NISTify ENERGY

E-LEARNING COURSE

Detaillierte Vorstellung der NCCS-Verordnung

NIS2U GmbH

1.0.0 – 02/02/2026

Contents

Chapter 1

Willkommen

Willkommen zur Einführung in das Schulungsmaterial zur Verordnung über den Netzkodex zur Cybersicherheit (NCCS)

Begeben Sie sich auf eine Reise, um die Komplexität der NCCS-Vorschriften mit unserem sorgfältig erstellten Schulungsmaterial zu meistern.

Ziel des Schulungsmaterials ist es, die Akteure im Elektrizitätssektor dabei zu unterstützen, sich mit den detaillierten Bestimmungen bestimmter Artikel der NCCS-Cybersicherheitsverordnung vertraut zu machen. Das Material stellt die Aufgaben der Beteiligten Artikel für Artikel dar, zeigt die Zusammenhänge zwischen einzelnen Artikeln auf und enthält einen Zeitplan der wichtigsten Aufgaben.

Detaillierte Bestimmungen: Ein vertiefter Blick auf ausgewählte Artikel der Verordnung.

Rollen und Verantwortlichkeiten: Welche Aufgaben und Pflichten die einzelnen Akteure im Elektrizitätssektor erfüllen müssen, um die Einhaltung sicherzustellen.

Zusammenhänge: Wie verschiedene Artikel und Bestimmungen ineinandergreifen und sich gegenseitig unterstützen.

Zeitplanung der Aufgaben: Ein Zeitplan für die Erledigung der wichtigsten Aufgaben.

Chapter 2

Einführung

Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates [1] legt Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union fest. Verordnung (EU) 2019/941 des Europäischen Parlaments und des Rates [2] ergänzt die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates [3], indem sie sicherstellt, dass Cybersicherheitsvorfälle im Elektrizitätssektor ordnungsgemäß als Risiko identifiziert werden und dass die zu ihrer Bewältigung ergriffenen Maßnahmen angemessen in den Risikovorsorgeplänen berücksichtigt werden. Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates [4] ergänzt die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates [5] und die Verordnung (EU) 2019/941 des Europäischen Parlaments und des Rates [6], indem sie auf Unionsebene spezifische Vorschriften für den Elektrizitätssektor festlegt. Darüber hinaus ergänzt diese delegierte Verordnung die Bestimmungen der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates [7] für den Elektrizitätssektor, soweit grenzüberschreitende Stromflüsse betroffen sind.

Zu den zentralen Maßnahmen der Kommission gehört die Schaffung eines umfassenden Legislativrahmens, der auf Folgendem aufbaut: the EU-Cybersicherheitsstrategie (JOIN/2013/01) [8] the Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates [9] the Cybersicherheitspaket (JOIN/2017/450 final) [10] vom September 2017, das auch den Cybersicherheitsakt umfasst

- NCCS ist am 13. Juni 2024 in Kraft getreten.
- Ein delegierter Rechtsakt der Europäischen Kommission ist **in allen EU-Mitgliedstaaten unmittelbar anwendbar und rechtlich bindend.**

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[4] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[5] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[8] https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1553779410177&uri=CELEX:52013JC0001
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[10] https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN

- NCCS legt **sektorspezifische Vorschriften** für **Cybersicherheits**-Aspekte grenzüberschreitender Stromflüsse fest.
- NCCS **ergänzt andere europäische Cybersicherheitsvorschriften**, insbesondere Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates [11], soweit grenzüberschreitende Stromflüsse betroffen sind.

Die **ENTSO-E** (Europäisches Netz der Übertragungsnetzbetreiber für Strom) hat in Zusammenarbeit mit der **EU DSO** (Europäische Organisation der Verteilernetzbetreiber) eine **vorläufige Liste unionsweiter Prozesse mit hohen und kritischen Auswirkungen** erstellt.

Die vorläufige Liste der Prozesse ist über die folgenden Links abrufbar:

> FILE 1
>
> Vorläufige Liste unionsweiter Prozesse mit hohen und kritischen Auswirkungen (Englisch)
>
> **files/Provisional list of Union-wide high-impact and critical-impact processes.pdf**

Das **begleitende methodische Dokument** enthält zusätzliche Informationen und Begründungen zu den aufgeführten Prozessen.

> FILE 2
>
> Begleitdokument zur vorläufigen Liste unionsweiter Prozesse mit hohen und kritischen Auswirkungen (Englisch)
>
> **files/Supporting document Provisional list of Union-wide high-impact and critical-impact processes.pdf**

Im Rahmen des NCCS hat **ENTSO-E** in Zusammenarbeit mit der **EU DSO** einen **vorläufigen Electricity Cybersecurity Impact Index (ECII) sowie Schwellenwerte für die Kategorien „hohe Auswirkungen" und „kritische Auswirkungen"** entwickelt.

Der vorläufige Electricity Cybersecurity Impact Index (ECII) kann über die folgenden Links aufgerufen werden:

> FILE 3
>
> Vorläufiger Electricity Cybersecurity Impact Index (ECII) (Englisch)
>
> **files/Provisional ECII.pdf**

Das **begleitende methodische Dokument** enthält zusätzliche Informationen und Begründungen zum ECII.

[11] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555

FILE 4

Begleitdokument zum vorläufigen Electricity Cybersecurity Impact Index (ECII) (Englisch)

files/Supporting document provisional ECII.pdf

Im weiteren Verlauf des Schulungsmaterials besteht die Möglichkeit, den Inhalt der NCCS-Verordnung umfassend, Absatz für Absatz, zu analysieren.

- **Vorwärts- und Zurück-Schaltflächen:** Verwenden Sie die Navigationsschaltflächen am unteren Seitenrand, um das Schulungsmaterial Schritt für Schritt durchzugehen.
- **Schriftliches Inhaltsverzeichnis links:** Bietet schnellen Zugriff auf einzelne Abschnitte und Teile.
- **Oberes Menü:** Von jeder Stelle im Schulungsmaterial können Sie zur Startseite zurückkehren. Dort können Sie die Artikel der NCCS-Verordnung in einer Kachelansicht anzeigen.

2.1 Interessenträger

Bei der Bearbeitung des Studienmaterials können Ihnen mehrere Akteure begegnen, die an der NCCS-Verordnung beteiligt sind. Es ist sinnvoll, diese vor Beginn des Lernprozesses kennenzulernen.

2.1.1 A

TERM

Anbieter kritischer IKT-Dienste

Bezeichnet eine Einrichtung, die einen IKT-Dienst oder einen IKT-Prozess bereitstellt, der für einen Prozess mit kritischen oder erheblichen Auswirkungen, der sich auf Cybersicherheitsaspekte grenzüberschreitender Stromflüsse auswirkt, erforderlich ist und bei dessen Kompromittierung ein Cyberangriff erfolgen könnte, dessen Auswirkungen den Schwellenwert für kritische oder erhebliche Auswirkungen überschreiten.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER)

Eine spezialisierte Agentur der Europäischen Union, die für die Förderung der Integration und des effizienten Funktionierens der EU-Energiemärkte zuständig ist.

https://www.acer.europa.eu/ [a]

VERORDNUNG (EU) 2019/942 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [b]

[a] https://www.acer.europa.eu/
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942

TERM

Agentur der Europäischen Union für Cybersicherheit (ENISA)

ENISA ist die Cybersicherheitsagentur der EU und unterstützt die Mitgliedstaaten bei der Abwehr von Cyberbedrohungen.

2.1.2 B

TERM

Benannter Strommarktbetreiber (NEMO)

Ein Marktteilnehmer, der von der zuständigen Behörde eines Mitgliedstaats benannt wurde, um an der Kopplung des einheitlichen Day-Ahead-Markts oder des einheitlichen Intraday-Markts teilzunehmen.

2.1.3 C

TERM

Computer-Notfallteams (CSIRT)

Eine Organisation, die für das Management von Sicherheitsvorfällen in Netz- und Informationssystemen zuständig ist. RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555

TERM

Cybersicherheit zuständigen Behörden (CS NCA)

Die nationale zuständige Behörde für Cybersicherheit in einem bestimmten Mitgliedstaat.

2.1.4 D

TERM

DG CONNECT (Generaldirektion Kommunikationsnetze, Inhalte und Technologien der Europäischen Kommission)

Die Generaldirektion Kommunikationsnetze, Inhalte und Technologien (DG CONNECT) entwickelt und implementiert die politischen Maßnahmen der Europäischen Kommission.

TERM

DG ENER (Generaldirektion Energie der Europäischen Kommission)

Die Generaldirektion Energie der Europäischen Kommission ist für die Energiepolitik der EU verantwortlich.

2.1.5 E

TERM

Europäische Kommission (EC)

Die Europäische Kommission ist das Exekutivorgan der Europäischen Union und verantwortlich für die Umsetzung der EU-Rechtsvorschriften, die Entwicklung von Politiken und die Verwaltung des Haushalts.

TERM

Elektrizitätskoordinierungsgruppe (ECG)

Ziel der Elektrizitätskoordinierungsgruppe ist es, Informationen über strompolitische Maßnahmen mit grenzüberschreitenden Auswirkungen auszutauschen und zu koordinieren und die Zusammenarbeit durch Wissens- und Erfahrungsaustausch zu erleichtern.

KOMMISSIONSENTSCHEIDUNG 2012/C 353/02 [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32012D1117(01)

TERM

Einrichtung mit erheblichen Auswirkungen (HIE)

Bezeichnet eine Einrichtung, die einen Prozess mit erheblichen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24 [a] ermittelt wird.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [b]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_24
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

Einrichtung mit kritischen Auswirkungen (CIE)

Bezeichnet eine Einrichtung, die einen Prozess mit kritischen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24 [a] bestimmt wird.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [b]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_24
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

EU-VNBO (EU DSO)

Europäische Organisation der Verteilnetzbetreiber

Die EU-VNBO wurde von der Europäischen Union gegründet, um die Koordinierung und Entwicklung der Stromverteilungsnetze zu fördern. Sie spielt eine zentrale Rolle bei der Integration der Energiemärkte, der Einbindung erneuerbarer Energiequellen und der Unterstützung der Energiewende.

Die Aktivitäten der EU-VNBO werden durch das EU-Paket „Saubere Energie“ und die Strommarktverordnung (Verordnung (EU) 2019/943) geregelt.

https://eudsoentity.eu/ [a]

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [b]

[a] https://eudsoentity.eu/
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943

2.1.6 K

TERM

Kooperationsgruppe für Netz- und Informationssysteme (NIS CG)

Kooperationsgruppe für Cybersicherheit

Die Kooperationsgruppe für Netz- und Informationssicherheit (NIS CG) koordiniert die Cybersicherheitszusammenarbeit in der EU. Die Aufgaben der NIS-Kooperationsgruppe sind in Artikel 11 der NIS-Richtlinie festgelegt.

DURCHFÜHRUNGSBESCHLUSS (EU) 2017/179 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32017D0179

2.1.7 M

TERM

Mitgliedstaat (MS)

Bezeichnet ein Land, das Mitglied der Europäischen Union ist und das EU-Recht einhält.

2.1.8 N

TERM

Nationale zuständige Behörde (NCA)

Eine nationale zuständige Behörde ist eine offizielle Stelle oder Organisation, die durch Rechtsvorschriften befugt ist, einen bestimmten Sektor oder Bereich zu regeln, zu überwachen und zu kontrollieren. Diese Behörden stellen die Einhaltung nationaler und gegebenenfalls internationaler Gesetze und Standards sicher.

TERM

Nationale Regulierungsbehörden (NRA)

Eine offizielle staatliche oder unabhängige Organisation, die für die Regulierung, Überwachung und Kontrolle bestimmter Bereiche innerhalb eines Landes oder einer Region zuständig ist.

2.1.9 R

TERM

Regionale Koordinierungszentren (RCC)

Regionale Koordinierungszentren (RCC) haben eine beratende Rolle bei der Entwicklung regionaler Cybersicherheitsrisikobewertungen und -minderungspläne und koordinieren die Zusammenarbeit der Mitgliedstaaten im Bereich der Cybersicherheit.

Eingerichtet gemäß Artikel 35 der Verordnung (EU) 2019/943.

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943

TERM

Risikovorsorge zuständigen Behörden (RP-NCA)

Die RP-NCA ist für die Entwicklung und Umsetzung von Risikovorsorgeplänen zuständig.

2.1.10 S

TERM

Systembetreiber

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung eines Übertragungs- oder Verteilernetzes verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944

2.1.11 Ü

TERM

Übertragungsnetzbetreiber (TSO)

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung des Übertragungsnetzes in einem bestimmten Gebiet sowie dessen Verbindung mit anderen Netzen und die langfristige Fähigkeit zur Deckung eines angemessenen Bedarfs an Stromübertragung verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944

2.1.12 V

TERM

Verband Europäischer Übertragungsnetzbetreiber (ENTSO-E)

Gemeinsame Organisation der europäischen Übertragungsnetzbetreiber. Sie spielt eine zentrale Rolle bei der Integration des europäischen Strommarktes und der Sicherstellung der Stabilität des Stromsystems.

Die Aktivitäten von ENTSO-E werden durch das EU-Paket „Saubere Energie“ und die Strommarktverordnung (Verordnung (EU) 2019/943) geregelt.

https://www.entsoe.eu/ [a]

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [b]

[a] https://www.entsoe.eu/
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943

TERM

Verteilnetzbetreiber (DSO)

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung eines Verteilernetzes in einem bestimmten Gebiet sowie für die langfristige

Fähigkeit zur Deckung gerechtfertigter Stromverteilungsanforderungen verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944

NOTE

TERM

Artikel 2: Anwendungsbereich

1. Diese Verordnung gilt für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse bei den Tätigkeiten der folgenden Einrichtungen, soweit diese gemäß Artikel 24 [a] als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft werden:

   a. Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944; [b]
   b. nominierte Strommarktbetreiber (NEMOs) im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/943; [c]
   c. organisierte Marktplätze oder organisierte Märkte im Sinne des Artikels 2 Nummer 4 der Durchführungsverordnung (EU) Nr. 1348/2014 der Kommission [d] (14), die Transaktionen mit Produkten arrangieren, die für grenzüberschreitende Stromflüsse relevant sind;
   d. Anbieter kritischer IKT-Dienste im Sinne des Artikels 3 Nummer 9 dieser Verordnung [e]
   e. ENTSO-E, das gemäß Artikel 28 der Verordnung (EU) 2019/943 [f] eingerichtet wurde;
   f. die EU-VNBO, die gemäß Artikel 52 der Verordnung (EU) 2019/943 [g] eingerichtet wurde;
   g. Bilanzkreisverantwortliche im Sinne des Artikels 2 Nummer 14 der Verordnung (EU) 2019/943; [h]
   h. Betreiber von Ladepunkten im Sinne des Anhangs I der Richtlinie (EU) 2022/2555; [i]
   i. regionale Koordinierungszentren (RCC) gemäß Artikel 35 der Verordnung (EU) 2019/943; [j]
   j. Anbieter verwalteter Sicherheitsdienste (MSSP) gemäß Artikel 6 Nummer 40 der Richtlinie (EU) 2022/2555; [k]
   k. alle sonstigen Einrichtungen oder Dritte, denen gemäß dieser Verordnung [l] Zuständigkeiten übertragen oder zugewiesen werden.

2. Die folgenden Behörden sind im Rahmen ihres derzeitigen Auftrags für die Wahrnehmung der in dieser Verordnung [m] festgelegten Aufgaben zuständig:

   a. die mit der Verordnung (EU) 2019/942 des Europäischen Parlaments und des Rates [n] eingerichtete Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER)
   b. die nationalen zuständigen Behörden, die für die Wahrnehmung der ihnen gemäß dieser Verordnung [o] übertragenen Aufgaben verantwortlich sind und von den Mitgliedstaaten gemäß Artikel 4 als „zuständige Behörde“ benannt wurden;
   c. die gemäß Artikel 57 Absatz 1 der Richtlinie (EU) 2019/944; [p] benannten nationalen Regulierungsbehörden (NRB) der einzelnen Mitgliedstaaten;
   d. die gemäß Artikel 3 der Verordnung (EU) 2019/941; [q] benannten für die Risikovorsorge zuständigen Behörden (RP-NCA);
   e. die gemäß Artikel 10 der Richtlinie (EU) 2022/2555; [r] benannten oder eingerichteten Computer-Notfallteams (CSIRTs);
   f. die gemäß Artikel 8 der Richtlinie (EU) 2022/2555; [s] benannten oder eingerichteten für die Cybersicherheit zuständigen Behörden (CS-NCA);
   g. die gemäß der Verordnung (EU) 2019/881 [t]; errichtete Agentur der Europäischen Union für Cybersicherheit;

TERM

Artikel 2: Anwendungsbereich

1. Diese Verordnung gilt für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse bei den Tätigkeiten der folgenden Einrichtungen, soweit diese gemäß Artikel 24 [a] als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft werden:

   a. Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944; [b]

   b. nominierte Strommarktbetreiber (NEMOs) im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/943; [c]

   c. organisierte Marktplätze oder organisierte Märkte im Sinne des Artikels 2 Nummer 4 der Durchführungsverordnung (EU) Nr. 1348/2014 der Kommission [d] (14), die Transaktionen mit Produkten arrangieren, die für grenzüberschreitende Stromflüsse relevant sind;

   d. Anbieter kritischer IKT-Dienste im Sinne des Artikels 3 Nummer 9 dieser Verordnung [e]

   e. ENTSO-E, das gemäß Artikel 28 der Verordnung (EU) 2019/943 [f] eingerichtet wurde;

   f. die EU-VNBO, die gemäß Artikel 52 der Verordnung (EU) 2019/943 [g] eingerichtet wurde;

   g. Bilanzkreisverantwortliche im Sinne des Artikels 2 Nummer 14 der Verordnung (EU) 2019/943; [h]

   h. Betreiber von Ladepunkten im Sinne des Anhangs I der Richtlinie (EU) 2022/2555; [i]

   i. regionale Koordinierungszentren (RCC) gemäß Artikel 35 der Verordnung (EU) 2019/943; [j]

   j. Anbieter verwalteter Sicherheitsdienste (MSSP) gemäß Artikel 6 Nummer 40 der Richtlinie (EU) 2022/2555; [k]

   k. alle sonstigen Einrichtungen oder Dritte, denen gemäß dieser Verordnung [l] Zuständigkeiten übertragen oder zugewiesen werden.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[c] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[d] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R1348
[e] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_3
[f] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[g] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[h] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[i] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art
[j] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[k] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[l] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

TERM

Artikel 2: Anwendungsbereich

1. Die folgenden Behörden sind im Rahmen ihres derzeitigen Auftrags für die Wahrnehmung der in dieser Verordnung [a] festgelegten Aufgaben zuständig:

   a. die mit der Verordnung (EU) 2019/942 des Europäischen Parlaments und des Rates [b] eingerichtete Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER)

   b. die nationalen zuständigen Behörden, die für die Wahrnehmung der ihnen gemäß dieser Verordnung [c] übertragenen Aufgaben verantwortlich sind und von den Mitgliedstaaten gemäß Artikel 4 als „zuständige Behörde“ benannt wurden;

   c. die gemäß Artikel 57 Absatz 1 der Richtlinie (EU) 2019/944; [d] benannten nationalen Regulierungsbehörden (NRB) der einzelnen Mitgliedstaaten;

   d. die gemäß Artikel 3 der Verordnung (EU) 2019/941; [e] benannten für die Risikovorsorge zuständigen Behörden (RP-NCA);

   e. die gemäß Artikel 10 der Richtlinie (EU) 2022/2555; [f] benannten oder eingerichteten Computer-Notfallteams (CSIRTs);

   f. die gemäß Artikel 8 der Richtlinie (EU) 2022/2555; [g] benannten oder eingerichteten für die Cybersicherheit zuständigen Behörden (CS-NCA);

   g. die gemäß der Verordnung (EU) 2019/881 [h]; errichtete Agentur der Europäischen Union für Cybersicherheit;

   h. alle sonstigen Behörden oder Dritte, denen gemäß Artikel 4 Absatz 3 [i] Zuständigkeiten übertragen oder zugewiesen werden.

2. Diese Verordnung gilt auch für alle Einrichtungen, die nicht in der Union niedergelassen sind, aber Dienstleistungen für Einrichtungen in der Union erbringen, sofern sie von den zuständigen Behörden gemäß Artikel 24 Absatz 2 [j] als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

3. Diese Verordnung lässt die Zuständigkeit der Mitgliedstaaten in Bezug auf die Aufrechterhaltung der nationalen Sicherheit und ihre Befugnis zum Schutz anderer wesentlicher staatlicher Funktionen, einschließlich der Wahrung der territorialen Unversehrtheit des Staates und der Aufrechterhaltung der öffentlichen Ordnung, unberührt.

4. Diese Verordnung lässt die Zuständigkeit der Mitgliedstaaten für die Aufrechterhaltung der nationalen Sicherheit in Bezug auf Tätigkeiten zur Stromerzeugung in Kernkraftwerken, einschließlich Tätigkeiten innerhalb der nuklearen Wertschöpfungskette, im Einklang mit den Verträgen unberührt.

5. Soweit dies für die Zwecke dieser Verordnung erforderlich ist, werden personenbezogene Daten von Einrichtungen, den zuständigen Behörden, den zentralen Anlaufstellen auf Ebene der Einrichtung und den CSIRTs im Einklang mit der Verordnung (EU) 2016/679 [k], insbesondere auf der Grundlage von Artikel 6 der genannten Verordnung, verarbeitet.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942
[c] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[d] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[e] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941
[f] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[g] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[h] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881
[i] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[j] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[k] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679

TERM

Artikel 4

1. So bald wie möglich, in jedem Fall aber bis zum 13 Dezember 2024, benennt jeder Mitgliedstaat eine nationale Regierungs- oder Regulierungsbehörde, die für die Wahrnehmung der ihr in dieser Verordnung übertragenen Aufgaben zuständig ist (im Folgenden „zuständige Behörde“). Bis die Aufgaben im Rahmen dieser Verordnung auf die zuständige Behörde übertragen wurden, nimmt die von jedem Mitgliedstaat gemäß Artikel 57 Absatz 1 der Richtlinie (EU) 2019/944 [a] benannte Regulierungsbehörde die Aufgaben der zuständigen Behörde im Einklang mit dieser Verordnung wahr.

2. Die Mitgliedstaaten unterrichten die Kommission, die ACER, die ENISA, die gemäß Artikel 14 der Richtlinie (EU) 2022/2555 [b] eingesetzte NIS-Kooperationsgruppe und die gemäß Artikel 1 des Beschlusses der Kommission vom 15. November 2012 [c] eingesetzte Koordinierungsgruppe „Strom“ unverzüglich und teilen ihnen den Namen und die Kontaktdaten ihrer gemäß Absatz 1 des vorliegenden Artikels benannten zuständigen Behörde sowie etwaige spätere Änderungen in Bezug auf diese Behörde mit.

3. Die Mitgliedstaaten können ihrer zuständigen Behörde gestatten, Aufgaben, die ihr in dieser Verordnung übertragen wurden, an andere nationale Behörden zu delegieren, mit Ausnahme der in Artikel 5 aufgeführten Aufgaben. Jede zuständige Behörde überwacht die Anwendung dieser Verordnung durch die Behörden, an die sie Aufgaben delegiert hat. Die zuständige Behörde teilt der Kommission, der ACER, der Koordinierungsgruppe „Strom“, der ENISA und der NISKooperationsgruppe den Namen der Behörden, an die sie Aufgaben delegiert hat, deren Kontaktdaten, die ihnen übertragenen Aufgaben sowie etwaige spätere Änderungen mit.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02019L0944-20240716#art_57
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_14
[c] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32012D1117(01)

TERM

Artikel 5

Die zuständigen Behörden koordinieren und gewährleisten eine angemessene Zusammenarbeit zwischen den für Cybersicherheit zuständigen Behörden, den Behörden für das Cyberkrisenmanagement, den NRB, den für die Risikovorsorge zuständigen Behörden und den CSIRTs im Hinblick auf die Erfüllung der in dieser Verordnung festgelegten einschlägigen Verpflichtungen. Zudem stimmen sich die zuständigen Behörden mit anderen von den einzelnen Mitgliedstaaten bestimmten Stellen oder Behörden ab, um effiziente Verfahren sicherzustellen und Überschneidungen von Aufgaben und Pflichten zu vermeiden. Die zuständigen Behörden können die jeweiligen NRB anweisen, die ACER gemäß Artikel 8 Absatz 3 um eine Stellungnahme zu ersuchen.

