establish national cybersecurity strategies |
| | Member States shall adopt a national cybersecurity strategy outlining objectives, resources, and measures to ensure high cybersecurity levels |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | MSs must designate competent authorities, CSIRTs, and single points of contact |
| | Member States shall adopt a national cybersecurity strategy outlining objectives, resources, and measures to ensure high cybersecurity levels |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Member States shall adopt a national cybersecurity strategy outlining objectives, resources, and measures to ensure high cybersecurity levels |
| | National Cybersecurity Strategy |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Member States shall enable relevant entities to voluntarily share cybersecurity information, including threats, vulnerabilities, and attack indicators |
| | Information Sharing |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Member States shall ensure entities implement measures to manage cybersecurity risks and minimize incident impact |
| | Risk Management |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Member States shall ensure entities promptly notify CSIRTs or authorities of significant incidents |
| | Reporting Obligations |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive |
| | Supervision and Enforcement |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Cybersecurity information-sharing arrangement |
| **Target** | enhance the level of cybersecurity |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Enhance the overall level of cybersecurity across the European Union |
| **Target** | Supervision and Enforcement |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Enhance the overall level of cybersecurity across the European Union |
| **Target** | Information Sharing |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Enhance the overall level of cybersecurity across the European Union |
| **Target** | Reporting Obligations |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Enhance the overall level of cybersecurity across the European Union |
| **Target** | Risk Management |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Enhance the overall level of cybersecurity across the European Union |
| **Target** | National Cybersecurity Strategy |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Enhance the overall level of cybersecurity across the European Union |
| **Target** | Cybersecurity |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Entity Information |
| **Target** | Entity Name |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Biennial |
| **Target** | Adopt report |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Appoint main crisis coordinator |
| **Target** | Implement plan |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Cyber crisis management authority |
| **Target** | Implement plan |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Implement plan |
| **Target** | Notify of coordinator and plan |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Notify of coordinator and plan |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Cyber crisis management authority |
| **Target** | Management of large-scale cybersecurity incidents and crises |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| | Notification of significant incidents, incidents, cyber threats or near misses |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | Entity |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | NIS2 cross-sector coordination |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Identify and contact the entities concerned |
| **Target** | Responsible Disclosure Management |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | Assist reporter in disclosure process |
| **Target** | Responsible Disclosure Management |

## Influence relation

| | |
|---|---|
| **Type** | Influence relation |
| **Source** | Coordinator CSIRT |
| **Target** | Trusted intermediary |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | EU-CyCLONe Core Behavior |
| **Target** | Relevant Secure Information Exchange |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | Cooperation Group Core Behavior |
| **Target** | Relevant Secure Information Exchange |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | International Agreement |
| **Target** | International Agreements Conclusion |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Committee |
| **Target** | Committee Procedure |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Committee Procedure |
| **Target** | Terminate procedure |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | NIS2 Single Point of Contact |
| **Target** | Liason Function |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Notify Parliament and Council of delegated act |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Publication in the Official Journal |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | within 2 months |
| **Target** | Raise objection |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Notify Parliament and Council of delegated act |
| **Target** | Raise objection |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Notify Parliament and Council of delegated act |
| **Target** | Delegation Act enters into force |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Committee Procedure |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | by 17 October 2027 and every 36 months thereafter |
| **Target** | Review NIS2 functioning |

## Flow relation

| | |
|---|---|
| **Type** | Flow relation |
| **Source** | Notify Commission of CSIRT |
| **Target** | European Commission |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cybersecurity Strategy |
| **Target** | Incident Coordination Service |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | every 18 months |
| **Target** | Develop EU-CyCLONe Work Assessment Report |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Develop EU-CyCLONe Work Assessment Report |
| **Target** | EU-CyCLONe Work Assessment Report |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | EU-CyCLONe Core Behavior |
| **Target** | Develop EU-CyCLONe Work Assessment Report |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Designate Cybersecurity Expert |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Designate Cybersecurity Expert |
| **Target** | Cybersecurity Expert |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | cooperation with eIDAS2 authorities |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | appropriate cooperation |
| **Target** | cooperation with eIDAS2 authorities |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | failure in the national power grid |
| **Target** | 11h30 CNCS  receives notification |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | 11h30 CNCS  receives notification |
| **Target** | Contacts counterparts in Spain, France, and the European Commission |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Portugal |
| **Target** | failure in the national power grid |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Contacts counterparts in Spain, France, and the European Commission |
| | Issues statements denying signs of cyberattacks and warning against misinformation on social media |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CNCS in action |
| **Target** | 11h30 CNCS  receives notification |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | CNCS in action |
| **Target** | Contacts counterparts in Spain, France, and the European Commission |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CNCS in action |
| | Issues statements denying signs of cyberattacks and warning against misinformation on social media |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | PT CNCS |
| **Target** | CNCS in action |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | CNCS in action |
| **Target** | European Commission |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| | Confirms coordination with Portuguese authorities and the ENTSO-E to investigate causes and coordinate a gradual power restoration plan |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Issues statements denying signs of cyberattacks and warning against misinformation on social media |
| | Confirms coordination with Portuguese authorities and the ENTSO-E to investigate causes and coordinate a gradual power restoration plan |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Publish a preliminary report |
| | Order a technical-strategic review to urgently modernize the SIRESP emergency communications system |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | File a formal complaint with the Public Prosecutor’s Office requesting investigation |
| | Address mobile network operators, demanding explanations for post-blackout voice and data service failures and information on backup power systems at cell towers |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | PT Government |
| | Order a technical-strategic review to urgently modernize the SIRESP emergency communications system |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | April 30 |
| | Issue renewed statements reaffirming no evidence of cyberattacks and urges media outlets to rely only on official sources |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CpC actions |
| | Report of an alleged sale of privileged access to energy infrastructures on the dark web, highlighting a possible link to the blackout |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | PT Citizens for Cybersecurity (CpC) |
| **Target** | CpC actions |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Issue renewed statements reaffirming no evidence of cyberattacks and urges media outlets to rely only on official sources |
| | Begin parallel technical investigation with CNCS and REN |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Report of an alleged sale of privileged access to energy infrastructures on the dark web, highlighting a possible link to the blackout |
| | File a formal complaint with the Public Prosecutor’s Office requesting investigation |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CpC actions |
| | File a formal complaint with the Public Prosecutor’s Office requesting investigation |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | PT Anacom |
| **Target** | Publish a preliminary report |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENTSO-E |
| | Concludes the blackout resulted from two successive frequency instabilities in the Iberian grid, undetected in time by synchronization systems |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CpC actions |
| | Address mobile network operators, demanding explanations for post-blackout voice and data service failures and information on backup power systems at cell towers |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | May 9 |
| | Concludes the blackout resulted from two successive frequency instabilities in the Iberian grid, undetected in time by synchronization systems |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | April 29 |
| | Report of an alleged sale of privileged access to energy infrastructures on the dark web, highlighting a possible link to the blackout |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | May 1 |
| **Target** | Publish a preliminary report |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Publish a preliminary report |
| **Target** | Preliminary report |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | SP INCIBE |
| **Target** | Begin parallel technical investigation with CNCS and REN |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |

| | |
|---|---|
| **Source** | Concludes the blackout resulted from two successive frequency instabilities in the Iberian grid, undetected in time by synchronization systems |
| | Close investigations |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | SP INCIBE |
| **Target** | Close investigations |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | PT CNCS |
| | Issue renewed statements reaffirming no evidence of cyberattacks and urges media outlets to rely only on official sources |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | PT CNCS |
| **Target** | Close investigations |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | June 25 |
| | Doubles “black start” capacity with additional power plants able to restart autonomously |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | June 25 |
| | Starts installation of battery systems in critical infrastructure (hospitals, communication stations) |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Government actions |
| | Doubles “black start” capacity with additional power plants able to restart autonomously |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Government actions |
| | Starts installation of battery systems in critical infrastructure (hospitals, communication stations) |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | PT Government |
| **Target** | Government actions |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | Near Miss |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | Cyber Threat |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | Significant Incident |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | National Cooperation |
| **Target** | Incident |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Processes |
| **Target** | Risk-based approach |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Processes |
| **Target** | Deployment of secure information-sharing tools |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Processes |
| **Target** | Cordinate vulnerability disclosure |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Requirements |
| **Target** | Redundant Communication Channels |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Requirements |
| **Target** | Request Management System |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Requirements |
| **Target** | Operational Confidentiality |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Requirements |
| **Target** | Secure Infrastructure |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Requirements |
| **Target** | Adequate and Trained Staffing |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Requirements |
| **Target** | Service Continuity and Backup |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | NIS2 CSIRT |
| **Target** | CSIRTs Core Requirements |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | CSIRTs Core Processes |
| **Target** | Take Standardised Practices for Cooperation |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENISA |
| **Target** | Develop and maintain European Vulnerability DB |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |

| | |
|---|---|
| **Source** | Develop and maintain European Vulnerability DB |
| **Target** | European Vulnerability Database |

### Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Cooperation Group Core Behavior |
| **Target** | Take security risk assessments |

### Flow relation

| | |
|---|---|
| **Type** | Flow relation |
| **Source** | Large-scale cybersecurity incident or crise MS request |
| **Target** | Take security risk assessments |

### Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Member State |
| | ensure effective, efficient and secure cooperation of their representatives in the Cooperation Group |

### Specialization relation

| | |
|---|---|
| **Type** | Specialization relation |
| **Source** | Member State Representative |
| **Target** | Member State |

### Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | NIS2 CSIRTs Network |
| **Target** | NIS2 CSIRT |

## Numbering: 3.15.2

### Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Core CSIRTs Network Behavior |
| **Target** | Incident |

### Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Incident |
| **Target** | Aid CSIRT |

### Flow relation

| | |
|---|---|
| **Type** | Flow relation |
| **Source** | Guarantee CSIRTs Cooperation |
| **Target** | Request of an individual CSIRT |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Relevant Secure Information Exchange |
| **Target** | Security Operations Centre |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |
| **Source** | Relevant Secure Information Exchange |
| **Target** | Member State |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Adopt report |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | European Commission |
| **Target** | Develop methodology |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRTs Network |
| **Target** | Develop methodology |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENISA |
| **Target** | Develop methodology |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Cooperation Group |
| **Target** | Develop methodology |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | EU-CyCLONe Core Behavior |
| **Target** | Adopt rules of procedure |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | Operational cooperation information handling |
| **Target** | Discuss and identify further forms of operational cooperation |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Operational cooperation information handling |
| **Target** | Assess the progress made |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Operational cooperation information handling |
| **Target** | Adopt a report |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Operational cooperation information handling |
| **Target** | Operational Cooperation Information |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Operational cooperation information handling |
| **Target** | Biennial |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Operational cooperation information handling |
| **Target** | Notify Cooperation Group |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Operational cooperation information handling |
| **Target** | Progress Report |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Operational cooperation information handling |
| **Target** | Report operations and activities |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRTs Network |
| **Target** | Operational cooperation information handling |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | EU-CyCLONe |
| **Target** | Large-scale cybersecurity incidents or crises handling |