TERM

Artikel 6

1. Die ÜNB entwickeln in Zusammenarbeit mit der EU-VNBO Vorschläge für die Modalitäten oder Methoden gemäß Absatz 2 bzw. für Pläne gemäß Absatz 3.
2. Die folgenden Modalitäten oder Methoden und etwaige Änderungen dieser Modalitäten oder Methoden bedürfen der Genehmigung aller zuständigen Behörden:
   a. die Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 18 Absatz 1;
   b. der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23;
   c. die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen gemäß Artikel 29, der Vergleich der Cybersicherheitskontrollen im Elektrizitätssektor anhand von Normen gemäß Artikel 34, einschließlich Mindest-Cybersicherheitskontrollen und erweiterter Cybersicherheitskontrollen in der Lieferkette gemäß Artikel 33;
   d. eine Empfehlung für die Cybersicherheit bei der Auftragsvergabe gemäß Artikel 35;
   e. die Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8.
3. Die Vorschläge für die regionalen Pläne zur Minderung des Cybersicherheitsrisikos gemäß Artikel 22 bedürfen der Genehmigung aller zuständigen Behörden der betreffenden Netzbetriebsregion.
4. Die Vorschläge für Modalitäten oder Methoden gemäß Absatz 2 bzw. für Pläne gemäß Absatz 3 müssen einen Vorschlag für den Zeitplan für ihre Umsetzung und eine Beschreibung ihrer erwarteten Auswirkungen auf die Ziele dieser Verordnung enthalten.
5. Die EU-VNBO kann den betreffenden ÜNB bis zu drei Wochen vor Ablauf der Frist für die Übermittlung des Vorschlags für Modalitäten, Methoden oder Pläne an die zuständigen Behörden eine mit Gründen versehene Stellungnahme übermitteln. Die für den Vorschlag für Modalitäten, Methoden oder Pläne zuständigen ÜNB berücksichtigen die mit Gründen versehene Stellungnahme der EU-VNBO, bevor sie den Vorschlag den zuständigen Behörden zur Genehmigung vorlegen. Wenn die ÜNB die Stellungnahme der EU-VNBO nicht berücksichtigen, begründen sie dies.
6. Bei der gemeinsamen Entwicklung von Modalitäten, Methoden und Plänen arbeiten die teilnehmenden ÜNB eng zusammen. Die ÜNB unterrichten die zuständigen Behörden und die ACER mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO regelmäßig über die Fortschritte bei der Entwicklung der Modalitäten, Methoden oder Pläne.

TERM

Artikel 7

1. Können ÜNB bei der Entscheidung über Vorschläge für Modalitäten oder Methoden keine Einigung erzielen, so entscheiden sie mit qualifizierter Mehrheit. Die qualifizierte Mehrheit für diese Vorschläge wird wie folgt berechnet:

   a. ÜNB, die mindestens 55 % der Mitgliedstaaten vertreten, und

   b. ÜNB, die Mitgliedstaaten vertreten, die mindestens 65 % der Bevölkerung der Union umfassen.

2. Eine Sperrminorität bei Entscheidungen über Vorschläge für in Artikel 6 Absatz 2 aufgeführte Modalitäten oder Methoden ist mit ÜNB erreicht, die mindestens vier Mitgliedstaaten vertreten; andernfalls gilt die qualifizierte Mehrheit als erreicht.

3. Können ÜNB einer Netzbetriebsregion bei der Entscheidung über Vorschläge für die in Artikel 6 Absatz 2 genannten Pläne keine Einigung erzielen und besteht die betreffende Netzbetriebsregion aus mehr als fünf Mitgliedstaaten, so entscheiden die ÜNB mit qualifizierter Mehrheit. Bei Vorschlägen gemäß Artikel 6 Absatz 2 ist für eine qualifizierte Mehrheit folgende Mehrheit erforderlich:

   a. ÜNB, die mindestens 72 % der betroffenen Mitgliedstaaten vertreten, und

   b. ÜNB, die Mitgliedstaaten vertreten, die mindestens 65 % der Bevölkerung der betroffenen Region umfassen.

4. Eine Sperrminorität für Entscheidungen über Vorschläge für die Pläne muss eine Mindestanzahl von ÜNB umfassen, die mehr als 35 % der Bevölkerung der teilnehmenden Mitgliedstaaten vertreten, zuzüglich ÜNB, die mindestens einen weiteren betroffenen Mitgliedstaat vertreten; ansonsten gilt die qualifizierte Mehrheit als erreicht.

5. Bei Entscheidungen der ÜNB über Vorschläge für in Artikel 6 Absatz 2 aufgeführte Modalitäten oder Methoden erhält jeder Mitgliedstaat eine Stimme. Gibt es im Hoheitsgebiet eines Mitgliedstaats mehr als einen ÜNB, teilt der Mitgliedstaat die Stimmrechte unter den ÜNB auf.

6. Legen ÜNB den jeweils zuständigen Behörden nicht innerhalb der in dieser Verordnung festgelegten Fristen in Zusammenarbeit mit der EU-VNBO einen ersten oder geänderten Vorschlag für Modalitäten oder Methoden oder für Pläne vor, so übermitteln sie den jeweils zuständigen Behörden und der ACER entsprechende Entwürfe der Modalitäten oder Methoden bzw. der Pläne. Sie erläutern, warum keine Einigung erzielt wurde. Die zuständigen Behörden treffen gemeinsam geeignete Maßnahmen für die Annahme der erforderlichen Modalitäten oder Methoden bzw. der erforderlichen Pläne. Dies kann z. B. durch Ersuchen um Änderungen der Entwürfe gemäß diesem Absatz, durch Überarbeitung und Vervollständigung dieser Entwürfe oder, falls keine Entwürfe vorgelegt wurden, durch Festlegung und Genehmigung der erforderlichen Modalitäten, Methoden oder Pläne erfolgen.

TERM

Artikel 8

1. Die ÜNB legen den jeweils zuständigen Behörden innerhalb der in den Artikeln 18, 23, 29, 33, 34, 35 und 37 festgelegten Fristen die Vorschläge für Modalitäten oder Methoden bzw. für Pläne zur Genehmigung vor. Die zuständigen Behörden können diese Fristen in Ausnahmefällen gemeinsam verlängern, insbesondere wenn eine Frist aufgrund von Umständen außerhalb des Verantwortungsbereichs der ÜNB oder der EU-VNBO nicht eingehalten werden kann.

2. Vorschläge für Modalitäten, Methoden oder bzw. Pläne gemäß Absatz 1 werden zeitgleich mit der Übermittlung an die zuständigen Behörden auch der ACER zur Information vorgelegt.

3. Auf gemeinsames Ersuchen der NRB gibt die ACER innerhalb von sechs Monaten nach Eingang des Vorschlags für Modalitäten oder Methoden oder für die Pläne eine Stellungnahme zu dem Vorschlag ab und übermittelt sie den NRB und den zuständigen Behörden. Die NRB, die CS-NCA und alle anderen als zuständige Behörden benannten Behörden stimmen sich untereinander ab, bevor die NRB die ACER um eine Stellungnahme ersuchen. Die ACER kann in dieser Stellungnahme Empfehlungen abgeben. Die ACER konsultiert die ENISA, bevor sie eine Stellungnahme zu den in Artikel 6 Absatz 2 aufgeführten Vorschlägen abgibt.

4. Die zuständigen Behörden konsultieren einander, arbeiten eng zusammen und stimmen sich untereinander ab, um zu einer Einigung über die vorgeschlagenen Modalitäten, Methoden oder Pläne zu gelangen. Vor der Genehmigung der Modalitäten oder Methoden oder der Pläne überarbeiten und ergänzen sie die Vorschläge nach Konsultation von ENTSO-E und der EU-VNBO erforderlichenfalls, um sicherzustellen, dass die Vorschläge mit dieser Verordnung im Einklang stehen und zu einem hohen gemeinsamen Cybersicherheitsniveau in der gesamten Union beitragen.

5. Die zuständigen Behörden entscheiden über die Modalitäten oder Methoden oder die Pläne innerhalb von sechs Monaten nach Eingang der Modalitäten oder Methoden bzw. der Pläne bei der jeweils zuständigen Behörde oder gegebenenfalls bei der letzten betroffenen zuständigen Behörde.

6. Gibt die ACER eine Stellungnahme ab, so tragen die jeweils zuständigen Behörden dieser Stellungnahme Rechnung und treffen ihre Entscheidungen innerhalb von sechs Monaten nach Eingang der Stellungnahme.

7. Verlangen die zuständigen Behörden für ihre Genehmigung gemeinsam eine Änderung der vorgeschlagenen Modalitäten oder Methoden oder der Pläne, so entwickeln die ÜNB in Zusammenarbeit mit der EU-VNBO einen Vorschlag für eine solche Änderung der Modalitäten oder Methoden bzw. der Pläne. Die ÜNB legen den zuständigen Behörden den geänderten Vorschlag innerhalb von zwei Monaten nach deren Aufforderung zur Genehmigung vor. Die zuständigen Behörden entscheiden über die geänderten Modalitäten oder Methoden oder Pläne innerhalb von zwei Monaten nach deren Vorlage.

8. Konnten die zuständigen Behörden innerhalb der in Absatz 5 oder Absatz 7 genannten Frist keine Einigung erzielen, so unterrichten sie die Kommission. Die Kommission kann geeignete Maßnahmen ergreifen, um die Annahme der erforderlichen Modalitäten, Methoden oder Pläne zu ermöglichen.

9. Die ÜNB veröffentlichen mit Unterstützung von ENTSO-E und der EU-VNBO die Modalitäten oder Methoden oder die Pläne nach der Genehmigung durch die jeweils zuständigen Behörden auf ihren Websites, soweit diese Informationen nicht gemäß Artikel 47 als vertraulich betrachtet werden.

10. Die zuständigen Behörden können von den ÜNB und der EU-VNBO gemeinsam Vorschläge für Änderungen der genehmigten Modalitäten oder Methoden oder der

TERM

Artikel 9

1. Die ÜNB konsultieren mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO die Interessenträger, einschließlich der ACER, der ENISA und der zuständigen Behörde jedes Mitgliedstaats, zu den Entwürfen von Vorschlägen für die in Artikel 6 Absatz 2 genannten Modalitäten oder Methoden und für die in Artikel 6 Absatz 3 genannten Pläne. Die Konsultation dauert mindestens einen Monat.

2. Die in Artikel 6 Absatz 2 genannten Vorschläge für Modalitäten oder Methoden, die von den ÜNB in Zusammenarbeit mit der EU-VNBO vorgelegt wurden, werden veröffentlicht und auf Unionsebene einer Konsultation unterzogen. Die von den relevanten ÜNB in Zusammenarbeit mit der EU-VNBO auf regionaler Ebene vorgelegten Vorschläge für Pläne gemäß Artikel 6 Absatz 3 werden mindestens auf regionaler Ebene einer Konsultation unterzogen.

3. Die ÜNB, unterstützt von ENTSO-E, und die für den Vorschlag für Modalitäten, Methoden oder Pläne zuständige EU-VNBO tragen den in den gemäß Absatz 1 durchgeführten Konsultationen geäußerten Ansichten der Interessenträger, gebührend Rechnung, bevor sie die Vorschläge zur regulatorischen Genehmigung vorlegen. In allen Fällen ist zusammen mit dem Vorschlag eine fundierte Begründung vorzulegen, weshalb die aus der Konsultation hervorgegangenen Stellungnahmen berücksichtigt bzw. nicht berücksichtigt wurden, und rechtzeitig — vor oder gleichzeitig mit dem Vorschlag für Modalitäten oder Methoden — zu veröffentlichen.

TERM

Artikel 10

Die ACER organisiert in enger Zusammenarbeit mit ENTSO-E und der EU-VNBO die Einbeziehung der Interessenträger, einschließlich regelmäßiger Treffen mit Interessenträgern, um Probleme zu ermitteln und Verbesserungen im Zusammenhang mit der Durchführung dieser Verordnung vorzuschlagen.

TERM

Artikel 11

1. Die Kosten, die aufgrund der Verpflichtungen aus dieser Verordnung bei ÜNB und VNB anfallen, die der Netzentgeltregulierung unterliegen, einschließlich der Kosten von ENTSO-E und der EU-VNBO, werden von der zuständigen NRB jedes Mitgliedstaats geprüft.
2. Als angemessen, effizient und verhältnismäßig bewertete Kosten werden durch Netzentgelte oder andere geeignete Mechanismen gedeckt, die von der zuständigen NRB festgelegt werden.
3. Auf Verlangen der zuständigen NRB stellen die in Absatz 1 genannten ÜNB und VNB innerhalb einer von der NRB festgelegten angemessenen Frist die erforderlichen Informationen bereit, um die Prüfung der entstandenen Kosten zu erleichtern.

TERM

Artikel 12

1. Die ACER überwacht die Durchführung dieser Verordnung gemäß Artikel 32 Absatz 1 der Verordnung (EU) 2019/943 und Artikel 4 Absatz 2 der Verordnung (EU) 2019/942. Bei der Durchführung der Überwachung kann die ACER mit der ENISA zusammenarbeiten und ENTSO-E und die EU-VNBO um Unterstützung ersuchen. Die ACER unterrichtet die Koordinierungsgruppe „Strom" und die NIS-Kooperationsgruppe regelmäßig über die Durchführung dieser Verordnung. Artikel 32(1) der Verordnung (EU) 2019/943 [a], Artikel 4(2) der Verordnung (EU) 2019/942 [b]

2. Die ACER veröffentlicht nach dem Inkrafttreten dieser Verordnung mindestens alle drei Jahre einen Bericht, um

   a. den Stand der Umsetzung der anwendbaren Risikomanagementmaßnahmen im Bereich der Cybersicherheit durch Einrichtungen mit erheblichen Auswirkungen und Einrichtungen mit kritischen Auswirkungen zu überprüfen;

   b. zu ermitteln, ob zur Prävention von Risiken für den Elektrizitätssektor zusätzliche Vorschriften über gemeinsame Anforderungen, Planung, Beobachtung, Berichterstattung und Krisenbewältigung erforderlich sein könnten, und

   c. Verbesserungsbedarf für die Überarbeitung dieser Verordnung zu bestimmen oder nicht abgedeckte Bereiche und neue Prioritäten zu ermitteln, die sich aufgrund technischer Entwicklungen ergeben können.

3. Bis zum 13 Juni 2025 kann die ACER in Zusammenarbeit mit der ENISA und nach Konsultation von ENTSO-E und der EU-VNBO auf der Grundlage der gemäß Absatz 5 festgelegten Leistungsindikatoren Leitlinien zu den relevanten Informationen, die der ACER zu Überwachungszwecken zu übermitteln sind, sowie zu dem Verfahren und der Häufigkeit der Einholung der Informationen vorlegen.

4. Die zuständigen Behörden können Zugang zu den einschlägigen Informationen erhalten, die sich im Besitz der ACER befinden und gemäß diesem Artikel erhoben wurden.

5. Die ACER legt in Zusammenarbeit mit der ENISA und mit Unterstützung von ENTSO-E und der EU-VNBO in Bezug auf Cybersicherheitsaspekte grenzüberschreitender Stromflüsse unverbindliche Leistungsindikatoren für die Bewertung der betrieblichen Zuverlässigkeit vor.

6. Die in Artikel 2 Absatz 1 dieser Verordnung aufgeführten Einrichtungen übermitteln der ACER die Informationen, die diese zur Wahrnehmung der in Absatz 2 genannten Aufgaben benötigt.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943&qid=1733993709560#d1e3462-54-1

[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942#d1e519-22-1

TERM

Artikel 13

1. Bis zum 13 Juni 2025 erstellt die ACER in Zusammenarbeit mit der ENISA einen unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit. In dem Leitfaden für die NRB werden die Grundsätze des Benchmarkings der durchgeführten Cybersicherheitskontrollen gemäß Absatz 2 erläutert, wobei die Kosten für die Durchführung der Kontrollen und die Wirksamkeit von Prozessen, Produkten, Diensten, Systemen und Lösungen, die zur Durchführung dieser Kontrollen genutzt werden, zu berücksichtigen sind. Die ACER berücksichtigt bei der Erstellung des unverbindlichen Leitfadens für das Benchmarking im Bereich der Cybersicherheit vorhandene Benchmarking-Berichte. Die ACER übermittelt den unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit den NRB zur Information.

2. Innerhalb von 12 Monaten nach Erstellung des Benchmarking-Leitfadens gemäß Absatz 1 führen die NRB eine Benchmarking-Analyse durch, um zu bewerten, ob die aktuellen Investitionen in die Cybersicherheit

   a. Risiken mit Auswirkungen auf grenzüberschreitende Stromflüsse mindern;
   b. zu den gewünschten Ergebnissen führen und die Effizienz bei der Entwicklung des Elektrizitätssystems verbessern;
   c. effizient sind und in die allgemeine Auftragsvergabe für Vermögenswerte und Dienstleistungen integriert werden.

3. Bei der Benchmarking-Analyse können die NRB den von der ACER erstellten unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit berücksichtigen, wobei sie insbesondere Folgendes bewerten:

   a. die durchschnittlichen Ausgaben für die Cybersicherheit zur Minderung von Risiken, die sich auf grenzüberschreitende Stromflüsse auswirken, insbesondere bei Einrichtungen mit erheblichen oder kritischen Auswirkungen;
   b. in Zusammenarbeit mit ENTSO-E und der EU-VNBO die Durchschnittspreise für Cybersicherheitsdienste, -systeme und -produkte, die in hohem Maß zur Verbesserung und Aufrechterhaltung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit in den verschiedenen Netzbetriebsregionen beitragen;
   c. das Vorhandensein von Cybersicherheitsdiensten, -systemen und -lösungen, die sich für die Durchführung dieser Verordnung eignen, sowie die Vergleichbarkeit der damit verbundenen Kosten und Funktionen, wobei sie mögliche Maßnahmen ermitteln, die zur Verbesserung der Effizienz der Ausgaben erforderlich sind, insbesondere wenn Investitionen in die Cybersicherheitstechnik erforderlich sein könnten.

4. Alle Informationen zu Benchmarking-Analysen werden gemäß den Anforderungen dieser Verordnung an dieDatenklassifizierung, die Mindest-Cybersicherheitskontrollen und den Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gehandhabt und verarbeitet. Die in den Absätzen 2 und 3 genannte Benchmarking-Analyse wird nicht veröffentlicht.

5. Unbeschadet der Vertraulichkeitsbestimmungen in Artikel 47 und der Notwendigkeit, die Sicherheit von Einrichtungen zu schützen, die den Bestimmungen dieser Verordnung unterliegen, wird die in den Absätzen 2 und 3 dieses Artikels genannte Benchmarking-Analyse allen NRB, allen zuständigen Behörden, der ACER, der ENISA und der Kommission übermittelt.

TERM

Artikel 14

1. Innerhalb von 18 Monaten nach dem Inkrafttreten dieser Verordnung bemühen sich die ÜNB einer Netzbetriebsregion, die an ein Drittland angrenzt, um den Abschluss von Vereinbarungen mit ÜNB des benachbarten Drittlands, die mit dem einschlägigen Unionsrecht im Einklang stehen, die Grundlage für die Zusammenarbeit zum Cybersicherheitsschutz bilden und Regelungen für die Zusammenarbeit mit diesen ÜNB im Bereich der Cybersicherheit enthalten.
2. Die ÜNB unterrichten die zuständige Behörde über die gemäß Absatz 1 geschlossenen Vereinbarungen.

TERM

Artikel 15

1. Einrichtungen, die keine Niederlassung in der Union haben, aber Dienstleistungen für Einrichtungen in der Union erbringen und gemäß Artikel 24 Absatz 6 über ihren Status als Einrichtungen mit erheblichen oder kritischen Auswirkungen unterrichtet wurden, benennen innerhalb von drei Monaten nach der Unterrichtung schriftlich einen Vertreter in der Union und informieren die zuständige Behörde entsprechend.

2. Dieser Vertreter wird beauftragt, zusätzlich zu oder anstelle der Einrichtung mit erheblichen oder kritischen Auswirkungen als Ansprechpartner zu fungieren, an den sich jede zuständige Behörde und jedes CSIRT in der Union in Bezug auf die Verpflichtungen der Einrichtung aus dieser Verordnung wenden kann. Die Einrichtung mit erheblichen oder kritischen Auswirkungen stattet ihren gesetzlichen Vertreter mit den erforderlichen Befugnissen und ausreichenden Ressourcen aus, um eine effiziente und rechtzeitige Zusammenarbeit mit den jeweils zuständigen Behörden oder CSIRTs zu gewährleisten.

3. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Einrichtung ihre Dienste anbietet. Die Einrichtung gilt als der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegend, in dem der Vertreter niedergelassen ist. Einrichtungen mit erheblichen oder kritischen Auswirkungen melden der zuständigen Behörde des Mitgliedstaats, in dem ihr gesetzlicher Vertreter ansässig oder niedergelassen ist, den Namen, die Postanschrift, die E-Mail-Adresse und die Telefonnummer des gesetzlichen Vertreters.

4. Der benannte gesetzliche Vertreter kann für Verstöße gegen Pflichten aus dieser Verordnung haftbar gemacht werden; dies berührt nicht die Haftung und die rechtlichen Schritte, die gegen die Einrichtung mit erheblichen oder kritischen Auswirkungen eingeleitet werden können.

5. Wurde in der Union kein Vertreter im Sinne dieses Artikels benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienstleistungen erbringt, gegen die Einrichtung rechtliche Schritte wegen Verstößen gegen Pflichten aus dieser Verordnung einleiten.

6. Die Benennung eines gesetzlichen Vertreters in der Union gemäß Absatz 1 gilt nicht als Niederlassung in der Union.

TERM

Artikel 16

1. ENTSO-E und die EU-VNBO arbeiten bei der Durchführung der Bewertungen des Cybersicherheitsrisikos gemäß Artikel 19 und Artikel 21 zusammen, insbesondere bei den folgenden Aufgaben:

   a. Entwicklung der Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 18 Absatz 1;

   b. Erstellung des umfassenden Berichts über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23;

   c. Entwicklung des gemeinsamen Rahmens für die Cybersicherheit im Elektrizitätssektor gemäß Kapitel III;

   d. Erstellung der Empfehlung für die Cybersicherheit bei der Auftragsvergabe gemäß Artikel 35;

   e. Entwicklung der Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8;

   f. Entwicklung des vorläufigen Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor (ECII) gemäß Artikel 48 Absatz 1 Buchstabe a;

   g. Erstellung der konsolidierten vorläufigen Liste der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 48 Absatz 3;

   h. Erstellung der vorläufigen Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen gemäß Artikel 48 Absatz 4;

   i. Erstellung der vorläufigen Liste europäischer und internationaler Normen und Kontrollen gemäß Artikel 48 Absatz 6;

   j. Durchführung der unionsweiten Bewertung des Cybersicherheitsrisikos gemäß Artikel 19;

   k. Durchführung der regionalen Bewertung des Cybersicherheitsrisikos gemäß Artikel 21;

   l. Festlegung der regionalen Pläne zur Minderung des Cybersicherheitsrisikos gemäß Artikel 22;

   m. Entwicklung von Leitlinien für europäische Schemata für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen gemäß Artikel 36;

   n. Entwicklung von Leitlinien für die Durchführung dieser Verordnung, in Absprache mit der ACER und der ENISA.

2. Die Zusammenarbeit zwischen ENTSO-E und der EU-VNBO kann über eine Arbeitsgruppe für Cybersicherheitsrisiken erfolgen.

3. ENTSO-E und die EU-VNBO unterrichten die ACER, die ENISA, die NIS-Kooperationsgruppe und die Koordinierungsgruppe „Strom“ regelmäßig über die Fortschritte bei der Umsetzung der unionsweiten und regionalen Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 und Artikel 21.

TERM

Artikel 17

1. Die ACER überwacht in Zusammenarbeit mit jeder zuständigen Behörde

(1) die Umsetzung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit gemäß Artikel 12 Absatz 2 Buchstabe a und der Berichterstattungspflichten gemäß den Artikeln 27 und 39 sowie

(2) das Verfahren zur Annahme der Modalitäten, Methoden oder Pläne gemäß Artikel 6 Absätze 2 und 3 und deren Umsetzung. Die Zusammenarbeit zwischen der ACER, der ENISA und jeder zuständigen Behörde kann über ein Gremium zur Überwachung von Cybersicherheitsrisiken erfolgen.

TERM

Artikel 18

1. Bis zum 13 März 2025 legen die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und nach Konsultation der NIS-Kooperationsgruppe einen Vorschlag für die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten vor.
2. Die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten müssen Folgendes umfassen:
   a. eine Liste der zu berücksichtigenden Cyberbedrohungen, einschließlich mindestens der folgenden Bedrohungen der Lieferkette:
      i. schwere und unerwartete Kompromittierung der Lieferkette;
      ii. Nichtverfügbarkeit von IKT-Produkten, -Diensten oder -Prozessen aus der Lieferkette;
      iii. von Akteuren in der Lieferkette ausgelöste Cyberangriffe;
      iv. Weitergabe sensibler Informationen durch die Lieferkette, einschließlich der Nachverfolgung der Lieferkette;
      v. Einführung von Schwachstellen oder Hintertüren in IKT-Produkten, -Diensten oder -Prozessen durch Akteure in der Lieferkette;
   b. die Kriterien für die Einstufung der Auswirkungen von Cybersicherheitsrisiken als erheblich oder kritisch, wobei festgelegte Schwellenwerte für deren Folgen und Wahrscheinlichkeit zu nutzen sind;
   c. einen Ansatz zur Analyse der Cybersicherheitsrisiken, die sich aus Altsystemen, den Kaskadeneffekten von Cyberangriffen und dem Echtzeitcharakter der Netzbetriebssysteme ergeben;
   d. einen Ansatz zur Analyse der Cybersicherheitsrisiken, die sich aus der Abhängigkeit von einem einzigen Anbieter von IKT-Produkten, -Diensten oder -Prozessen ergeben.
3. Die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten müssen dieselbe Risiko-Auswirkungs-Matrix umfassen. Mit der Risiko-Auswirkungs-Matrix
   a. werden die Folgen von Cyberangriffen anhand folgender Kriterien gemessen:
      i. Lastverlust;
      ii. Verringerung der Stromerzeugung;
      iii. Kapazitätsverlust in der primären Frequenzreserve;
      iv. Verlust von Kapazitäten für die Wiederherstellung des Betriebs eines Stromnetzes ohne Rückgriff auf das externe Übertragungsnetz nach einer vollständigen oder teilweisen Abschaltung („Schwarzstart“);
      v. voraussichtliche Dauer eines Stromausfalls mit Auswirkungen auf die Kunden in Verbindung mit dem Ausmaß des Ausfalls (nach Zahl der Kunden) und
      vi. alle sonstigen quantitativen oder qualitativen Kriterien, die als sinnvolle Indikatoren für die Auswirkungen eines Cyberangriffs auf grenzüberschreitende Stromflüsse dienen könnten;
   b. wird die Wahrscheinlichkeit eines Vorfalls als Häufigkeit der Cyberangriffe pro Jahr gemessen.
4. In den Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene wird beschrieben, wie die ECIIS chwellenwerte für erhebliche und kritische Auswirkungen bestimmt werden. Der ECII muss es den Einrichtungen ermöglichen, im Rahmen der von ihnen gemäß Artikel 26 Absatz 4 Buchstabe c Ziffer i durchgeführten

TERM

Artikel 19

1. Innerhalb von neun Monaten nach der Genehmigung der Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 8 und danach alle drei Jahre führt ENTSO-E in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe unbeschadet des Artikels 22 der Richtlinie (EU) 2022/2555 [a] eine unionsweite Bewertung des Cybersicherheitsrisikos durch und erstellt einen Entwurf eines Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos. Dabei wenden sie die gemäß Artikel 18 entwickelten und gemäß Artikel 8 genehmigten Methoden an, um die möglichen Folgen von Cyberangriffen, die sich auf die Betriebssicherheit des Elektrizitätssystems auswirken und grenzüberschreitende Stromflüsse stören, zu ermitteln, zu analysieren und zu bewerten. Bei der unionsweiten Bewertung des Cybersicherheitsrisikos werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

2. Der Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos muss Folgendes enthalten:

   a. die unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen;

   b. eine Risiko-Auswirkungs-Matrix, die Einrichtungen und die zuständigen Behörden nutzen müssen, um die Cybersicherheitsrisiken zu bewerten, die in der Bewertung des Cybersicherheitsrisikos auf der Ebene der Mitgliedstaaten gemäß Artikel 20 und in der Bewertung des Cybersicherheitsrisikos auf der Ebene von, Einrichtungen gemäß Artikel 26 Absatz 2 Buchstabe b ermittelt wurden.

3. In Bezug auf die unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen muss der Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos Folgendes enthalten:

   a. eine Bewertung der möglichen Folgen eines Cyberangriffs anhand der Parameter, die in der gemäß Artikel 18 Absätze 2, 3 und 4 entwickelten und gemäß Artikel 8 genehmigten Methode zur Bewertung des Cybersicherheitsrisikos festgelegt sind;

   b. den ECII und die Schwellenwerte für erhebliche und kritische Auswirkungen, die die zuständigen Behörden gemäß Artikel 24 Absätze 1 und 2 nutzen müssen, um Einrichtungen mit erheblichen oder kritischen Auswirkungen zu ermitteln, die an unionsweiten Prozessen mit erheblichen bzw. kritischen Auswirkungen beteiligt sind.

4. ENTSO-E legt der ACER in Zusammenarbeit mit der EU-VNBO den Entwurf des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos mit den Ergebnissen der unionsweiten Bewertung des Cybersicherheitsrisikos zur Stellungnahme vor. Die ACER gibt innerhalb von drei Monaten nach Eingang eine Stellungnahme zu dem Entwurf des Berichts ab. ENTSO-E und die EU-VNBO tragen der Stellungnahme der ACER bei der Fertigstellung dieses Berichts so weit wie möglich Rechnung.

5. Innerhalb von drei Monaten nach Eingang der Stellungnahme der ACER übermittelt ENTSO-E in Zusammenarbeit mit der EU-VNBO der ACER, der Kommission, der ENISA und den zuständigen Behörden den endgültigen Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_22

TERM

Artikel 20

1. Jede zuständige Behörde führt in Bezug auf alle Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat eine Bewertung des Cybersicherheitsrisikos des Mitgliedstaats durch und nutzt dabei die gemäß Artikel 18 entwickelten und gemäß Artikel 8 genehmigten Methoden. Bei der Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten werden die Risiken von Cyberangriffen ermittelt und analysiert, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören. Bei der Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

2. Innerhalb von 21 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre übermittelt jede zuständige Behörde mit Unterstützung des CSIRT und nach Konsultation der für Elektrizität zuständigen CS-NCA dem ENTSO-E und der EU-VNBO einen Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats, der in Bezug auf jeden Geschäftsprozess mit erheblichen oder kritischen Auswirkungen folgende Informationen enthält:

   a. den Stand der Umsetzung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskorntrollen gemäß Artikel 29;
   b. eine Liste aller in den letzten drei Jahren gemäß Artikel 38 Absatz 3 gemeldeten Cyberangriffe;
   c. eine Zusammenfassung aller in den letzten drei Jahren gemäß Artikel 38 Absatz 6 gemeldeten Informationen zu Cyberbedrohungen;
   d. für jeden unionsweiten Prozess mit erheblichen oder kritischen Auswirkungen eine Schätzung der mit einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten verbundenen Risiken;
   e. erforderlichenfalls eine Liste zusätzlicher Einrichtungen, die gemäß Artikel 24 Absätze 1, 2, 3 und 5 als Einrichtungen mit erheblichen oder kritischen Auswirkungen ermittelt wurden.

3. Der Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats muss dem gemäß Artikel 10 der Verordnung (EU) 2019/941 [a] erstellten Risikovorsorgeplan des Mitgliedstaats Rechnung tragen.

4. Die Informationen in dem Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats gemäß Absatz 2 Buchstaben a bis d dürfen nicht mit bestimmten Einrichtungen oder Vermögenswerten verknüpft sein. In dem Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats sind auch die Risiken im Zusammenhang mit den von den zuständigen Behörden der Mitgliedstaaten gemäß Artikel 30 gewährten befristeten Ausnahmen zu bewerten.

5. ENTSO-E und die EU-VNBO können im Zusammenhang mit den in Unterabsatz 2 Buchstaben a und c genannten Aufgaben die zuständigen Behörden um zusätzliche Informationen ersuchen.

6. Die zuständigen Behörden stellen sicher, dass die von ihnen bereitgestellten Informationen genau und zutreffend sind.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e928-1-1

TERM

Artikel 21

1. ENTSO-E führt in Zusammenarbeit mit der EU-VNBO und in Absprache mit dem zuständigen regionalen Koordinierungszentrum für jede Netzbetriebsregion eine regionale Bewertung des Cybersicherheitsrisikos durch und nutzt dabei die gemäß Artikel 19 entwickelten und gemäß Artikel 8 genehmigten Methoden, um die Risiken von Cyberangriffen, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören, zu ermitteln, zu analysieren und zu bewerten. Bei der regionalen Bewertung des Cybersicherheitsrisikos werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

2. Innerhalb von 30 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe für jede Netzbetriebsregion einen Bericht über die regionale Bewertung des Cybersicherheitsrisikos.

3. Der Bericht über die regionale Bewertung des Cybersicherheitsrisikos muss den einschlägigen Informationen Rechnung tragen, die in den Berichten über die unionsweite Bewertung des Cybersicherheitsrisikos und in den Berichten der Mitgliedstaaten über die Bewertung des Cybersicherheitsrisikos enthalten sind.

4. Bei der regionalen Bewertung des Cybersicherheitsrisikos werden die gemäß Artikel 6 der Verordnung (EU) 2019/941 [a] bestimmten regionalen Szenarien für Stromversorgungskrisen im Bereich der Cybersicherheit berücksichtigt.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e698-1-1

TERM

Artikel 22

1. Innerhalb von 36 Monaten nach Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6, spätestens jedoch am 13 Juni 2031, und danach alle drei Jahre erstellen die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit den regionalen Koordinierungszentren und der NIS-Kooperationsgruppe für jede Netzbetriebsregion einen regionalen Plan zur Minderung des Cybersicherheitsrisikos.
2. Die regionalen Pläne zur Minderung des Cybersicherheitsrisikos müssen Folgendes enthalten:
   a. die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen, die die Einrichtungen mit erheblichen bzw. kritischen Auswirkungen in der Netzbetriebsregion anwenden müssen;
   b. die verbleibenden Cybersicherheitsrisiken in den Netzbetriebsregionen nach Anwendung der unter Buchstabe a genannten Kontrollen.
3. ENTSO-E legt die regionalen Pläne zur Minderung des Cybersicherheitsrisikos den relevanten Übertragungsnetzbetreibern, den zuständigen Behörden und der Koordinierungsgruppe „Strom“ vor. Die Koordinierungsgruppe „Strom“ kann Änderungen empfehlen.
4. Die ÜNB aktualisieren mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe die regionalen Risikominderungspläne alle drei Jahre, soweit aufgrund der Umstände keine häufigere Aktualisierung erforderlich ist.

TERM

Artikel 23

1. Innerhalb von 40 Monaten nach Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre übermitteln die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe der Koordinierungsgruppe „Strom“ einen Bericht über die Ergebnisse der Bewertung der Cybersicherheitsrisiken in Bezug auf grenzüberschreitende Stromflüsse (im Folgenden „umfassender Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse“).

2. Der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse stützt sich auf den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos, die Berichte der Mitgliedstaaten über die Bewertung des Cybersicherheitsrisikos und die Berichte über die regionale Bewertung des Cybersicherheitsrisikos und muss folgende Informationen enthalten:

   a. die Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen, die im Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 2 Buchstabe a ermittelt wurden, einschließlich der Schätzung der Wahrscheinlichkeit und der Auswirkungen von Cybersicherheitsrisiken, die in den Berichten über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 und Artikel 19 Absatz 3 Buchstabe a bewertet wurden;

   b. aktuelle Cyberbedrohungen, insbesondere neu aufkommende Bedrohungen und Risiken für das Elektrizitätssystem;

   c. Cyberangriffe im vorangegangenen Zeitraum auf Unionsebene mit einem kritischen Überblick darüber, wie sich diese Cyberangriffe auf grenzüberschreitende Stromflüsse ausgewirkt haben könnten;

   d. allgemeiner Stand der Umsetzung der Cybersicherheitsmaßnahmen;

   e. Stand der Umsetzung der Informationsflüsse gemäß den Artikeln 37 und 38;

   f. Liste der Informationen oder spezifische Kriterien für die Klassifizierung von Informationen gemäß Artikel 46;

   g. ermittelte und besonders zu beachtende Risiken, die sich aus einem unsicheren Lieferkettenmanagement ergeben können;

   h. Ergebnisse der regionalen und überregionalen Cybersicherheitsübungen gemäß Artikel 44 und dabei insgesamt gewonnene Erfahrungen;

   i. eine Analyse der Entwicklung des allgemeinen Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse seit den letzten regionalen Bewertungen des Cybersicherheitsrisikos;

   j. alle sonstigen Informationen, die nützlich sein können, um mögliche Verbesserungen dieser Verordnung oder die Notwendigkeit einer Überarbeitung dieser Verordnung oder ihrer Instrumente zu ermitteln, sowie

   k. aggregierte und anonymisierte Informationen über die gemäß Artikel 30 Absatz 3 gewährten Ausnahmen.

3. Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen können zur Ausarbeitung des umfassenden Berichts über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse beitragen, wobei sie die Vertraulichkeit der Informationen gemäß Artikel 47 wahren müssen. Die ÜNB konsultieren diese Einrichtungen mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO frühzeitig.

4. Der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für gren-

TERM

Artikel 24

1. Jede zuständige Behörde ermittelt anhand des ECII und der Schwellenwerte für erhebliche und kritische Auswirkungen, die im Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 3 Buchstabe b enthalten sind, die Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat, die an unionsweiten Prozessen mit erheblichen bzw. kritischen Auswirkungen beteiligt sind. Die zuständigen Behörden können von einer Einrichtung in ihrem Mitgliedstaat Informationen anfordern, um die ECII-Werte für diese Einrichtung zu bestimmen. Liegt der ermittelte ECII einer Einrichtung über dem Schwellenwert für erhebliche oder kritische Auswirkungen, wird die ermittelte Einrichtung in dem in Artikel 20 Absatz 2 genannten Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats aufgeführt.

2. Jede zuständige Behörde ermittelt anhand des ECII und der Schwellenwerte für erhebliche und kritische Auswirkungen aus dem Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 3 Buchstabe b die nicht in der Union niedergelassenen Einrichtungen mit erheblichen oder kritischen Auswirkungen, soweitsie in der Union tätig sind. Die zuständige Behörde kann von einer nicht in der Union niedergelassenen Einrichtung Informationen anfordern, um die ECII-Werte für die Einrichtung zu bestimmen.

3. Jede zuständige Behörde kann weitere Einrichtungen in ihrem Mitgliedstaat als Einrichtungen mit erheblichen oder kritischen Auswirkungen einstufen, wenn die folgenden Kriterien erfüllt sind:

   a. Die Einrichtung ist Teil einer Gruppe von Einrichtungen, für die ein erhebliches Risiko besteht, dass sie zeitgleich Ziel eines Cyberangriffs sein könnten;

   b. der über die Gruppe von Einrichtungen aggregierte ECII liegt über dem Schwellenwert für erhebliche oder kritische Auswirkungen.

4. Ermittelt eine zuständige Behörde gemäß Absatz 3 zusätzliche Einrichtungen, so gelten alle Prozesse dieser Einrichtungen, deren über die Gruppe aggregierter ECII über dem Schwellenwert für erhebliche Auswirkungen liegt, als Prozesse mit erheblichen Auswirkungen, und alle Prozesse, deren über die Gruppe aggregierter ECII über den Schwellenwerten für kritische Auswirkungen liegt, gelten als Prozesse mit kritischen Auswirkungen.

5. Ermittelt eine zuständige Behörde Einrichtungen gemäß Absatz 3 Buchstabe a in mehr als einem Mitgliedstaat, so unterrichtet sie die anderen zuständigen Behörden, ENTSO-E und die EU-VNBO. ENTSO-E übermittelt den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO auf der Grundlage der von allen zuständigen Behörden übermittelten Informationen eine Analyse der Aggregierung von Einrichtungen in mehr als einem Mitgliedstaat, die zu einer von verschiedenen Punkten ausgehenden Störung der grenzüberschreitenden Stromflüsse führen und einen Cyberangriff nach sich ziehen können. Wird eine Gruppe von Einrichtungen in mehreren Mitgliedstaaten als Aggregierung ermittelt, deren ECII über dem Schwellenwert für erhebliche oder kritische Auswirkungen liegt, so stufen alle betroffenen zuständigen Behörden die Einrichtungen in dieser Gruppe für ihren jeweiligen Mitgliedstaat auf der Grundlage des aggregierten ECII für die Gruppe der Einrichtungen als Einrichtungen mit erheblichen bzw. kritischen Auswirkungen ein, und die ermittelten Einrichtungen werden in den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos aufgenommen.

6. Jede zuständige Behörde unterrichtet innerhalb von neun Monaten, nachdem ENTSO-E und die EU-VNBO den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 5 übermittelt haben, spätestens jedoch bis zum 13 Juni 2028, die in der Liste aufgeführten Einrichtungen, dass sie in ihrem

TERM

Artikel 25

1. Die zuständigen Behörden können ein nationales Überprüfungssystem einrichten, um zu überprüfen, ob die gemäß Artikel 24 Absatz 1 ermittelten Einrichtungen mit kritischen Auswirkungen den nationalen Rechtsrahmen umgesetzt haben, der in der Vergleichsmatrix gemäß Artikel 34 aufgeführt ist. Das nationale Überprüfungssystem kann sich auf eine von der zuständigen Behörde durchgeführte Inspektion, unabhängige Sicherheitsaudits oder gegenseitige Peer Reviews durch Einrichtungen mit kritischen Auswirkungen in demselben Mitgliedstaat, die von der zuständigen Behörde beaufsichtigt werden, stützen.

2. Beschließt eine zuständige Behörde, ein nationales Überprüfungssystem einzurichten, so stellt sie sicher, dass die Überprüfung nach den folgenden Anforderungen durchgeführt wird:

   a. Jede Partei, die die Peer Review, das Audit oder die Inspektion durchführt, muss von der zu überprüfenden Einrichtung mit kritischen Auswirkungen unabhängig sein und darf sich nicht in einem Interessenkonflikt befinden;

   b. das Personal, das die Peer Reviews, Audits oder Inspektionen durchführt, muss nachweislich Kenntnisse haben über

      i. die Cybersicherheit im Elektrizitätssektor;
      ii. Cybersicherheitsmanagementsysteme;
      iii. Audit-Grundsätze;
      iv. die Bewertung von Cybersicherheitsrisiken;
      v. den gemeinsamen Rahmen für die Cybersicherheit im Elektrizitätssektor;
      vi. den nationalen Rechts- und Verwaltungsrahmen sowie europäische und internationale Normen, die für die Überprüfung relevant sind;
      vii. die Prozesse mit kritischen Auswirkungen, die Gegenstand der Überprüfung sind;

   c. die Partei, die die Peer Reviews, Audits oder Inspektionen durchführt, erhält ausreichend Zeit für die Durchführung dieser Tätigkeiten;

   d. die Partei, die die Peer Reviews, Audits oder Inspektionen durchführt, ergreift geeignete Maßnahmen, um die bei der Überprüfung erhobenen Informationen im Einklang mit ihrem Vertraulichkeitsgrad zu schützen, und

   e. Peer Reviews, Audits oder Inspektionen werden mindestens einmal jährlich durchgeführt und umfassen mindestens alle drei Jahre den gesamten Prüfumfang.

3. Beschließt eine zuständige Behörde, ein nationales Überprüfungssystem einzurichten, so teilt sie der ACER jährlich mit, wie oft sie Inspektionen im Rahmen dieses Systems durchgeführt hat.

TERM

Artikel 26

1. Jede von den zuständigen Behörden gemäß Artikel 24 Absatz 1 ermittelte Einrichtung mit erheblichen oder kritischen Auswirkungen führt das Cybersicherheitsrisikomanagement für alle ihre Vermögenswerte in ihren Perimetern mit erheblichen oder kritischen Auswirkungen durch. Jede Einrichtung mit erheblichen oder kritischen Auswirkungen führt alle drei Jahre ein Risikomanagement durch, das die in Absatz 2 genannten Phasen umfasst.
2. Jede Einrichtung mit erheblichen oder kritischen Auswirkungen stützt ihr Cybersicherheitsrisikomanagement auf einen Ansatz, der auf den Schutz ihrer Netz- und Informationssysteme abzielt und folgende Phasen umfasst:
   a. Bestimmung des Kontexts;
   b. Bewertung des Cybersicherheitsrisikos auf der Ebene der Einrichtung;
   c. Behandlung von Cybersicherheitsrisiken;
   d. Akzeptanz von Cybersicherheitsrisiken.
3. Bei der Bestimmung des Kontexts trifft jede Einrichtung mit erheblichen oder kritischen Auswirkungen folgende Maßnahmen:
   a. Festlegung des Umfangs der Bewertung des Cybersicherheitsrisikos, einschließlich der von ENTSO-E und der EU-VNBO ermittelten Prozesse mit erheblichen oder kritischen Auswirkungen sowie anderer Prozesse, die Ziel von Cyberangriffen mit erheblichen oder kritischen Auswirkungen auf grenzüberschreitende Stromflüsse sein können, und
   b. Festlegung der Kriterien für die Risikobewertung und die Risikoakzeptanz im Einklang mit der Risiko-AuswirkungsMatrix, die Einrichtungen und die zuständigen Behörden nach den von ENTSO-E und der EU-VNBO gemäß Artikel 19 Absatz 2 entwickelten Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf Ebene der Mitgliedstaaten nutzen müssen, um Cybersicherheitsrisiken zu bewerten.
4. Bei der Bewertung des Cybersicherheitsrisikos muss jede Einrichtung mit erheblichen oder kritischen Auswirkungen
   a. Cybersicherheitsrisiken unter Berücksichtigung folgender Aspekte ermitteln:
      i. aller Vermögenswerte, die unionsweite Prozesse mit erheblichen oder kritischen Auswirkungen unterstützen, wobei die möglichen Auswirkungen auf grenzüberschreitende Stromflüsse für den Fall einer Kompromittierung des Vermögenswerts zu bewerten sind;
      ii. möglicher Cyberbedrohungen unter Berücksichtigung der Cyberbedrohungen, die im jüngsten umfassenden Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23 ermittelt wurden, sowie Bedrohungen der Lieferkette;
      iii. Schwachstellen, einschließlich Schwachstellen in Altsystemen;
      iv. möglicher Szenarien von Cyberangriffen, einschließlich Cyberangriffen, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören;
      v. einschlägiger Risikobeurteilungen und -bewertungen auf Unionsebene, einschließlich koordinierter Risikobewertungen kritischer Lieferketten gemäß Artikel 22 der Richtlinie (EU) 2022/2555 [a], und
      vi. bestehender umgesetzter Kontrollen;
   b. die Wahrscheinlichkeit und Folgen der unter Buchstabe a genannten Cybersicherheitsrisiken analysieren und das Ausmaß des Cybersicherheitsrisikos an-

TERM

Artikel 27

Innerhalb von 12 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre legt jede Einrichtung mit erheblichen oder kritischen Auswirkungen der zuständigen Behörde einen Bericht vor, der folgende Informationen enthält:

1. eine Liste der für den Risikominderungsplan auf Ebene der Einrichtung gemäß Artikel 26 Absatz 5 ausgewählten Kontrollen mit dem aktuellen Stand der Umsetzung jeder Kontrolle;
2. für jeden unionsweiten Prozess mit erheblichen oder kritischen Auswirkungen eine Schätzung des Risikos einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten. Die Schätzung dieses Risikos ist im Einklang mit der Risiko-Auswirkungs-Matrix gemäß Artikel 19 Absatz 2 zu bestimmen;
3. für ihre Prozesse mit kritischen Auswirkungen eine Liste der Anbieter kritischer IKT-Dienste.