## Flow relation

| | |
|---|---|
| **Type** | Flow relation |
| **Source** | Large-scale cybersecurity incident or crise |
| **Target** | Large-scale cybersecurity incident or crise MS request |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Large-scale cybersecurity incidents or crises handling |
| **Target** | Propose possible mitigation measures |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Large-scale cybersecurity incidents or crises handling |
| | Discuss national large-scale cybersecurity incident and crisis response plans |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Large-scale cybersecurity incidents or crises handling |
| | Coordinate management for large-scale cybersecurity incidents and crises |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Large-scale cybersecurity incidents or crises handling |
| **Target** | Report management and trends |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Large-scale cybersecurity incidents or crises handling |
| **Target** | Support decision-making at political level |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Large-scale cybersecurity incidents or crises handling |
| **Target** | Large-scale cybersecurity incident or crise |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | Large-scale cybersecurity incidents or crises handling |
| | Assess the consequences and impact for large-scale cybersecurity incidents and crises |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Large-scale cybersecurity incidents or crises handling |
| **Target** | Large-scale cybersecurity incident or crise MS request |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Large-scale cybersecurity incidents or crises handling |
| | Increase the level of preparedness of the management of large-scale cybersecurity incidents and crises |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Large-scale cybersecurity incidents or crises handling |
| | Develop a shared situational awareness for large-scale cybersecurity incidents and crises |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Take cybersecurity risk-management measure |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | People Training |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | Entity |
| **Target** | Important Entities |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | Entity |
| **Target** | Essential Entities |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Compliance Risk Assessment |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Compliance Risk Assessment |
| **Target** | Assess compliance with measure |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | ICT Group |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Require use of certified ICT * and Qualified Trust Services for compliance |
| | Define certification requirements for entities |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Significant Incident |
| **Target** | Notify recipients of service |

## Aggregation relation

| | |
|---|---|
| **Type** | Aggregation relation |
| **Source** | Determine Judisdiction |
| **Target** | Determination of main establishment for cybersecurity oversight |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Entity |
| **Target** | Registry of entities |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Submit Entity information |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | Notify changes to Competent Authority |

## Serving relation

| | |
|---|---|
| **Type** | Serving relation |

| | |
|---|---|
| **Source** | Notify competent authority of participation or withdrawal |
| **Target** | NIS2 Competent Authority |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Competent Authority |
| **Target** | Processing Notification |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Implement supervisory measure |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Essential Entity Supervision |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Implement enforcement measure |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Set out a detailed reasoning |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Notify entities concerned of their preliminary findings |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Supervisory measure |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |

| | |
|---|---|
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Proactive (ex ante) |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Automatic oversight; ongoing supervision |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 Competent Authority |
| | Supervisory and enforcement measures in relation to essential entities Core |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Establish Enforcement Deadline |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Suspend temporarily a certification or authorisation |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Temporarily prohibit key managers from their duties |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | shall comply with the rights of the defence and take account of the circumstances of each individual case |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Supervisory and enforcement measures in relation to essential entities Core |
| | Enforcement measure |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Implement supervisory measure |
| **Target** | Important Entity Supervision |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | Lay down rules and compliance to fines |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Lay down rules and compliance to fines |
| **Target** | Administrative fines |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Entity |
| **Target** | personal data breach incident |

## Realization relation

| | |
|---|---|
| **Type** | Realization relation |
| **Source** | NIS2 Competent Authority |
| **Target** | Joint supervisory actions |

## Triggering relation

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | April 28 |
| **Target** | failure in the national power grid |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Report on the state of cybersecurity |
| | Aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | ENISA |
| **Target** | Report on the state of cybersecurity |

## Assignment relation

| | |
|---|---|
| **Type** | Assignment relation |

| | |
|---|---|
| **Source** | NIS2 Competent Authority |
| **Target** | Carry out Cybersecurity maturity self-assessment |

## Access relation

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Carry out Cybersecurity maturity self-assessment |
| **Target** | Cybersecurity maturity self-assessment |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union |
| | Cybersecurity maturity self-assessment |

## Flow relation

| | |
|---|---|
| **Type** | Flow relation |
| **Source** | Member State |
| **Target** | NIS2 Competent Authority |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Maturity Levels |
| **Target** | Maturity Level 1 - Initial / Ad-hoc |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Maturity Levels |
| **Target** | Maturity Level 4 - Managed |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Maturity Levels |
| **Target** | Maturity Level 2 - Developing |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Maturity Levels |
| **Target** | Maturity Level 5 - Optimized |

## Composition relation

| | |
|---|---|
| **Type** | Composition relation |
| **Source** | Maturity Levels |
| **Target** | Maturity Level 3 - Defined |

## Association relation

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Cybersecurity maturity self-assessment |
| **Target** | Maturity Levels |

## Flow relation

| | |
|---|---|
| **Type** | Flow relation |
| **Source** | Entity |
| **Target** | Carry out Cybersecurity maturity self-assessment |

- They are the source of the data on cybersecurity capabilities, resources, and practices.
- They implement risk management measures (Art. 21) and incident reporting (Art. 24).
- Their performance and compliance feed into the national authority reports, which are then aggregated by ENISA.