NOTE

TERM

Artikel 28

1. Der gemeinsame Rahmen für die Cybersicherheit im Elektrizitätssektor umfasst die folgenden Kontrollen und Systeme für das Cybersicherheitsmanagement:
   a. die gemäß Artikel 29 entwickelten Mindest-Cybersicherheitskontrollen;
   b. die gemäß Artikel 29 entwickelten erweiterten Cybersicherheitskontrollen;
   c. die gemäß Artikel 34 entwickelte Vergleichsmatrix, in der die Kontrollen gemäß den Buchstaben a und b anhand ausgewählter europäischer und internationaler Normen und nationaler Rechts- oder Verwaltungsrahmen verglichen werden;
   d. das gemäß Artikel 32 eingerichtete Cybersicherheitsmanagementsystem.
2. Alle Einrichtungen mit erheblichen Auswirkungen wenden die Mindest-Cybersicherheitskontrollen gemäß Absatz 1 Buchstabe a innerhalb ihres Perimeters mit erheblichen Auswirkungen an.
3. Alle Einrichtungen mit kritischen Auswirkungen wenden die erweiterten Cybersicherheitskontrollen gemäß Absatz 1 Buchstabe b innerhalb ihres Perimeters mit kritischen Auswirkungen an.
4. Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 wird der in Absatz 1 genannte gemeinsame Rahmen für die Cybersicherheit im Elektrizitätssektor durch die gemäß Artikel 33 entwickelten Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen in der Lieferkette ergänzt.

TERM

Artikel 29

1. Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO einen Vorschlag für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen.
2. Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO der zuständigen Behörde eine Änderung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.
3. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen müssen überprüft werden können; dazu werden sie entweder im Einklang mit dem Verfahren gemäß Artikel 31 in ein nationales Überprüfungssystem einbezogen oder Sicherheitsaudits durch unabhängige Dritte gemäß den in Artikel 25 Absatz 2 aufgeführten Anforderungen unterzogen.
4. Die gemäß Absatz 1 entwickelten anfänglichen Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen müssen auf den Risiken beruhen, die in dem Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß

Chapter 3

Artikel 1: Gegenstand

Diese Verordnung enthält einen Netzkodex mit sektorspezifischen Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse, einschließlich Vorschriften über gemeinsame Mindestanforderungen, Planung, Beobachtung, Berichterstattung und die Krisenbewältigung.

Chapter 4

Artikel 2: Anwendungsbereich

1. Diese Verordnung gilt für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse bei den Tätigkeiten der folgenden Einrichtungen, soweit diese gemäß Artikel 24 [1] als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft werden:
   a. Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944; [2]
   b. nominierte Strommarktbetreiber (NEMOs) im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/943; [3]
   c. organisierte Marktplätze oder organisierte Märkte im Sinne des Artikels 2 Nummer 4 der Durchführungsverordnung (EU) Nr. 1348/2014 der Kommission [4] (14), die Transaktionen mit Produkten arrangieren, die für grenzüberschreitende Stromflüsse relevant sind;
   d. Anbieter kritischer IKT-Dienste im Sinne des Artikels 3 Nummer 9 dieser Verordnung [5]
   e. ENTSO-E, das gemäß Artikel 28 der Verordnung (EU) 2019/943 [6] eingerichtet wurde;
   f. die EU-VNBO, die gemäß Artikel 52 der Verordnung (EU) 2019/943 [7] eingerichtet wurde;
   g. Bilanzkreisverantwortliche im Sinne des Artikels 2 Nummer 14 der Verordnung (EU) 2019/943; [8]
   h. Betreiber von Ladepunkten im Sinne des Anhangs I der Richtlinie (EU) 2022/2555; [9]
   i. regionale Koordinierungszentren (RCC) gemäß Artikel 35 der Verordnung (EU) 2019/943; [10]
   j. Anbieter verwalteter Sicherheitsdienste (MSSP) gemäß Artikel 6 Nummer 40 der Richtlinie (EU) 2022/2555; [11]

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[4] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R1348
[5] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_3
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[8] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art
[10] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[11] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

k. alle sonstigen Einrichtungen oder Dritte, denen gemäß dieser Verordnung [12] Zuständigkeiten übertragen oder zugewiesen werden.

2. Die folgenden Behörden sind im Rahmen ihres derzeitigen Auftrags für die Wahrnehmung der in dieser Verordnung [13] festgelegten Aufgaben zuständig:

   a. die mit der Verordnung (EU) 2019/942 des Europäischen Parlaments und des Rates [14] eingerichtete Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER)

   b. die nationalen zuständigen Behörden, die für die Wahrnehmung der ihnen gemäß dieser Verordnung [15] übertragenen Aufgaben verantwortlich sind und von den Mitgliedstaaten gemäß Artikel 4 als „zuständige Behörde" benannt wurden;

   c. die gemäß Artikel 57 Absatz 1 der Richtlinie (EU) 2019/944; [16] benannten nationalen Regulierungsbehörden (NRB) der einzelnen Mitgliedstaaten;

   d. die gemäß Artikel 3 der Verordnung (EU) 2019/941; [17] benannten für die Risikovorsorge zuständigen Behörden (RP-NCA);

   e. die gemäß Artikel 10 der Richtlinie (EU) 2022/2555; [18] benannten oder eingerichteten Computer-Notfallteams (CSIRTs);

   f. die gemäß Artikel 8 der Richtlinie (EU) 2022/2555; [19] benannten oder eingerichteten für die Cybersicherheit zuständigen Behörden (CS-NCA);

   g. die gemäß der Verordnung (EU) 2019/881; [20] errichtete Agentur der Europäischen Union für Cybersicherheit;

   h. alle sonstigen Behörden oder Dritte, denen gemäß Artikel 4 Absatz 3 [21] Zuständigkeiten übertragen oder zugewiesen werden.

3. Diese Verordnung gilt auch für alle Einrichtungen, die nicht in der Union niedergelassen sind, aber Dienstleistungen für Einrichtungen in der Union erbringen, sofern sie von den zuständigen Behörden gemäß Artikel 24 Absatz 2 [22] als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

4. Diese Verordnung lässt die Zuständigkeit der Mitgliedstaaten in Bezug auf die Aufrechterhaltung der nationalen Sicherheit und ihre Befugnis zum Schutz anderer wesentlicher staatlicher Funktionen, einschließlich der Wahrung der territorialen Unversehrtheit des Staates und der Aufrechterhaltung der öffentlichen Ordnung, unberührt.

5. Diese Verordnung lässt die Zuständigkeit der Mitgliedstaaten für die Aufrechterhaltung der nationalen Sicherheit in Bezug auf Tätigkeiten zur Stromerzeugung in Kernkraftwerken, einschließlich Tätigkeiten innerhalb der nuklearen Wertschöpfungskette, im Einklang mit den Verträgen unberührt.

[12] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[13] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[14] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942
[15] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[16] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[17] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941
[18] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[19] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[20] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881
[21] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[22] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

6. Soweit dies für die Zwecke dieser Verordnung erforderlich ist, werden personenbezogene Daten von Einrichtungen, den zuständigen Behörden, den zentralen Anlaufstellen auf Ebene der Einrichtung und den CSIRTs im Einklang mit der Verordnung (EU) 2016/679 [23], insbesondere auf der Grundlage von Artikel 6 der genannten Verordnung, verarbeitet.

[23] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679

Chapter 5

Artikel 3: Begriffsbestimmungen

Es gelten die folgenden Begriffsbestimmungen:

1. „Vermögenswert“ bezeichnet alle Informationen sowie jede Software oder Hardware, gleich ob materieller oder immaterieller Art, in Netz- und Informationssystemen, die für eine natürliche Person, eine Organisation oder eine Regierung von Wert sind;
2. „für die Risikovorsorge zuständige Behörde“ bezeichnet die gemäß Artikel 3 der Verordnung (EU) 2019/941; [1] benannte zuständige Behörde;
3. „Computer-Notfallteam“ bezeichnet ein Team, das gemäß Artikel 10 der Richtlinie (EU) 2022/2555; [2] für die Bewältigung von Risiken und Sicherheitsvorfällen zuständig ist;
4. „Vermögenswert mit kritischen Auswirkungen“ bezeichnet einen Vermögenswert, der für die Durchführung eines Prozesses mit kritischen Auswirkungen erforderlich ist;
5. „Einrichtung mit kritischen Auswirkungen“ bezeichnet eine Einrichtung, die einen Prozess mit kritischen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24; [3] bestimmt wird;
6. „Perimeter mit kritischen Auswirkungen“ bezeichnet einen von einer in Artikel 2(1) [4] genannten Einrichtung definierten Perimeter, der alle Vermögenswerte mit kritischen Auswirkungen umfasst und in dem der Zugang zu diesen Vermögenswerten kontrolliert werden kann und der den Anwendungsbereich bestimmt, in dem die erweiterten Cybersicherheitskontrollen anzuwenden sind;
7. „Prozess mit kritischen Auswirkungen“ bezeichnet einen Geschäftsprozess einer Einrichtung, dessen Indizes für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor über dem Schwellenwert für kritische Auswirkungen liegen;

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[4] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

8. „Schwellenwert für kritische Auswirkungen“ bezeichnet die Werte der in Artikel 19(3)b [5] genannten Indizes für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor, bei deren Überschreitung ein Cyberangriff auf einen Geschäftsprozess zu einer kritischen Störung grenzüberschreitender Stromflüsse führt;

9. „Anbieter kritischer IKT-Dienste“ bezeichnet eine Einrichtung, die einen IKT-Dienst oder einen IKT-Prozess bereitstellt, der für einen Prozess mit kritischen oder erheblichen Auswirkungen, der sich auf Cybersicherheitsaspekte grenzüberschreitender Stromflüsse auswirkt, erforderlich ist und bei dessen Kompromittierung ein Cyberangriff erfolgen könnte, dessen Auswirkungen den Schwellenwert für kritische oder erhebliche Auswirkungen überschreiten;

10. „grenzüberschreitender Stromfluss“ bezeichnet einen grenzüberschreitenden Stromfluss im Sinne des Artikels) 2(3) der Verordnung (EU) 2019/943; [6]

11. „Cyberangriff“ bezeichnet einen Vorfall im Sinne des Artikels) 3, Nummer 14, der Verordnung (EU) 2022/2554; [7]

12. „Cybersicherheit“ bezeichnet Cybersicherheit im Sinne des Artikels) 2, Nummer 1, der Verordnung (EU) 2019/881; [8]

13. „Cybersicherheitskontrolle“ bezeichnet die zur Vermeidung, Erkennung, Bekämpfung oder Minimierung von Cybersicherheitsrisiken durchgeführten Maßnahmen oder Verfahren;

14. „Cybersicherheitsvorfall“ bezeichnet einen Vorfall im Sinne von Artikel 6 [9] Nummer 6 der Richtlinie (EU) 2022/2555;

15. „Cybersicherheitsmanagementsystem“ bezeichnet die Konzepte, Verfahren, Leitlinien sowie die damit verbundenen Ressourcen und Tätigkeiten, die von einer Einrichtung insgesamt verwaltet werden, um ihre Informationsressourcen vor Cyberbedrohungen zu schützen, wobei die Sicherheit der Netz- und Informationssysteme einer Organisation systematisch bestimmt, umgesetzt, betrieben, überwacht, überprüft, aufrechterhalten und verbessert wird;

16. „Betriebszentrum für Cybersicherheit“ bezeichnet ein spezielles Zentrum, in dem ein aus einem oder mehreren Sachverständigen bestehendes technisches Team mithilfe von IT-Systemen für Cybersicherheit sicherheitsbezogene Aufgaben (Dienste von Cybersicherheits-Betriebszentren, CSOC-Dienste) wahrnimmt, wie z. B. den Umgang mit Cyberangriffen und Fehlern bei der Sicherheitskonfiguration, Sicherheitsüberwachung, Protokollanalyse und die Erkennung von Cyberangriffen;

17. „Cyberbedrohung“ bezeichnet eine Cyberbedrohung im Sinne des Artikels) 2, Nummer 8, der Verordnung (EU) 2019/881; [10]

18. „Schwachstellenmanagement im Bereich der Cybersicherheit“ bezeichnet die Praxis, Schwachstellen zu ermitteln und zu beheben;

19. „Einrichtung“ bezeichnet eine Einrichtung im Sinne des Artikels) 6, Nummer 38, der Richtlinie (EU) 2022/2555; [11]

[5] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2554
[8] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[10] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881
[11] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555

20. „Frühwarnung“ bezeichnet die erforderliche Unterrichtung, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

21. „Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor“ („ECII“) bezeichnet einen Index oder eine Klassifizierungsskala, mit dem/der die möglichen Folgen von Cyberangriffen auf Geschäftsprozesse im Zusammenhang mit grenzüberschreitenden Stromflüssen eingestuft werden;

22. „europäisches Schema für die Cybersicherheitszertifizierung“ bezeichnet ein Schema im Sinne des Artikels) 2, Nummer 9, der Verordnung (EU) 2019/881; [12]

23. „Einrichtung mit erheblichen Auswirkungen“ bezeichnet eine Einrichtung, die einen Prozess mit erheblichen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24; [13] ermittelt wird;

24. „Prozess mit erheblichen Auswirkungen“ bezeichnet jeden Geschäftsprozess einer Einrichtung, dessen Indizes für die Auswirkungen von Cybersicherheitsvorfällen im Elektrizitätssektor über den Schwellenwerten für erhebliche Auswirkungen liegen;

25. „Vermögenswert mit erheblichen Auswirkungen“ bezeichnet einen Vermögenswert, der für die Durchführung eines Prozesses mit erheblichen Auswirkungen erforderlich ist;

26. „Schwellenwert für erhebliche Auswirkungen“ bezeichnet die Werte der in Artikel 19(3)b, [14] genannten Indizes für die Auswirkungen von Cybersicherheitsvorfällen im Elektrizitätssektor, bei deren Überschreitung ein erfolgreich durchgeführter Cyberangriff auf einen Prozess zu einer erheblichen Störung grenzüberschreitender Stromflüsse führt;

27. „Perimeter mit erheblichen Auswirkungen“ bezeichnet einen von einer in Artikel 2(1) [15] genannten Einrichtung definierten Perimeter, der alle Vermögenswerte mit erheblichen Auswirkungen umfasst und in dem der Zugang zu diesen Vermögenswerten kontrolliert werden kann und der den Anwendungsbereich bestimmt, in dem die Mindestsicherheitskontrollen anzuwenden sind;

28. „IKT-Produkt“ bezeichnet ein IKT-Produkt im Sinne des Artikels) 2, Nummer 12, der Verordnung (EU) 2019/881; [16]

29. „IKT-Dienst“ bezeichnet einen IKT-Dienst im Sinne des Artikels) 2, Nummer 13, der Verordnung (EU) 2019/881; [17]

30. „IKT-Prozess“ bezeichnet einen IKT-Prozess im Sinne des Artikels) 2, Nummer 14, der Verordnung (EU) 2019/881; [18]

31. „Altsystem“ bezeichnet ein IKT-Altsystem im Sinne des Artikels) 3(3) der Verordnung (EU) 2022/2554; [19]

[12] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881
[13] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[14] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[15] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[16] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881
[17] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881
[18] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881
[19] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2554

32. „nationale zentrale Anlaufstelle“ bezeichnet die von jedem Mitgliedstaat gemäß Artikel 8(3) der Richtlinie (EU) 2022/2555; [20] benannte oder eingerichtete zentrale Anlaufstelle;

33. „NIS-Behörden für das Cyberkrisenmanagement“ bezeichnet die gemäß Artikel 9, point (1) of Directive (EU) 2022/2555; [21] benannten oder eingerichteten Behörden;

34. „Urheber“ bezeichnet eine Einrichtung, die einen Informationsaustausch, eine Informationsübermittlung oder die Speicherung von Informationen einleitet;

35. „Spezifikationen für die Auftragsvergabe“ bezeichnet die von Einrichtungen für die Beschaffung neuer oder aktualisierter IKT-Produkte, -Prozesse oder -Dienste festgelegten Spezifikationen;

36. „Vertreter“ bezeichnet eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich dafür benannt wurde, im Namen einer Einrichtung mit erheblichen oder kritischen Auswirkungen, die nicht in der Union niedergelassen ist, aber Dienstleistungen für Einrichtungen in der Union erbringt, zu handeln, und an die sich eine zuständige Behörde oder ein CSIRT — statt an die Einrichtung mit erheblichen oder kritischen Auswirkungen — in Bezug auf die in dieser Verordnung festgelegten Verpflichtungen dieser Einrichtung wenden kann;

37. „Risiko“ bezeichnet ein Risiko im Sinne des Artikels) 6, Nummer 9, der Richtlinie (EU) 2022/2555; [22]

38. „Risiko-Auswirkungs-Matrix“ bezeichnet eine Matrix, die bei der Risikobewertung genutzt wird, um für jedes bewertete Risiko die mit ihm verbundenen Auswirkungen zu bestimmen;

39. „zeitgleich auftretende Stromversorgungskrise“ bezeichnet eine Stromversorgungskrise im Sinne des Artikels) 2, Nummer 10, der Verordnung (EU) 2019/941; [23]

40. „zentrale Anlaufstelle auf Ebene der Einrichtung“ bezeichnet eine zentrale Anlaufstelle bei der Einrichtung gemäß Artikel 38(1) point (c); [24]

41. „Interessenträger“ bezeichnet jede Partei, die am Erfolg und laufenden Betrieb einer Organisation oder eines Prozesses beteiligt ist, wie z. B. Beschäftigte, Direktoren, Anteilseigner, Regulierungsbehörden, Verbände, Lieferanten und Kunden;

42. „Norm“ bezeichnet eine Norm im Sinne des Artikels) 2 Nummer 1 Buchstabe c der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates (16); [25]

43. „Netzbetriebsregion“ bezeichnet die gemäß Anhang) I zur Entscheidung 05-2022 der ACER über die Definition der Netzbetriebsregionen [26] festgelegten Netzbetriebsregionen, die in Übereinstimmung mit Artikel 36 der Verordnung (EU) 2019/943 bestimmt wurden;

44. „Netzbetreiber“ bezeichnet „Verteilernetzbetreiber“ (VNB) und „Übertragungsnetzbetreiber“ (ÜNB) im Sinne des Artikels) 2(29) bzw. 2(35) der Richtlinie (EU) 2019/944; [27]

[20] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[21] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[22] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[23] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941
[24] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[25] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[26] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[27] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944

45. „unionsweiter Prozess mit kritischen Auswirkungen“ bezeichnet jeden Prozess im Elektrizitätssektor, an dem mehrere Einrichtungen beteiligt sein können und bei dem die möglichen Auswirkungen eines Cyberangriffs bei der Durchführung der unionsweiten Bewertung des Cybersicherheitsrisikos für kritisch erachtet werden können;

46. „unionsweiter Prozess mit erheblichen Auswirkungen“ bezeichnet jeden Prozess im Elektrizitätssektor, an dem mehrere Einrichtungen beteiligt sein können und bei dem die möglichen Auswirkungen eines Cyberangriffs bei der Durchführung der unionsweiten Bewertung des Cybersicherheitsrisikos für erheblich erachtet werden können;

47. „aktiv ausgenutzte Schwachstelle ohne Patch“ bezeichnet eine noch nicht öffentlich bekannt gegebene und noch nicht mit einem Patch versehene Schwachstelle, in Bezug auf die verlässliche Nachweise dafür vorliegen, dass ein Akteur ohne Zustimmung des Systemeigners einen schädlichen Programmcode in einem System ausgeführt hat;

48. „Schwachstelle“ bezeichnet eine Schwachstelle im Sinne des Artikels) 6, Nummer 15, der Richtlinie (EU) 2022/2555. [28]

[28] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555

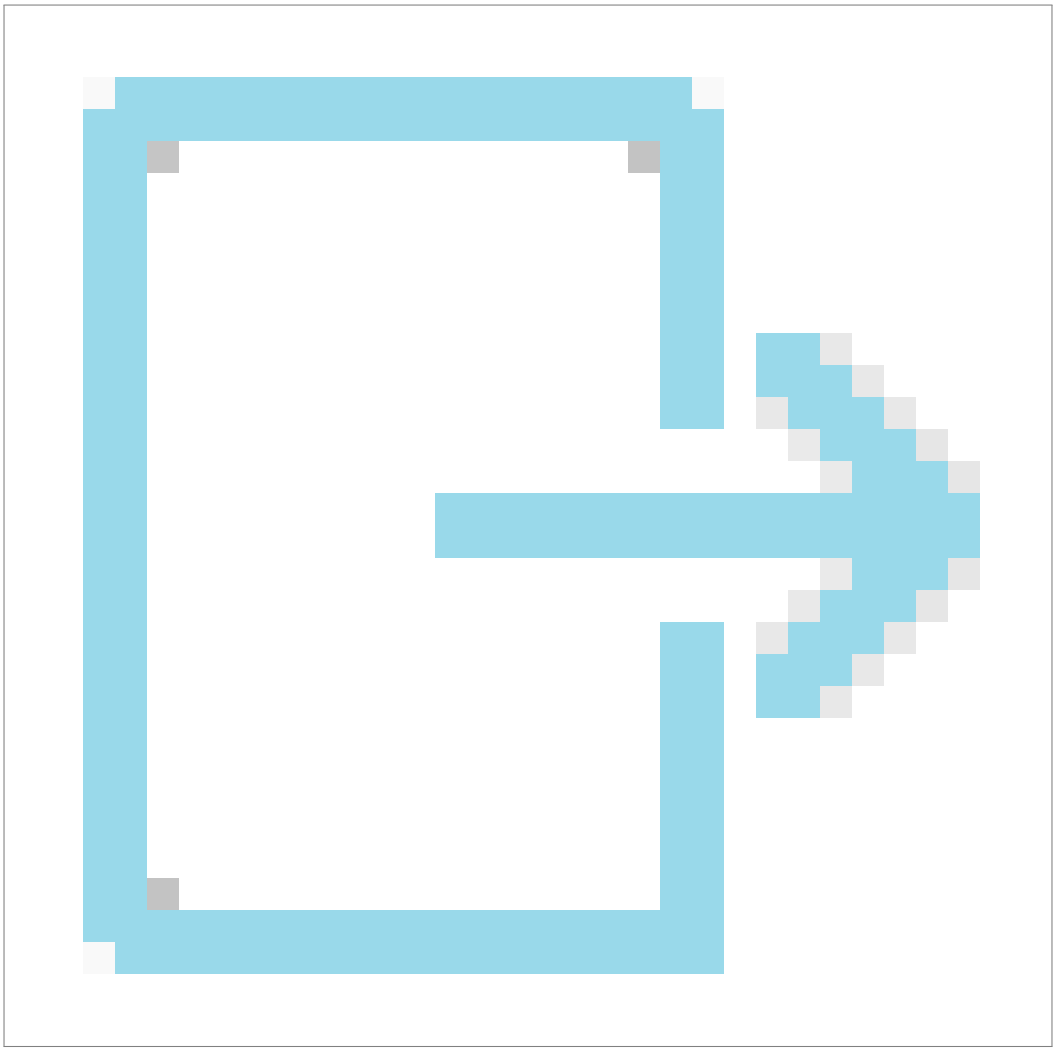
Chapter 6

Artikel 4. : Zuständige Behörde

6.1 Absatz 1

So bald wie möglich, in jedem Fall aber bis zum 13 Dezember 2024, benennt jeder Mitgliedstaat eine nationale Regierungs- oder Regulierungsbehörde, die für die Wahrnehmung der ihr in dieser Verordnung übertragenen Aufgaben zuständig ist (im Folgenden „zuständige Behörde“). Bis die Aufgaben im Rahmen dieser Verordnung auf die zuständige Behörde übertragen wurden, nimmt die von jedem Mitgliedstaat gemäß Artikel 57 Absatz 1 der Richtlinie (EU) 2019/944 [a] benannte Regulierungsbehörde die Aufgaben der zuständigen Behörde im Einklang mit dieser Verordnung wahr.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02019L0944-20240716#art_57



Output

- Zuständige Behörde

GOOD TO KNOW

Zeitpunkt

So bald wie möglich, spätestens jedoch bis zum 13. Dezember 2024

Verantwortlich für die Aktivität: MS

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: MS

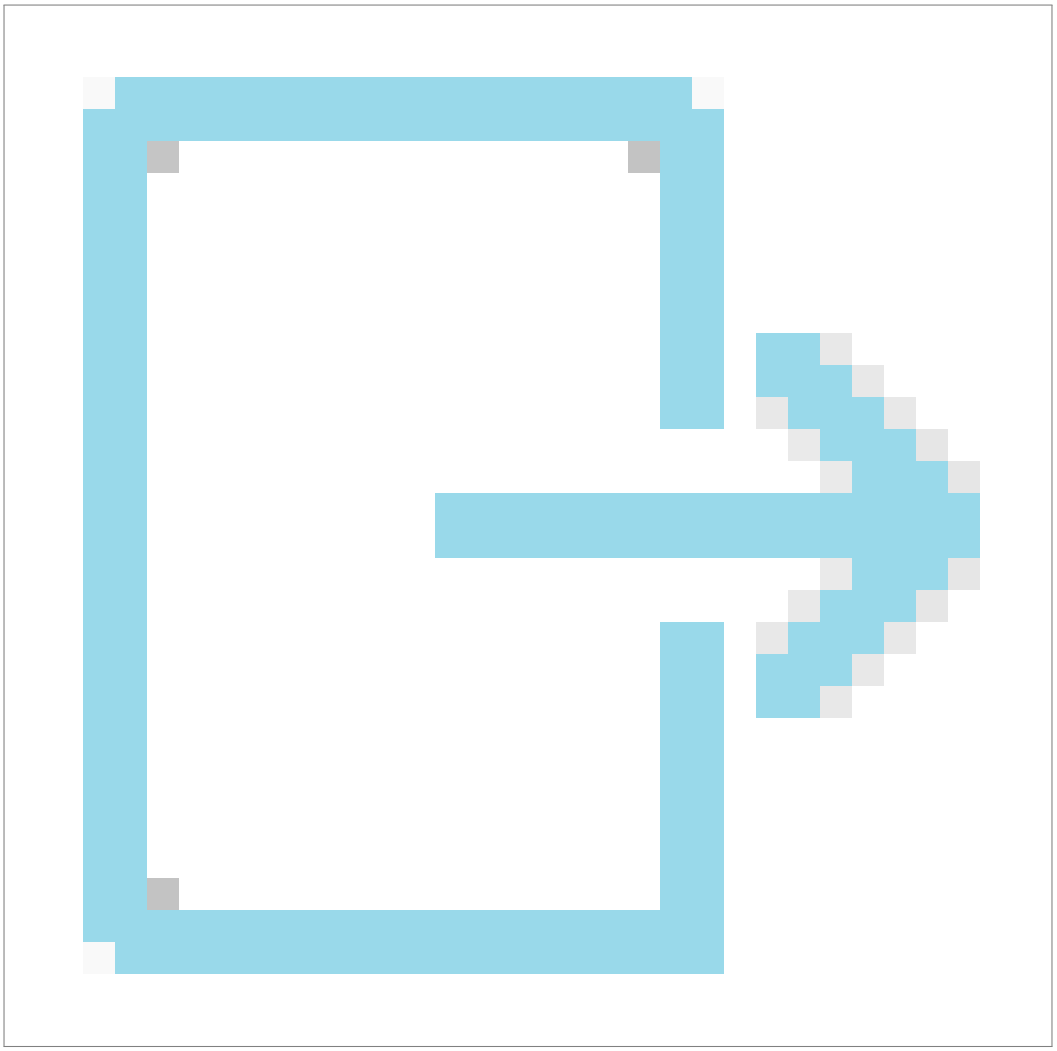
6.2 Absatz 2

Die Mitgliedstaaten unterrichten die Kommission, die ACER, die ENISA, die gemäß Artikel 14 der Richtlinie (EU) 2022/2555 [a] eingesetzte NIS-Kooperationsgruppe und die gemäß Artikel 1 des Beschlusses der Kommission vom 15. November 2012 [b] eingesetzte Koordinierungsgruppe „Strom“ unverzüglich und teilen ihnen den Namen und die Kontaktdaten ihrer gemäß Absatz 1 des vorliegenden Artikels benannten zuständigen Behörde sowie etwaige spätere Änderungen in Bezug auf diese Behörde mit.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_14
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32012D1117(01)

Relevante NCCS-Artikel

- Artikel 4 (1)



Output

- Benachrichtigung

GOOD TO KNOW

Zeitpunkt

Ohne Verzögerung

Verantwortlich für die Aktivität: MS

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: MS

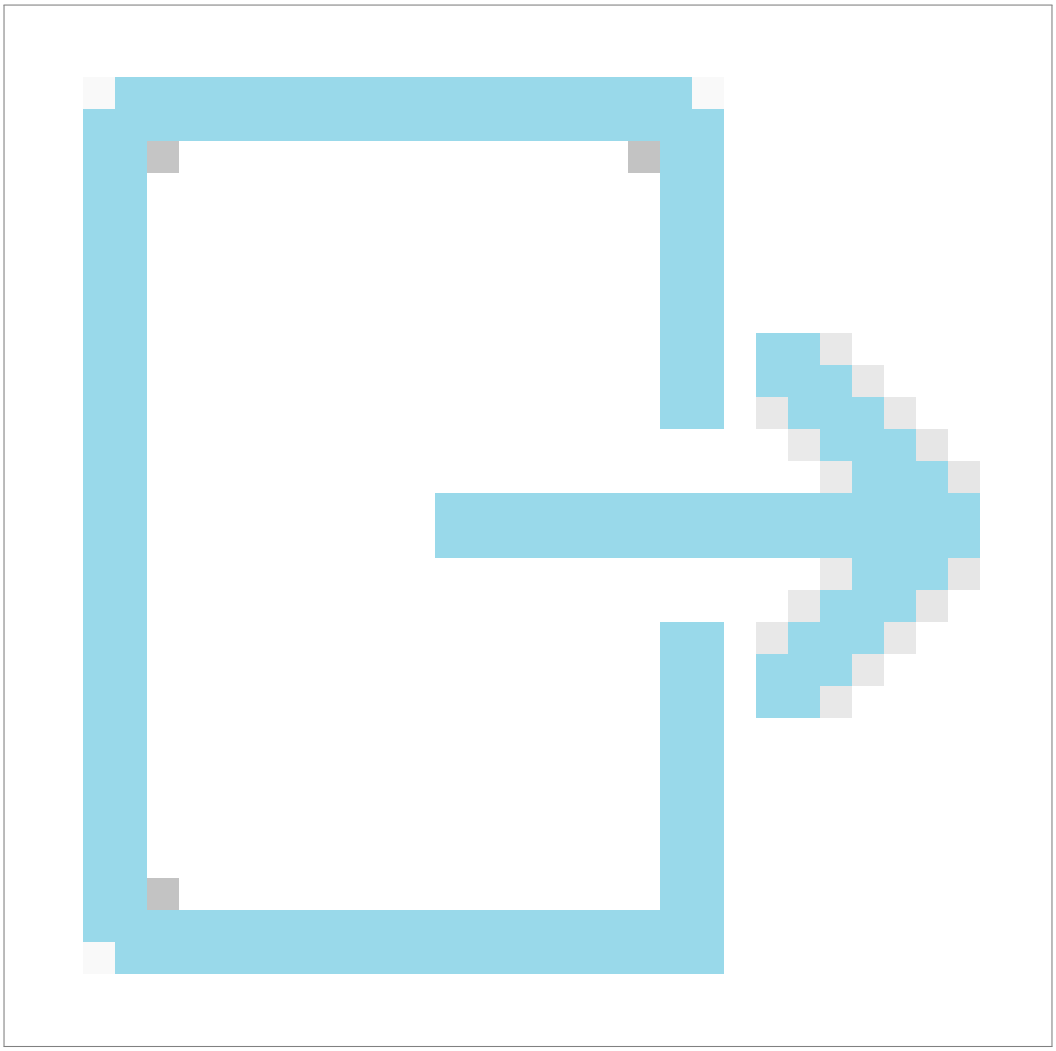
Zu informieren: EC, ACER, ENISA, NIS CG, ECG

6.3 Absatz 3

Die Mitgliedstaaten können ihrer zuständigen Behörde gestatten, Aufgaben, die ihr in dieser Verordnung übertragen wurden, an andere nationale Behörden zu delegieren, mit Ausnahme der in Artikel 5 aufgeführten Aufgaben. Jede zuständige Behörde überwacht die Anwendung dieser Verordnung durch die Behörden, an die sie Aufgaben delegiert hat.

Relevante NCCS-Artikel

- Artikel 5



Output

- Delegierung

A

Verantwortlich für die Aktivität: MS

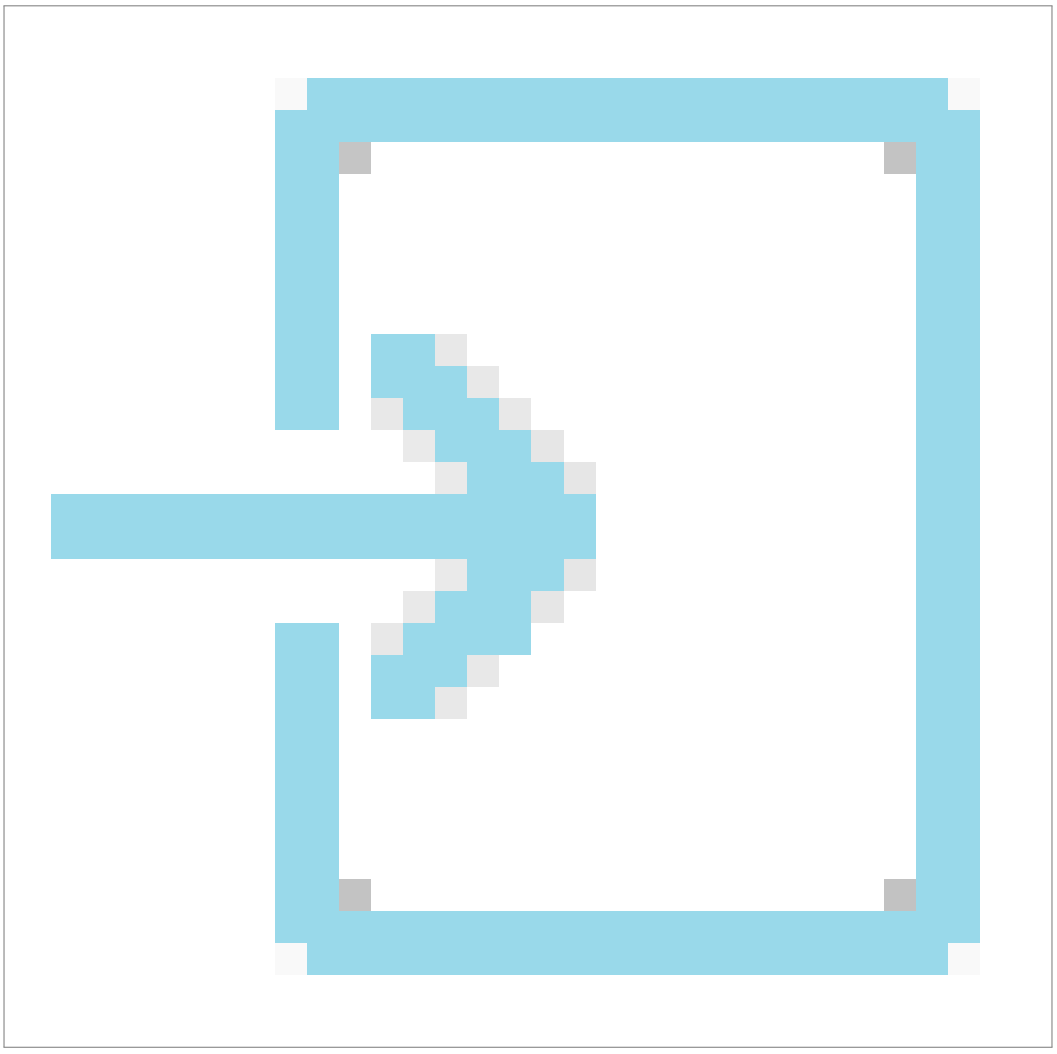
Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: MS, NCA

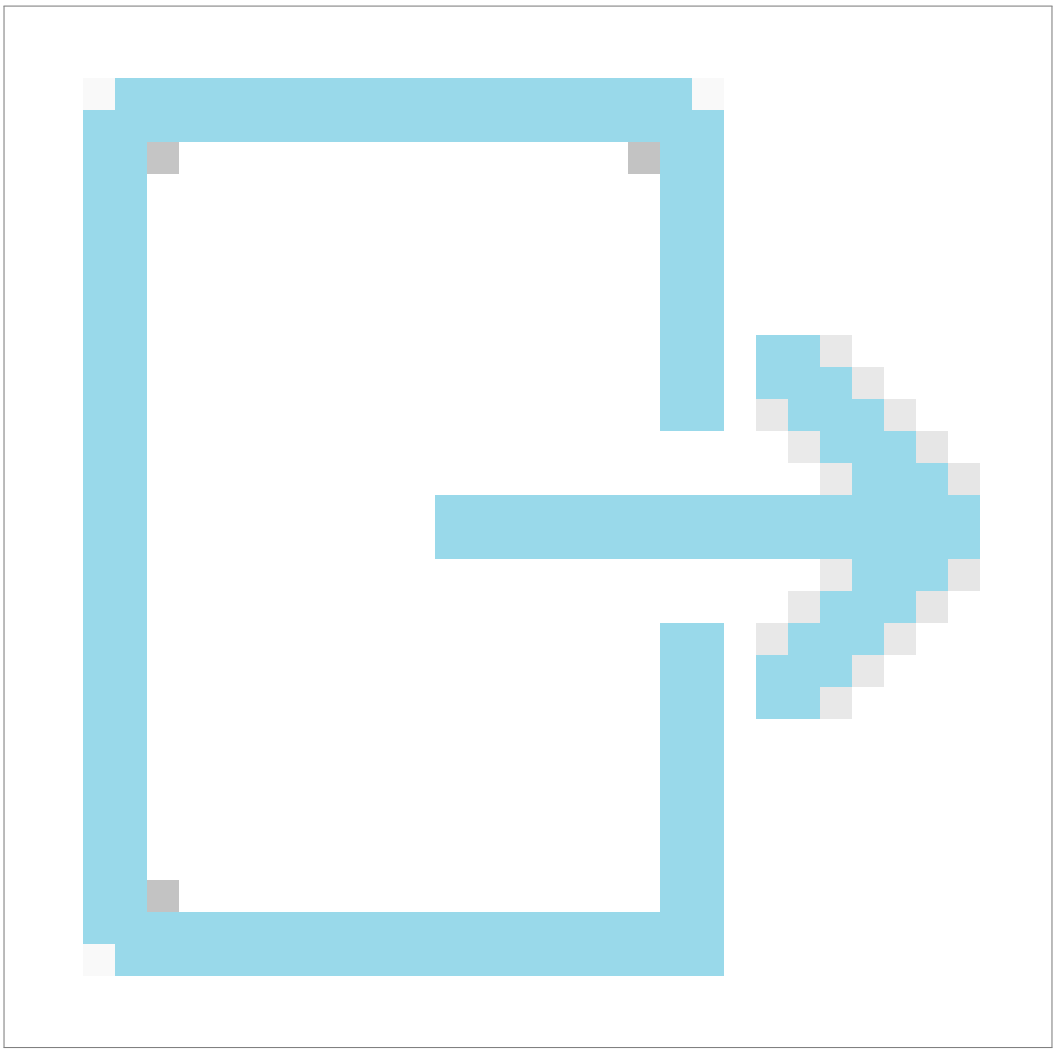
6.4 Absatz 3

Die zuständige Behörde teilt der Kommission, der ACER, der Koordinierungsgruppe „Strom“, der ENISA und der NISKooperationsgruppe den Namen der Behörden, an die sie Aufgaben delegiert hat, deren Kontaktdaten, die ihnen übertragenen Aufgaben sowie etwaige spätere Änderungen mit.



Input

- Delegierung



Output

- Delegationsdetails

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu informieren: EC, ACER, ENISA, NIS CG, ECG

Chapter 7

Artikel 5. : Zusammenarbeit zwischen den zuständigen Behörden und Stellen auf nationaler Ebene

7.1 Absatz

Die zuständigen Behörden koordinieren und gewährleisten eine angemessene Zusammenarbeit zwischen den für Cybersicherheit zuständigen Behörden, den Behörden für das Cyberkrisenmanagement, den NRB, den für die Risikovorsorge zuständigen Behörden und den CSIRTs im Hinblick auf die Erfüllung der in dieser Verordnung festgelegten einschlägigen Verpflichtungen. Zudem stimmen sich die zuständigen Behörden mit anderen von den einzelnen Mitgliedstaaten bestimmten Stellen oder Behörden ab, um effiziente Verfahren sicherzustellen und Überschneidungen von Aufgaben und Pflichten zu vermeiden. Die zuständigen Behörden können die jeweiligen NRB anweisen, die ACER gemäß Artikel 8 Absatz 3 um eine Stellungnahme zu ersuchen.

Relevante NCCS-Artikel

- Artikel 8 (3)

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ACER, NCA, NRA, RP NCA, CSIRT, CS NCA

Chapter 8

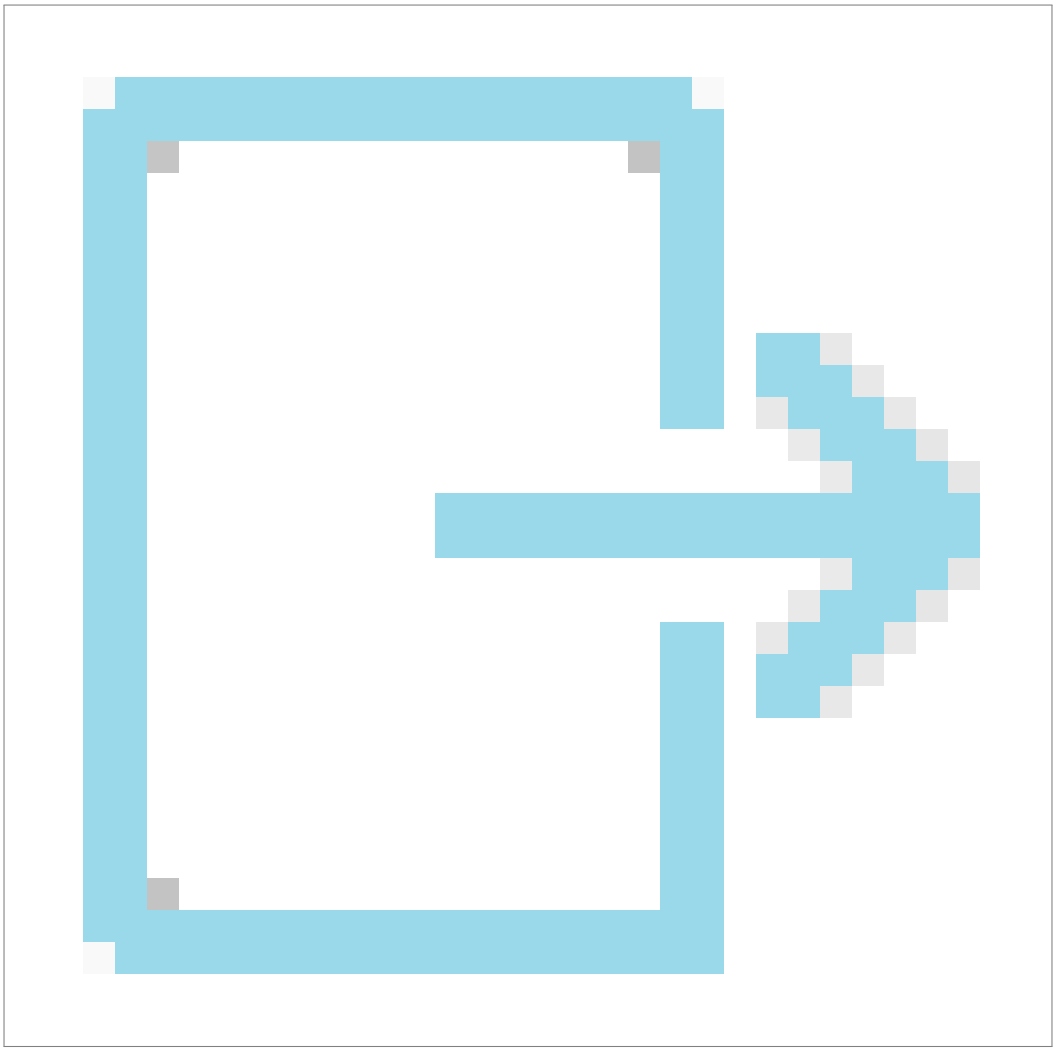
Artikel 6. : Modalitäten oder Methoden oder Pläne

8.1 Absatz 1

Die ÜNB entwickeln in Zusammenarbeit mit der EU-VNBO Vorschläge für die Modalitäten oder Methoden gemäß Absatz 2 bzw. für Pläne gemäß Absatz 3.

Relevante NCCS-Artikel

- Artikel 6 (2)
- Artikel 6 (3)



Output

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Regionaler Plan zur Risikominderung (Entwurf)

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu informieren: ACER, NCA

8.2 Absatz 2

Die folgenden Modalitäten oder Methoden und etwaige Änderungen dieser Modalitäten oder Methoden bedürfen der Genehmigung aller zuständigen Behörden:

a. die Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 18 Absatz 1;

b. der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23;

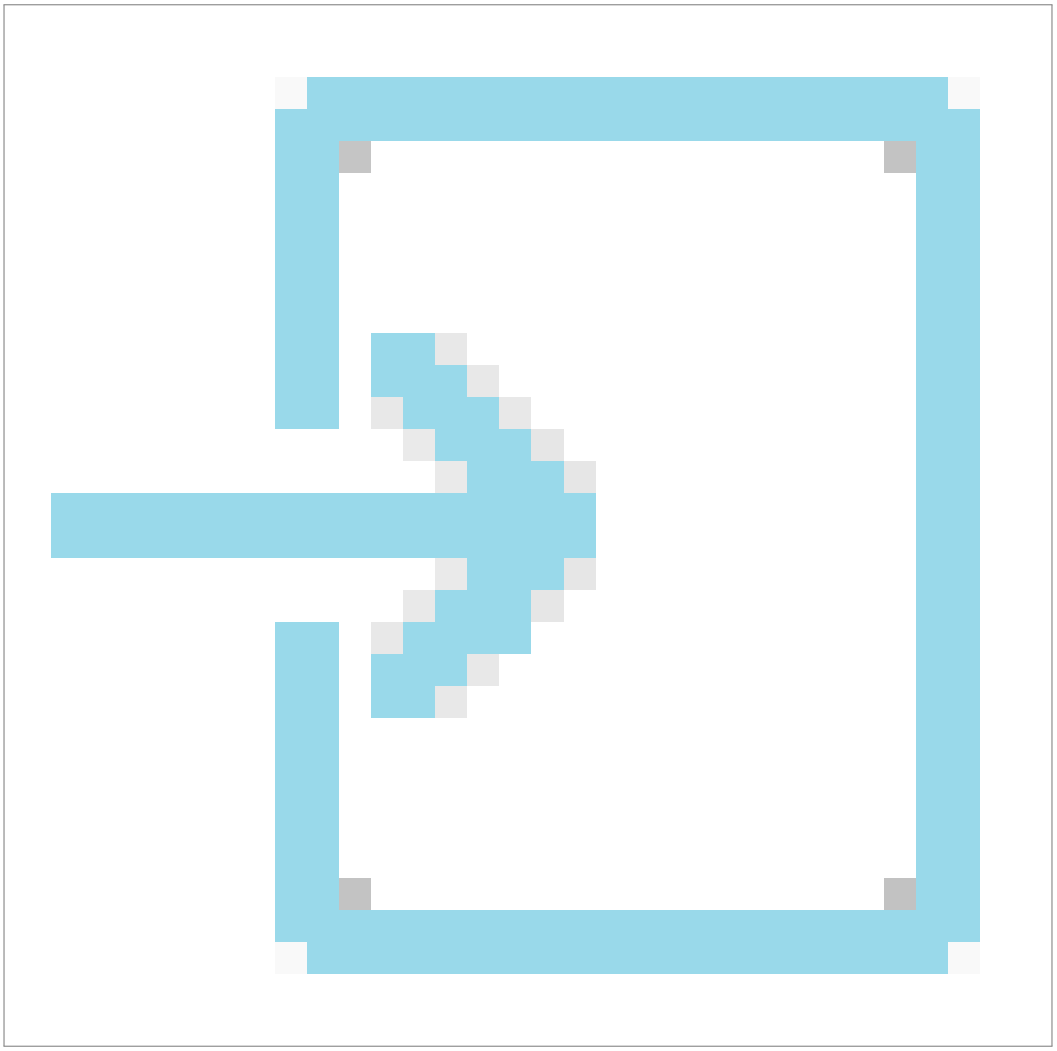
c. die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen gemäß Artikel 29, der Vergleich der Cybersicherheitskontrollen im Elektrizitätssektor anhand von Normen gemäß Artikel 34, einschließlich Mindest-Cybersicherheitskontrollen und erweiterter Cybersicherheitskontrollen in der Lieferkette gemäß Artikel 33;

d. eine Empfehlung für die Cybersicherheit bei der Auftragsvergabe gemäß Artikel 35;

e. die Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8.