## Specialization relation

| | |
|---|---|
| **Type** | Specialization relation |
| **Source** | Cybersecurity risk-management measures |
| **Target** | Cybersecurity risk-management measure |

## (composed of)

| | |
|---|---|
| **Type** | Association relation |
| **Source** | EU-CyCLONe |
| **Target** | Cyber crisis management authority |

Numbering: 3.16.2

## (composed of)

| | |
|---|---|
| **Type** | Association relation |
| **Source** | NIS2 CSIRTs Network |
| **Target** | EU CERT-EU |

Numbering: 3.15.2

## (if cross-border)

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Determine cross-border or cross-sectoral impact of the incident |
| **Target** | Notify SPC of cross-* incident |

## (impact >1 MSs)

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Notify SPC of cross-* incident |
| **Target** | Notify other MSs and ENISA |

Numbering: 4.23.6

(observer)

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Representative of relevant stakeholder |
| **Target** | EU-CyCLONe |

> Numbering: 3.16.2
>
> EU-CyCLONe may invite them

(triggers)

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Establish CSIRT |
| **Target** | Notify Commission of CSIRT |

(triggers)

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Establish CSIRT |
| **Target** | NIS2 CSIRT |

(upon request)

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENISA |
| **Target** | NCS Lifecycle |

access

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Stakeholder |
| **Target** | Vulnerability Information |

assistance

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | ENISA |
| **Target** | Cybersecurity information-sharing arrangement |

> Numbering: 6.29.5

could also be

| | |
|---|---|
| **Type** | Association relation |
| **Source** | NIS2 Competent Authority |
| **Target** | NIS2 Single Point of Contact |

> Numbering: 2.8.3
>
> Where a Member State designates or establishes only one competent authority pursuant to paragraph 1, that competent authority shall also be the single point of contact for that Member State.

### else

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Junction |
| **Target** | Implement enforcement measure |

### establish

| | |
|---|---|
| **Type** | Association relation |
| **Source** | Member State |
| **Target** | Entity |

### if entity comply

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Junction |
| **Target** | Take cybersecurity risk-management measure |

### if entity do not comply

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Junction |
| **Target** | Take appropriate and proportionate corrective measures |

### if entity is not compliant

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Essential Entity Supervision |
| **Target** | Implement enforcement measure |

### if entity outside EU

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Determine Judisdiction |
| **Target** | Appoint Jurisdiction Representative |

> Numbering: 5.26.3

### if significant impact

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | NIS2 CSIRTs Network |
| **Target** | Responsible Disclosure Management |

> Numbering: 2.12.1

### measure is ineffective

| | |
|---|---|
| **Type** | Triggering relation |
| **Source** | Junction |
| **Target** | Establish Enforcement Deadline |

Numbering: 7.32.5

## observe

| | |
|---|---|
| **Type** | Association relation |
| **Source** | European Commission |
| **Target** | NIS2 CSIRTs Network |

Numbering: 3.15.2

## observes

| | |
|---|---|
| **Type** | Association relation |
| **Source** | European External Action Service |
| **Target** | Cooperation Group Core Behavior |

Numbering: 3.14.3

## shall ensure

| | |
|---|---|
| **Type** | Assignment relation |
| **Source** | Member State |
| **Target** | National Cooperation |

Numbering: 2.13.*

## store inside

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Collect and maintain accurate and complete domain name registration data |
| | Database of domain name registration data |

## verify

| | |
|---|---|
| **Type** | Access relation |
| **Source** | Establish and publish domain data verification policies |
| **Target** | Database of domain name registration data |