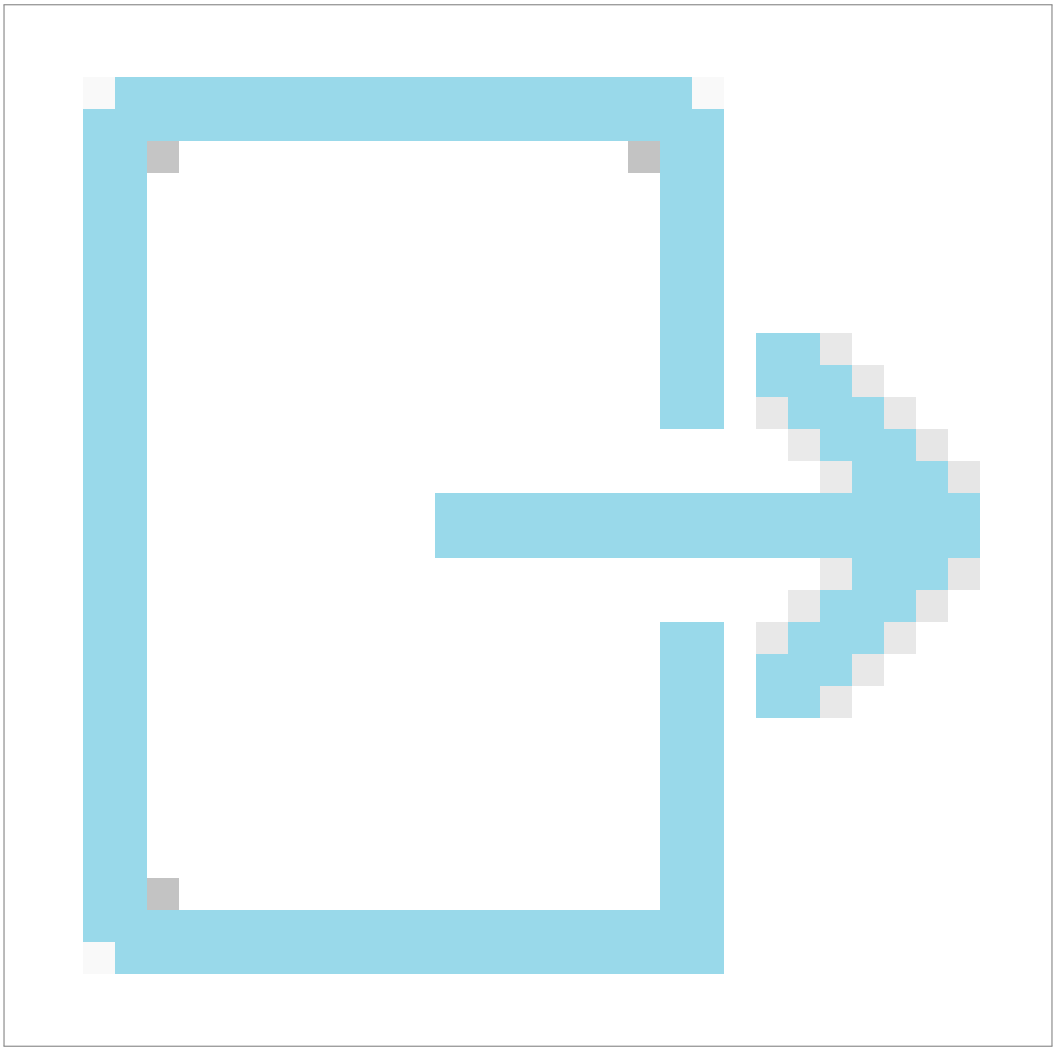
Relevante NCCS-Artikel

- Artikel 18 (1)
- Artikel 29
- Artikel 34
- Artikel 33
- Artikel 35
- Artikel 37 (8)



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)
- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)



Output

- Methoden zur Risikobewertung (genehmigt)
- Umfassender Risikobewertungsbericht (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen (genehmigt)
- Erweiterte Cybersicherheitskontrollen (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (genehmigt)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (genehmigt)
- Zuordnungsmatrix (genehmigt)
- Empfehlungen für die Beschaffung (genehmigt)
- Methodik zur Klassifizierung von Cyberangriffen (genehmigt)

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

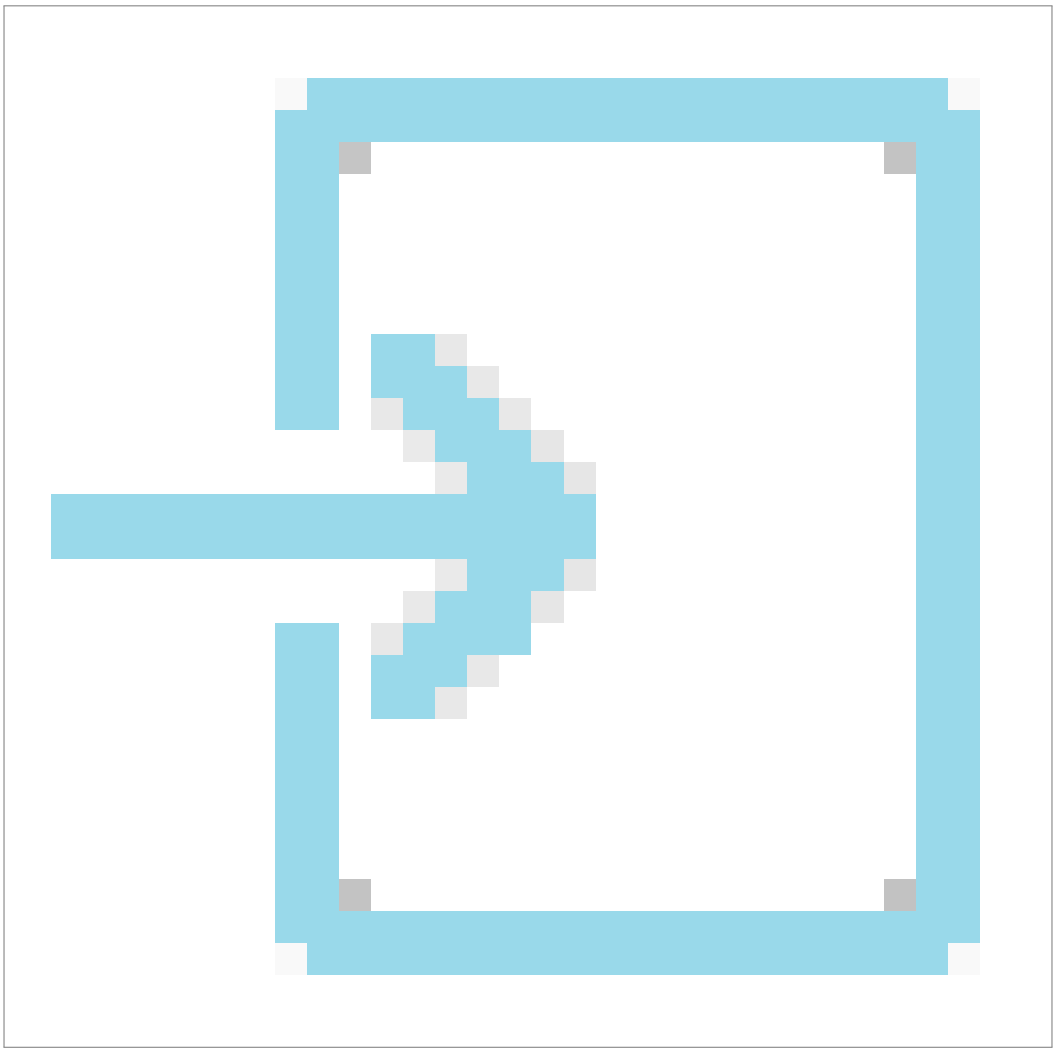
Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO, NCA

8.3 Absatz 3

Die Vorschläge für die regionalen Pläne zur Minderung des Cybersicherheitsrisikos gemäß Artikel 22 bedürfen der Genehmigung aller zuständigen Behörden der betreffenden Netzbetriebsregion.

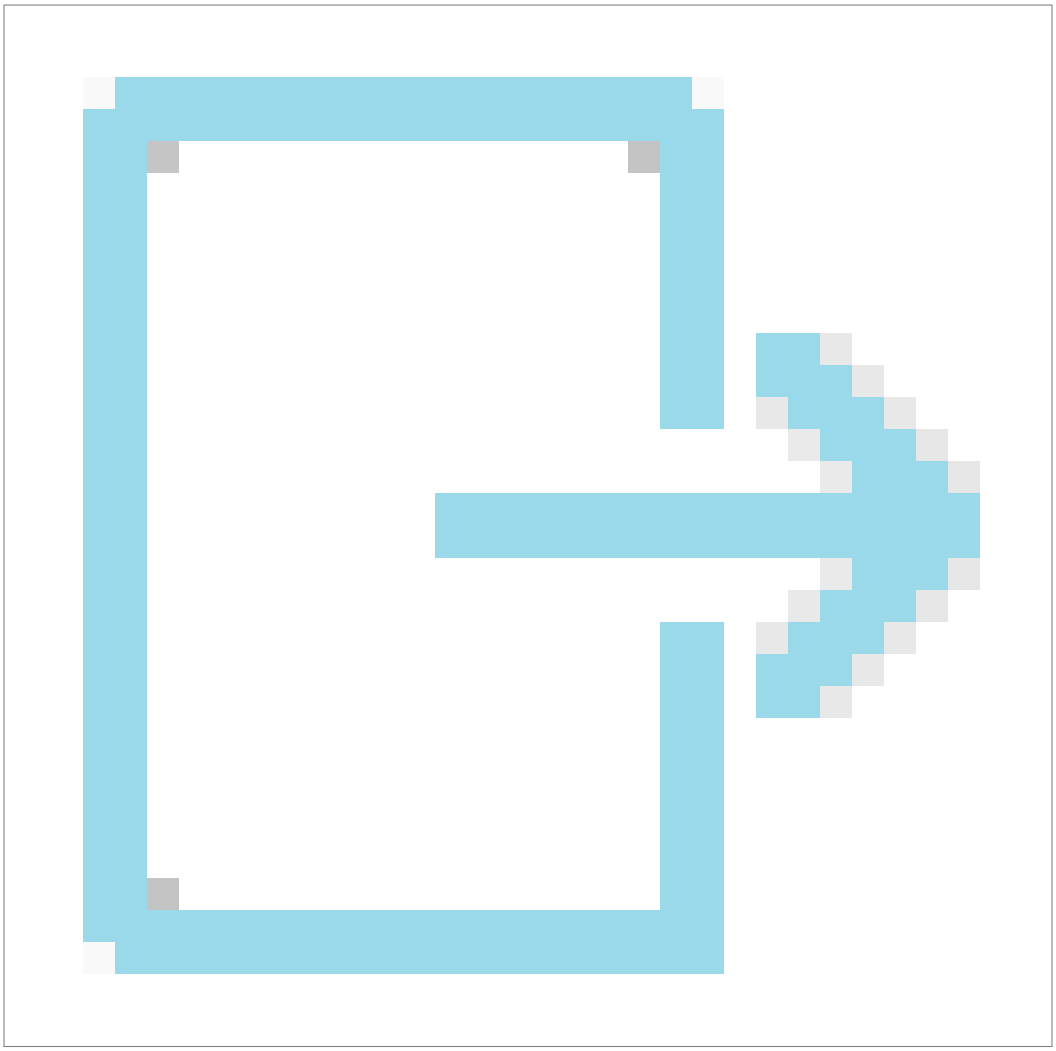
Relevante NCCS-Artikel

- Artikel 22



Input

- Regionaler Risikominderungsplan (Entwurf)



Output

- Regionaler Risikominderungsplan (genehmigt)

A

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO, NCA

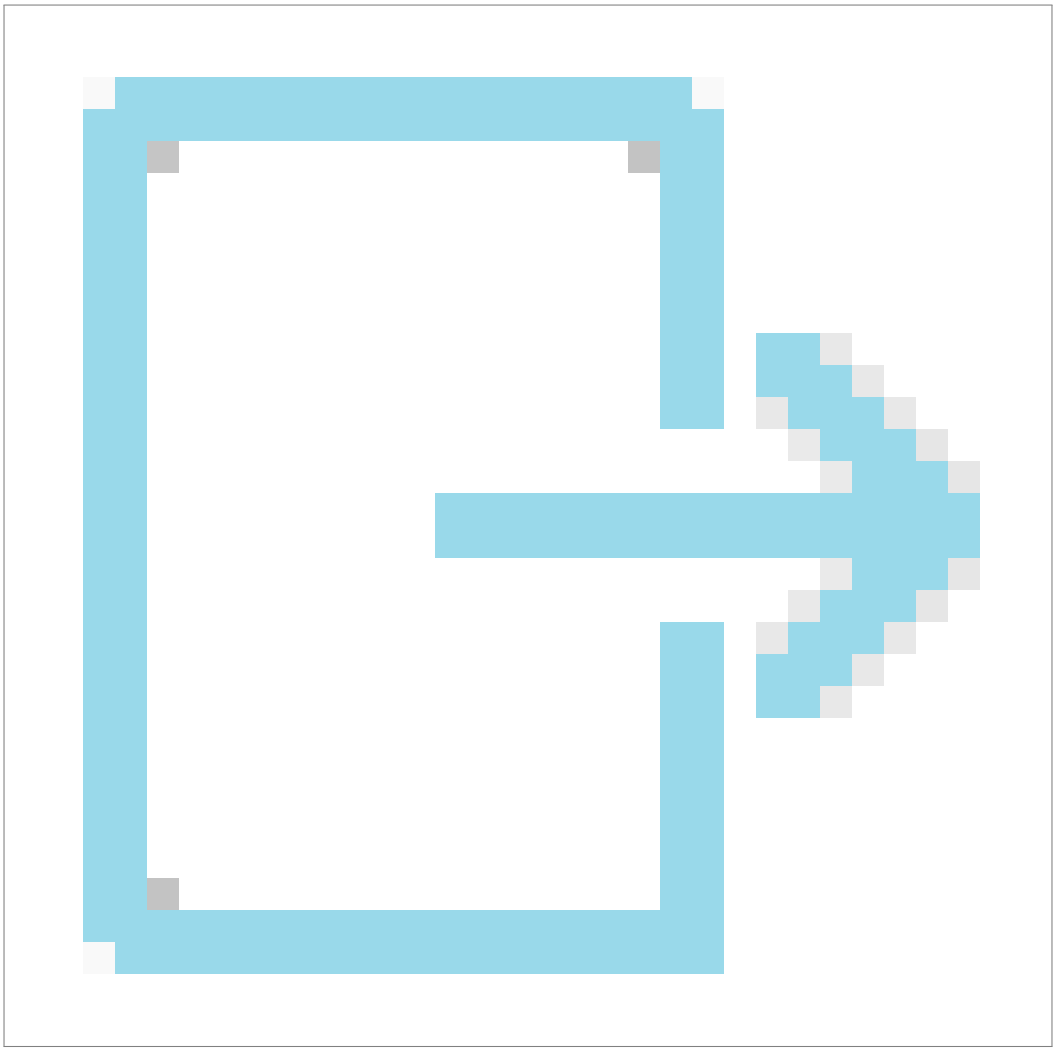
Zu konsultieren: NIS CG, RCC

8.4 Absatz 4

Die Vorschläge für Modalitäten oder Methoden gemäß Absatz 2 bzw. für Pläne gemäß Absatz 3 müssen einen Vorschlag für den Zeitplan für ihre Umsetzung und eine Beschreibung ihrer erwarteten Auswirkungen auf die Ziele dieser Verordnung enthalten.

Relevante NCCS-Artikel

- Artikel 32 (1)
- Artikel 6 (3)



Output

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Regionaler Plan zur Risikominderung (Entwurf)

Verantwortlich für die Aktivität: TSO

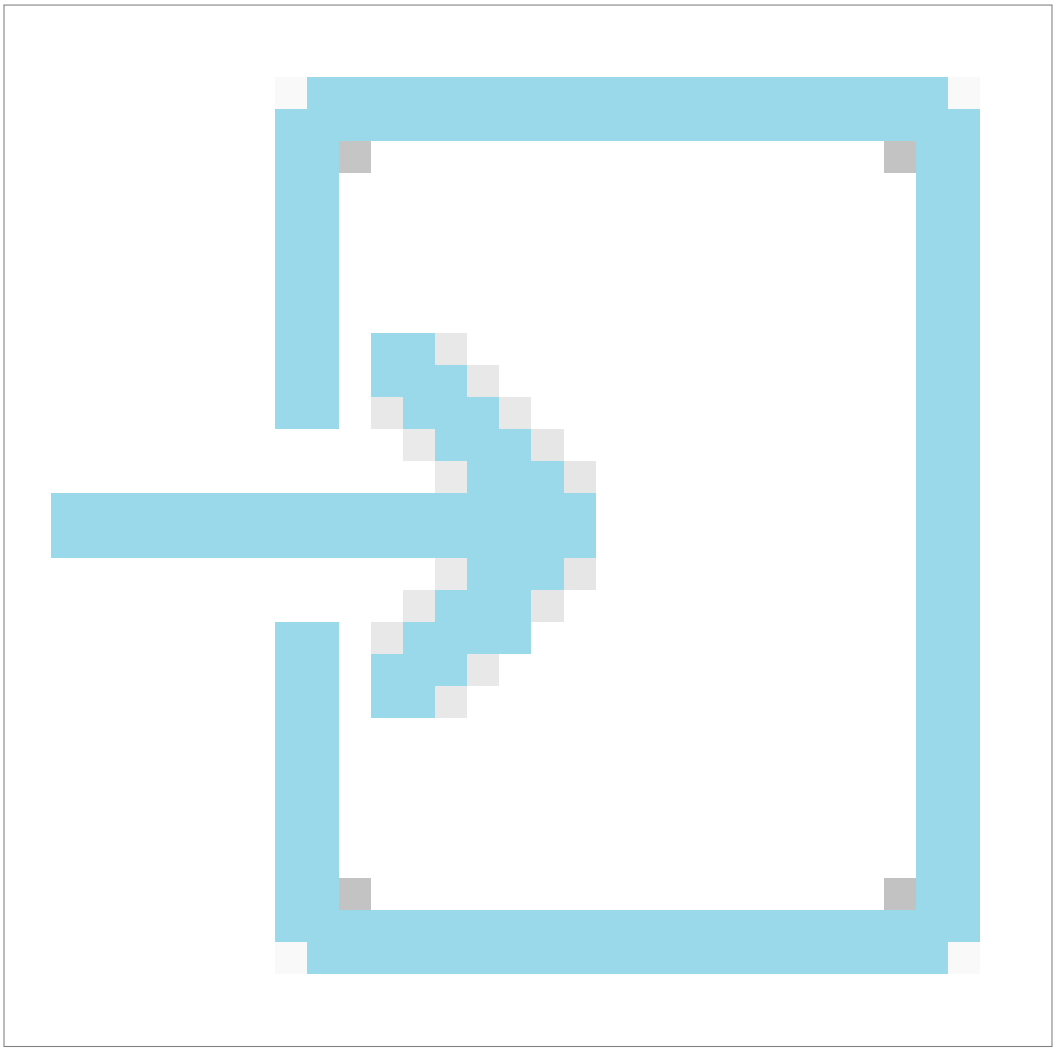
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu informieren: ACER, NCA

8.5 Absatz 5

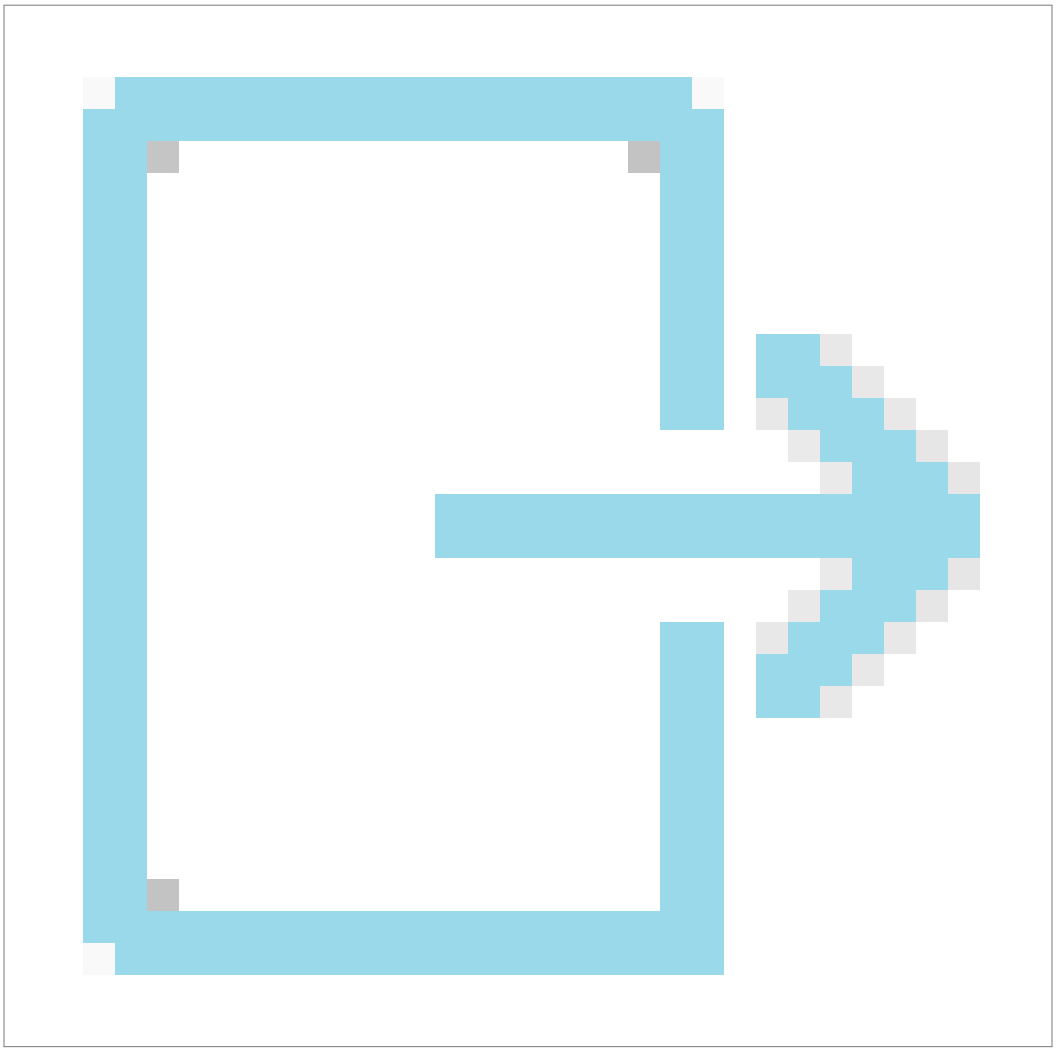
Die EU-VNBO kann den betreffenden ÜNB bis zu drei Wochen vor Ablauf der Frist für die Übermittlung des Vorschlags für Modalitäten, Methoden oder Pläne an die zuständigen Behörden eine mit Gründen versehene Stellungnahme übermitteln.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Regionaler Plan zur Risikominderung (Entwurf)



Output

- Meinung der EU-DSO

GOOD TO KNOW

Zeitpunkt

> bis 3 Wochen vor Einreichung

Verantwortlich für die Aktivität: EU DSO

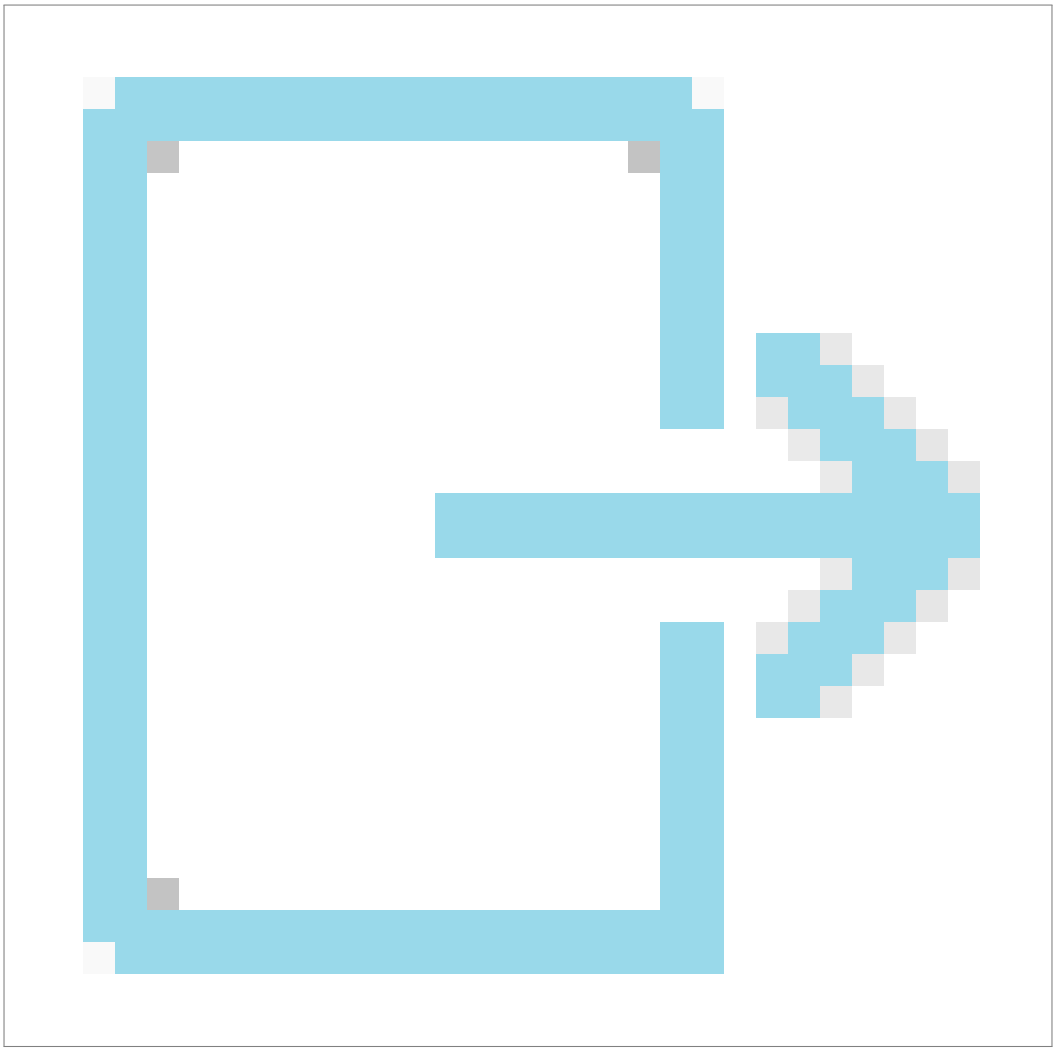
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: EU DSO

Zu informieren: TSO

8.6 Absatz 5

Die für den Vorschlag für Modalitäten, Methoden oder Pläne zuständigen ÜNB berücksichtigen die mit Gründen versehene Stellungnahme der EU-VNBO, bevor sie den Vorschlag den zuständigen Behörden zur Genehmigung vorlegen. Wenn die ÜNB die Stellungnahme der EU-VNBO nicht berücksichtigen, begründen sie dies.



Output

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Regionaler Plan zur Risikominderung (Entwurf)

Verantwortlich für die Aktivität: TSO

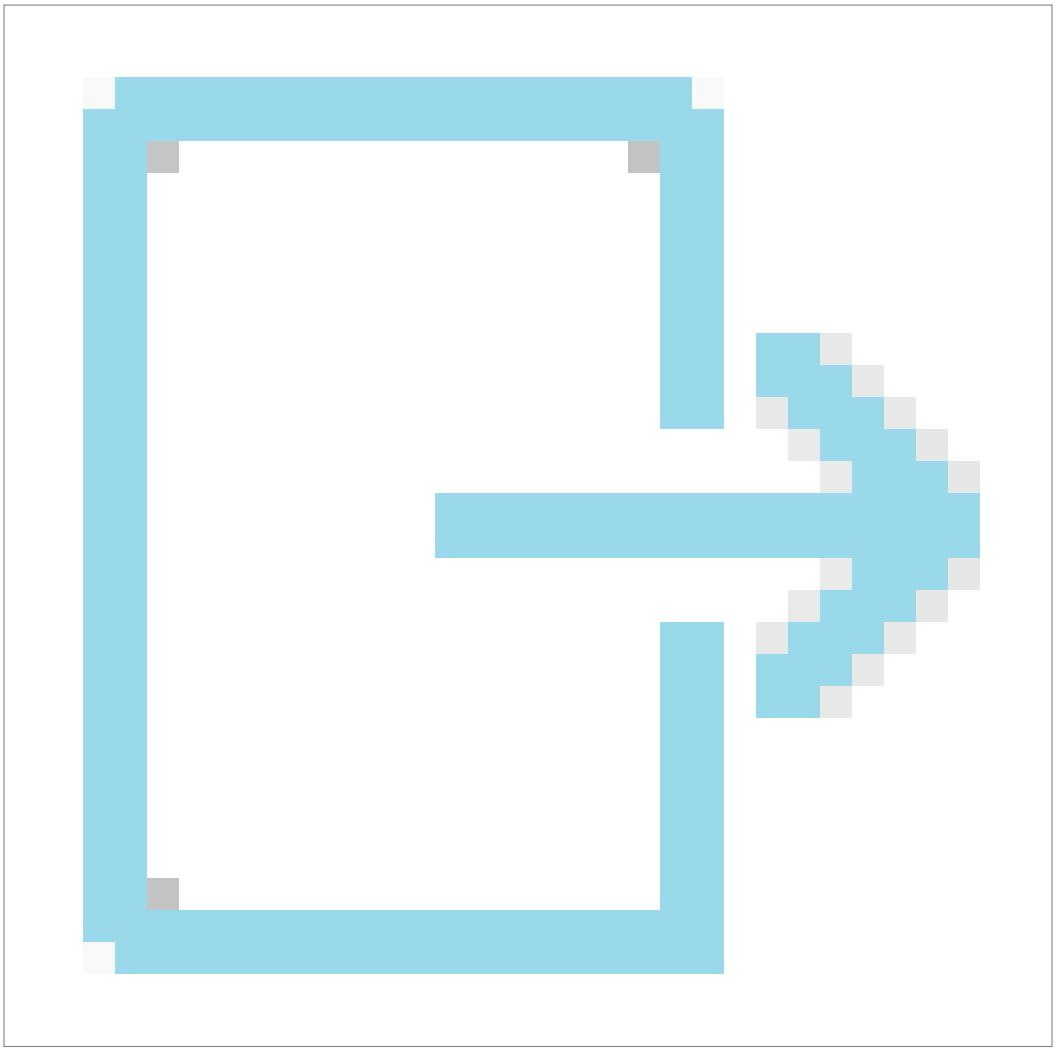
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu informieren: ACER, NCA

8.7 Absatz 6

Bei der gemeinsamen Entwicklung von Modalitäten, Methoden und Plänen arbeiten die teilnehmenden ÜNB eng zusammen. Die ÜNB unterrichten die zuständigen Behörden und die ACER mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO regelmäßig über die Fortschritte bei der Entwicklung der Modalitäten, Methoden oder Pläne.



Output

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Regionaler Plan zur Risikominderung (Entwurf)

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu informieren: ACER, NCA

Chapter 9

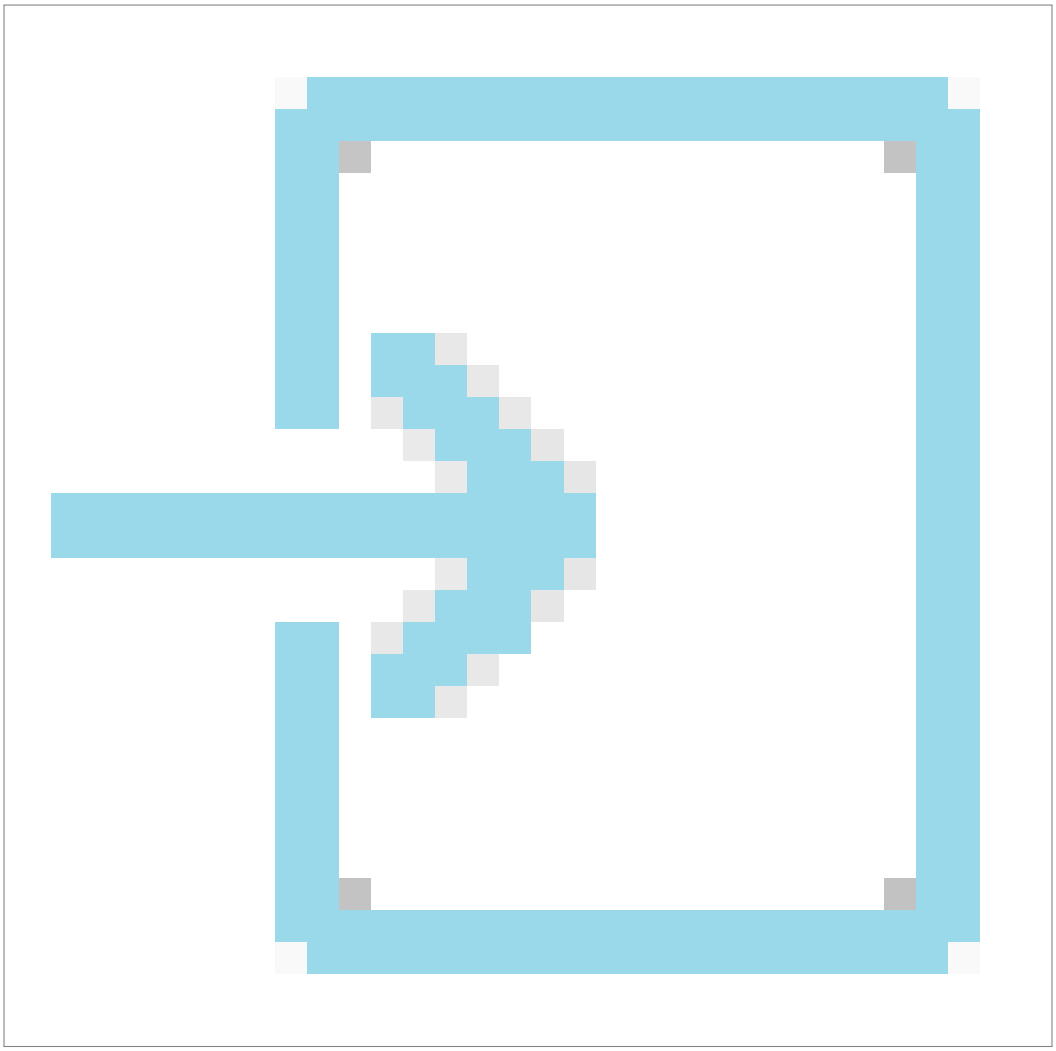
Artikel 7. : Vorschriften für Abstimmungen der ÜNB

9.1 Absatz 1

Können ÜNB bei der Entscheidung über Vorschläge für Modalitäten oder Methoden keine Einigung erzielen, so entscheiden sie mit qualifizierter Mehrheit. Die qualifizierte Mehrheit für diese Vorschläge wird wie folgt berechnet:

a. ÜNB, die mindestens 55 % der Mitgliedstaaten vertreten, und

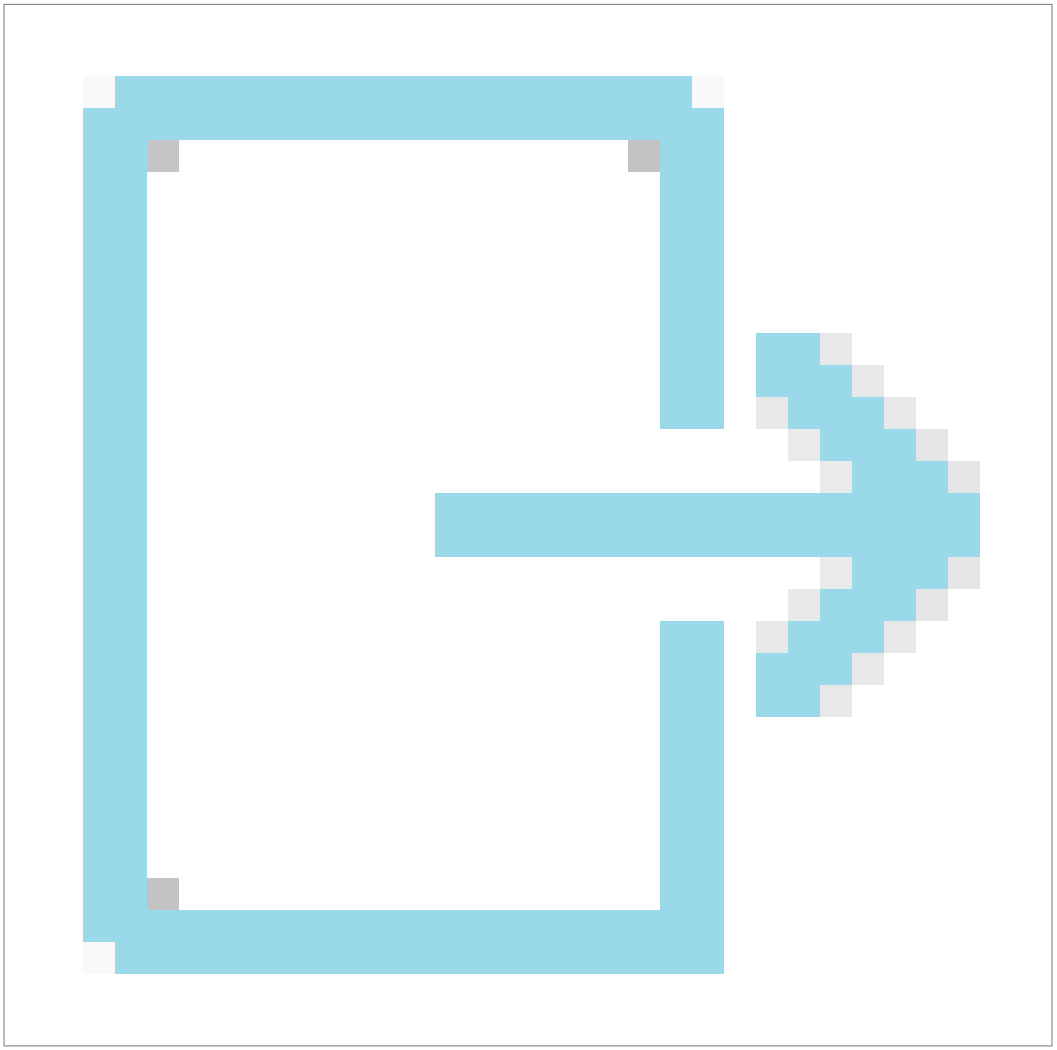
b. ÜNB, die Mitgliedstaaten vertreten, die mindestens 65 % der Bevölkerung der Union umfassen.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)



Output

- Entscheidung über Vorschläge

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

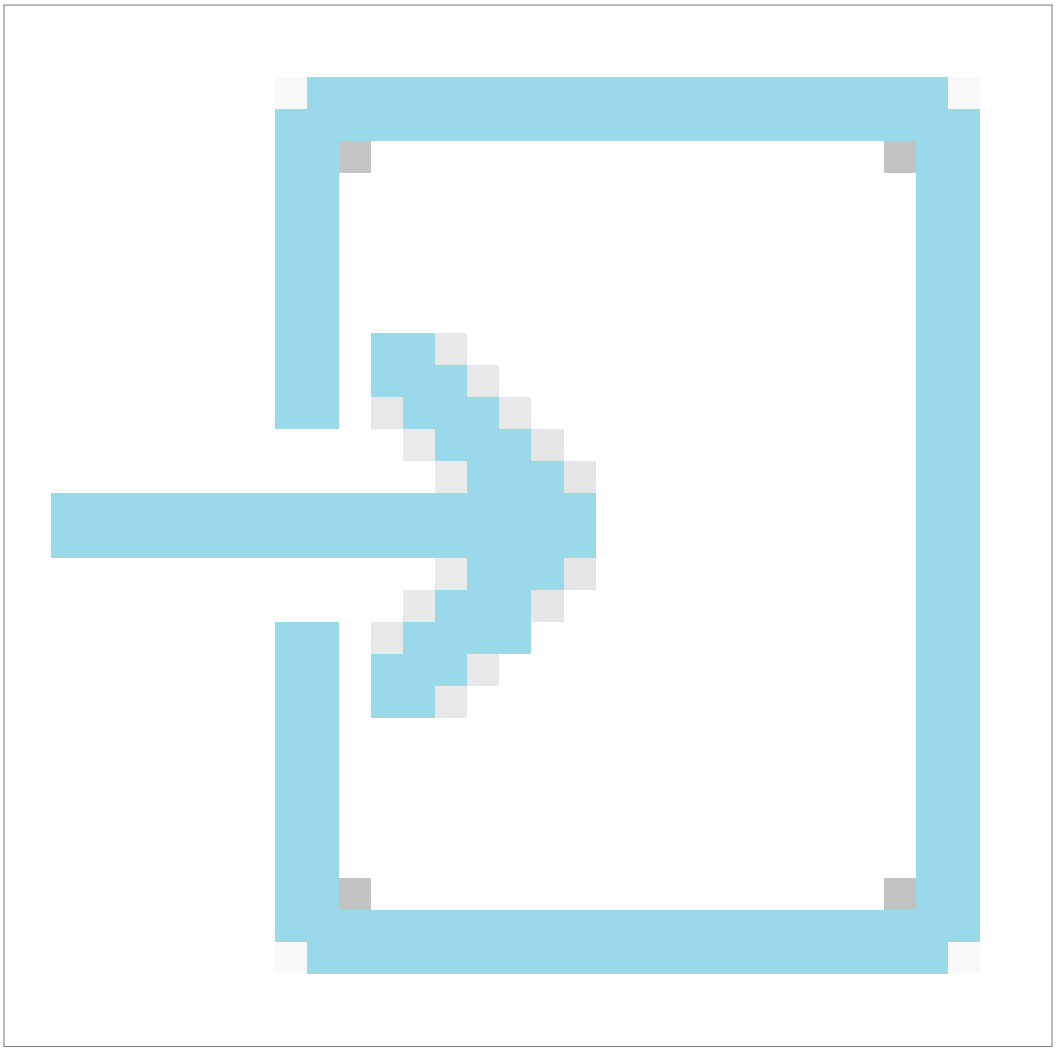
Beteiligt an der Aufgabenausführung: TSO

9.2 Absatz 2

Eine Sperrminorität bei Entscheidungen über Vorschläge für in Artikel 6 Absatz 2 aufgeführte Modalitäten oder Methoden ist mit ÜNB erreicht, die mindestens vier Mitgliedstaaten vertreten; andernfalls gilt die qualifizierte Mehrheit als erreicht.

Relevante NCCS-Artikel

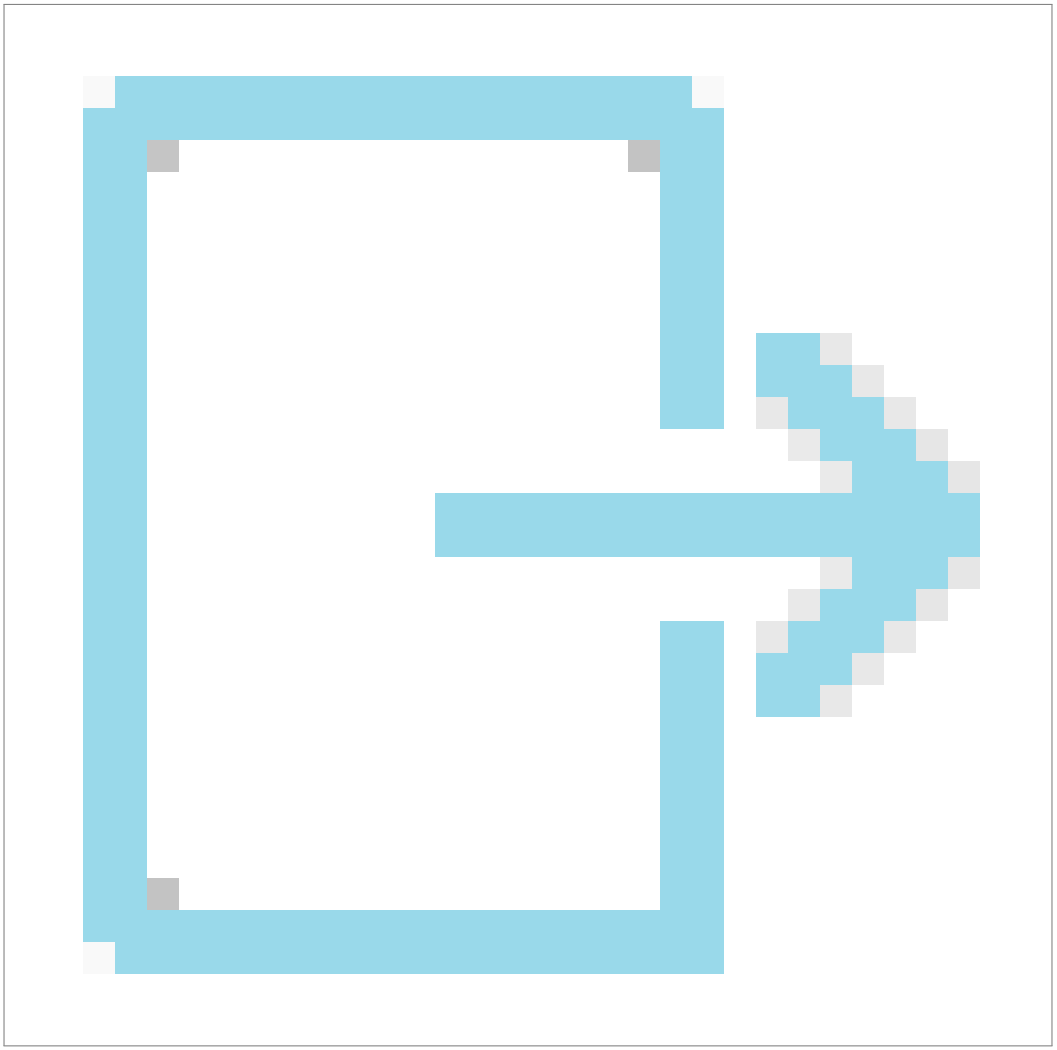
- Artikel 6 (2)



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)



Output

- Entscheidung über Vorschläge

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: TSO

9.3 Absatz 3

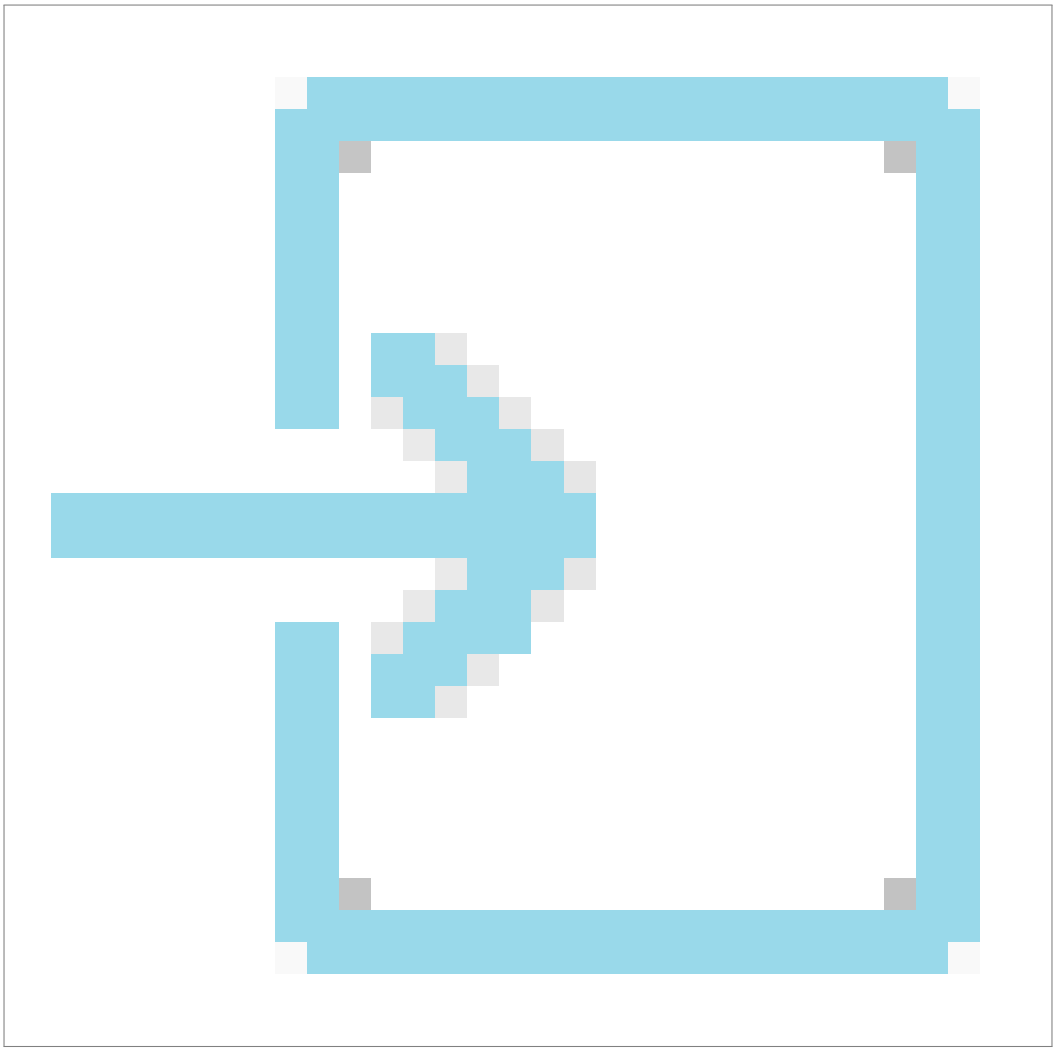
Können ÜNB einer Netzbetriebsregion bei der Entscheidung über Vorschläge für die in Artikel 6 Absatz 2 genannten Pläne keine Einigung erzielen und besteht die betreffende Netzbetriebsregion aus mehr als fünf Mitgliedstaaten, so entscheiden die ÜNB mit qualifizierter Mehrheit. Bei Vorschlägen gemäß Artikel 6 Absatz 2 ist für eine qualifizierte Mehrheit folgende Mehrheit erforderlich:

a. ÜNB, die mindestens 72 % der betroffenen Mitgliedstaaten vertreten, und

b. ÜNB, die Mitgliedstaaten vertreten, die mindestens 65 % der Bevölkerung der betroffenen Region umfassen.

Relevante NCCS-Artikel

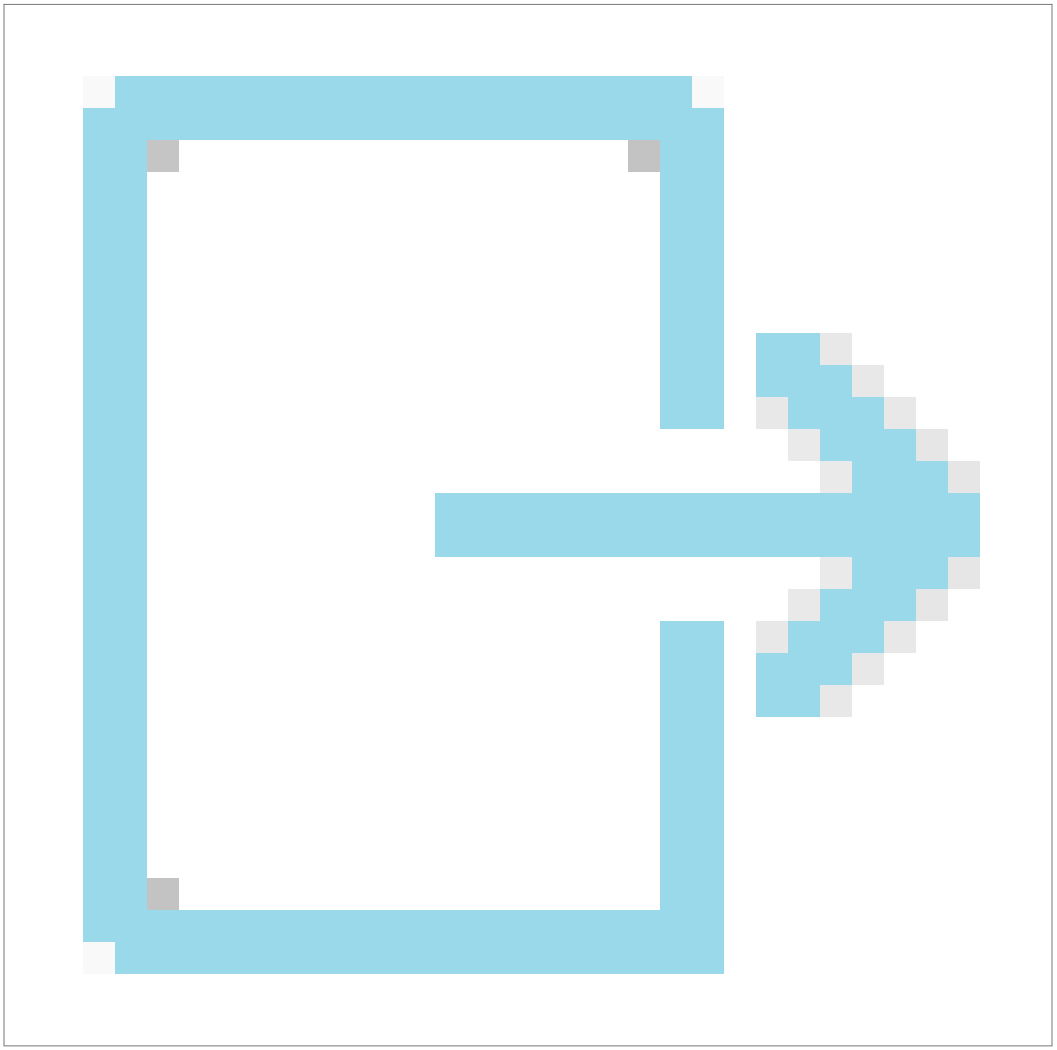
- Artikel 6 (2)



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)



Output

- Entscheidung über Vorschläge

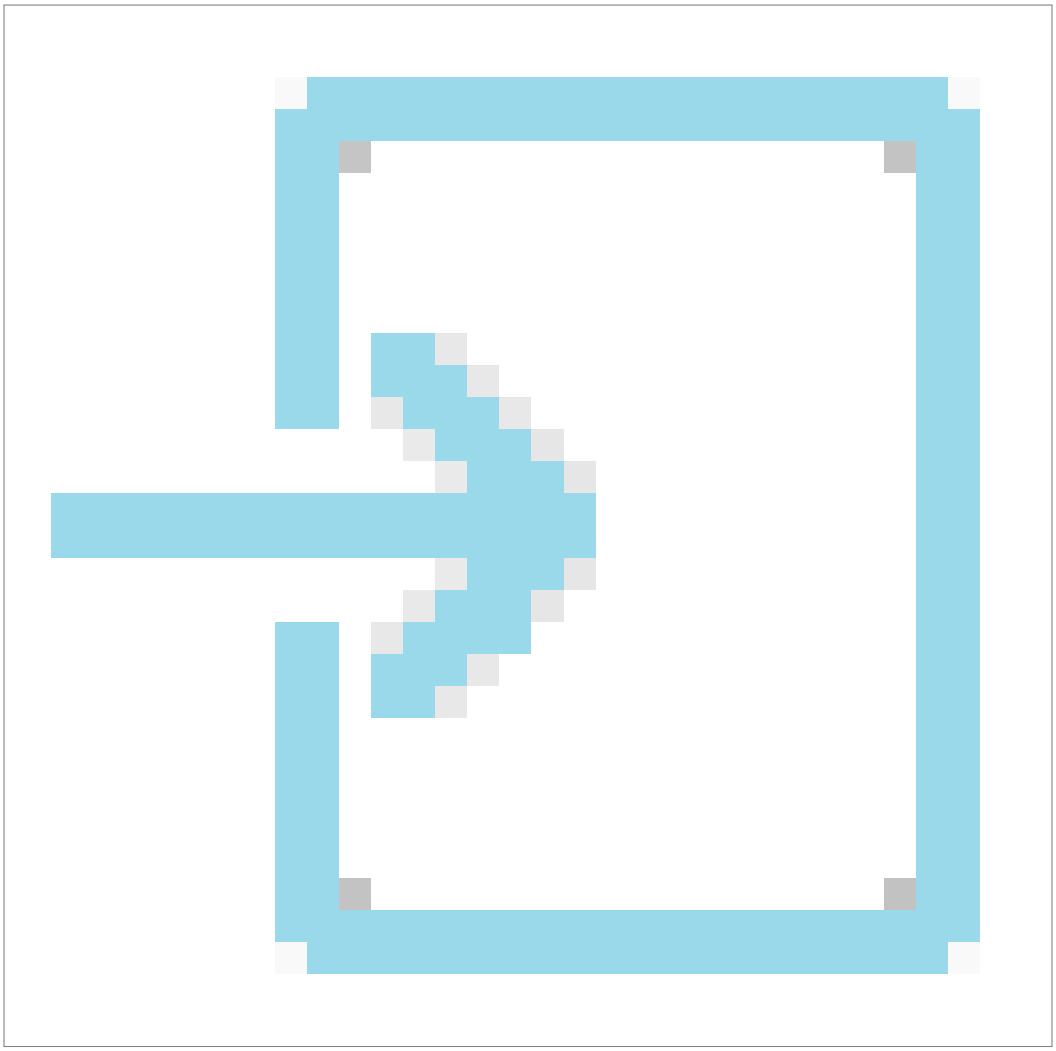
Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: TSO

9.4 Absatz 4

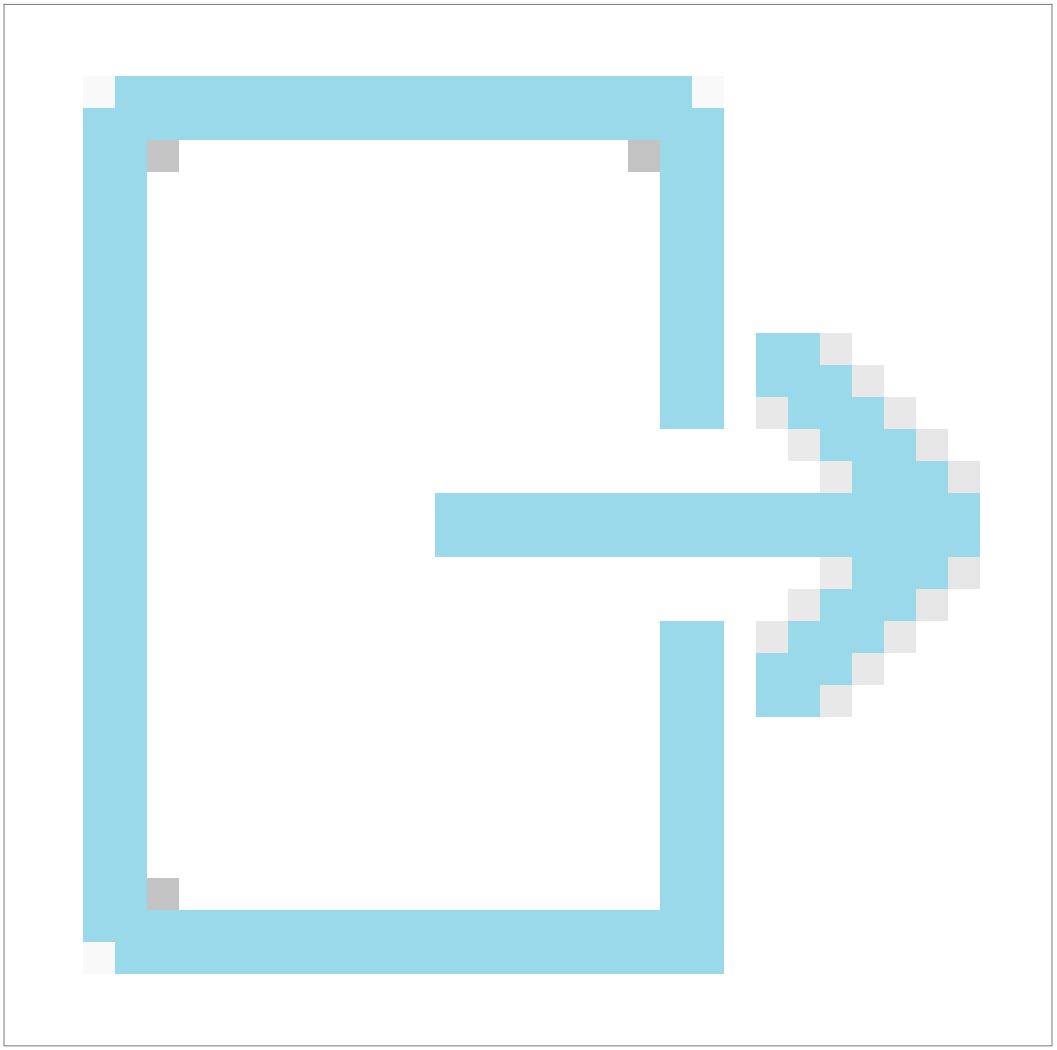
Eine Sperrminorität für Entscheidungen über Vorschläge für die Pläne muss eine Mindestanzahl von ÜNB umfassen, die mehr als 35 % der Bevölkerung der teilnehmenden Mitgliedstaaten vertreten, zuzüglich ÜNB, die mindestens einen weiteren betroffenen Mitgliedstaat vertreten; ansonsten gilt die qualifizierte Mehrheit als erreicht.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)



Output

- Entscheidung über Vorschläge

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

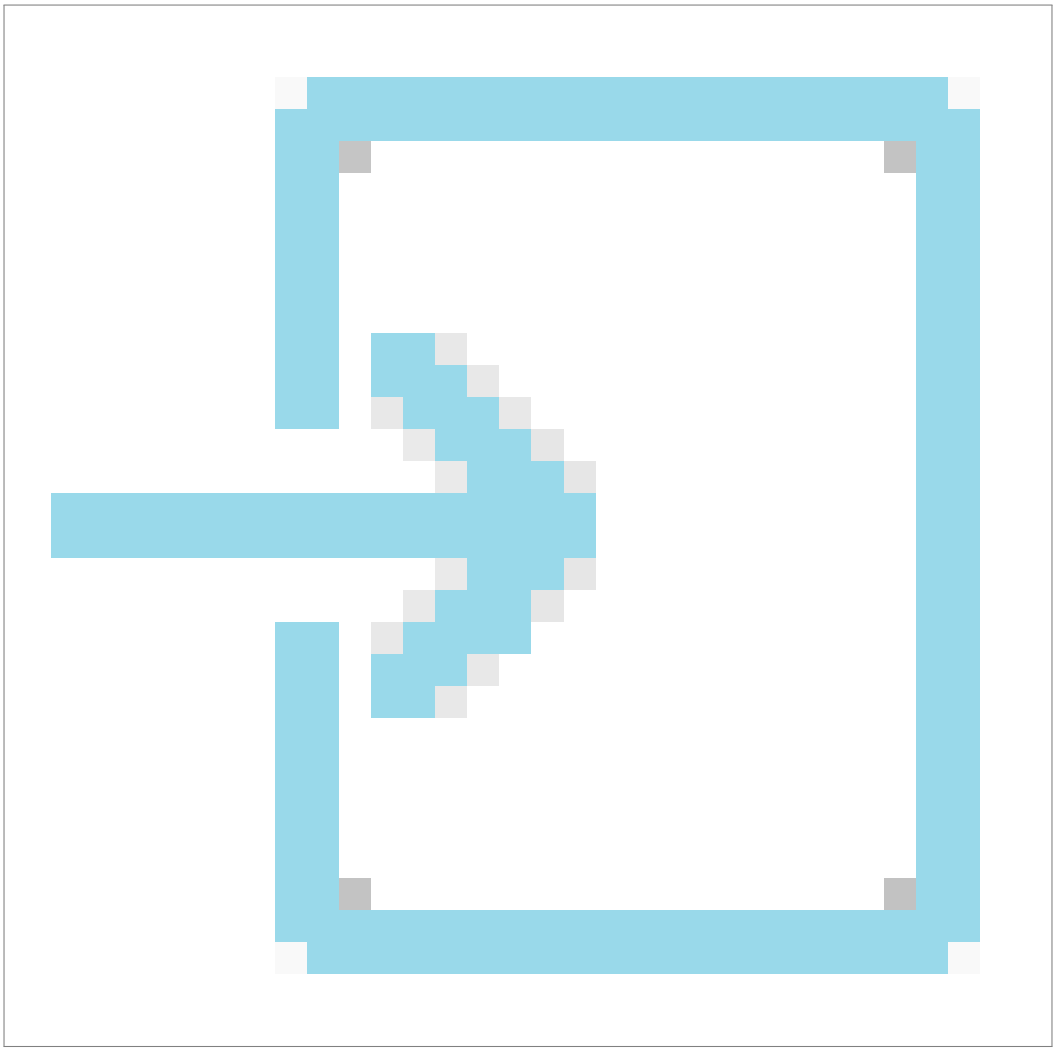
Beteiligt an der Aufgabenausführung: TSO

9.5 Absatz 5

Bei Entscheidungen der ÜNB über Vorschläge für in Artikel 6 Absatz 2 aufgeführte Modalitäten oder Methoden erhält jeder Mitgliedstaat eine Stimme. Gibt es im Hoheitsgebiet eines Mitgliedstaats mehr als einen ÜNB, teilt der Mitgliedstaat die Stimmrechte unter den ÜNB auf.

Relevante NCCS-Artikel

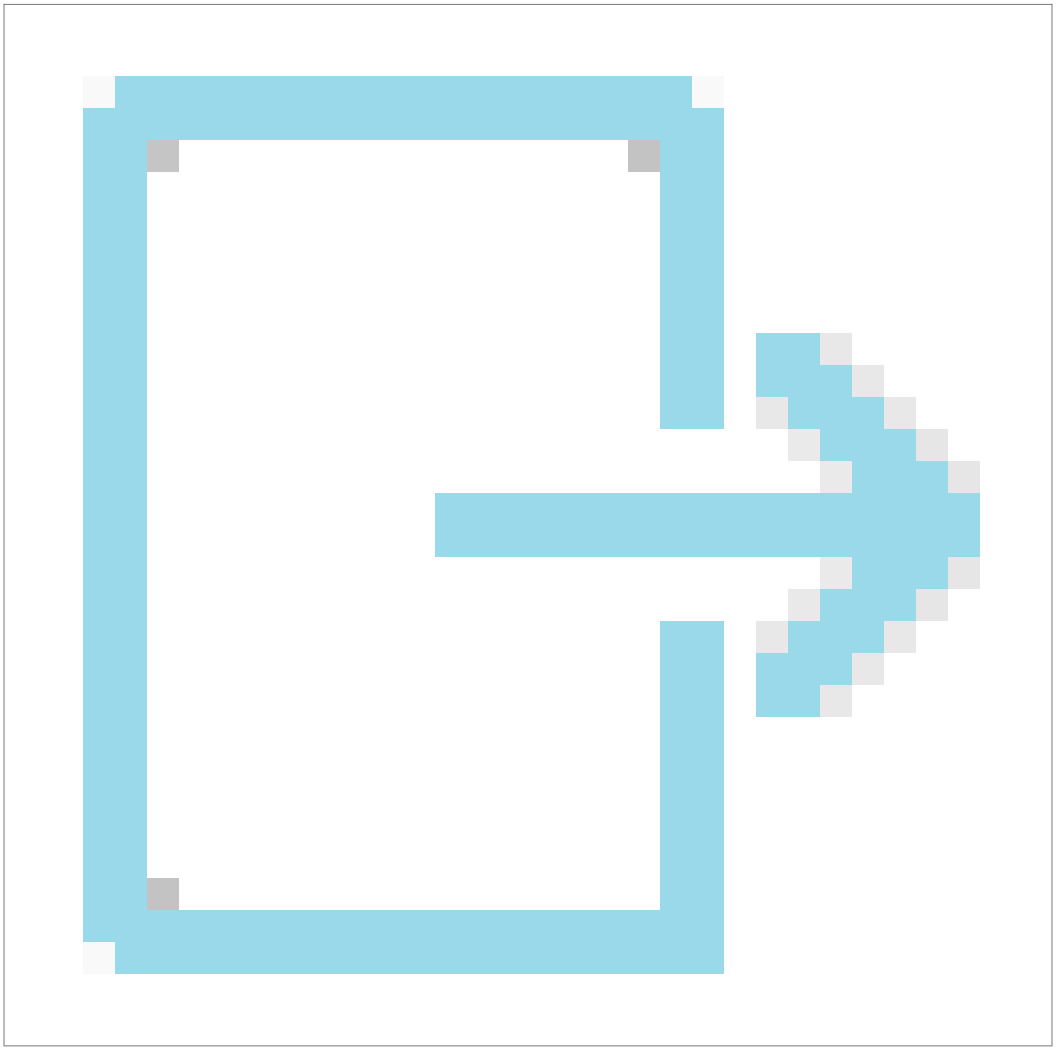
- Artikel 6 (2)



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)



Output

- Entscheidung über Vorschläge

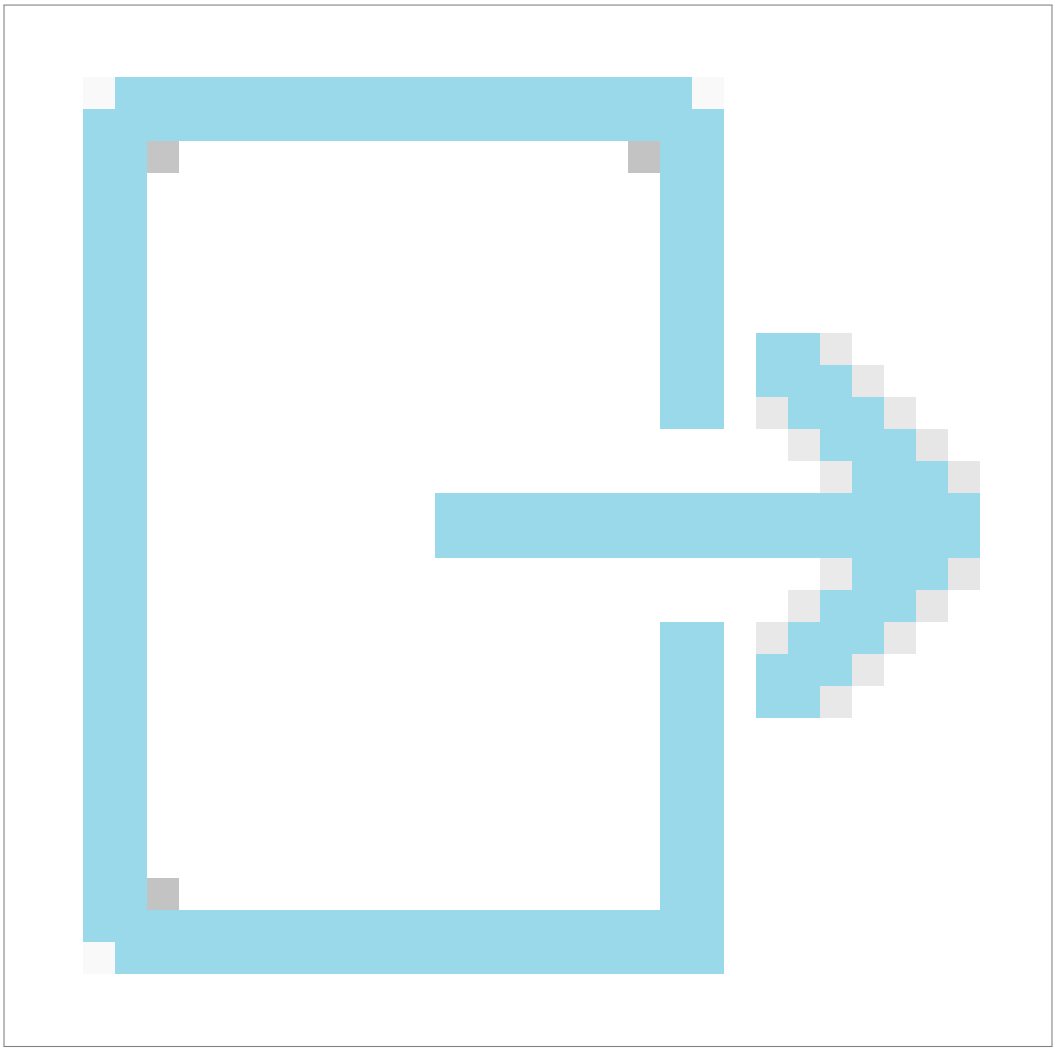
Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: TSO

9.6 Absatz 6

Legen ÜNB den jeweils zuständigen Behörden nicht innerhalb der in dieser Verordnung festgelegten Fristen in Zusammenarbeit mit der EU-VNBO einen ersten oder geänderten Vorschlag für Modalitäten oder Methoden oder für Pläne vor, so übermitteln sie den jeweils zuständigen Behörden und der ACER entsprechende Entwürfe der Modalitäten oder Methoden bzw. der Pläne. Sie erläutern, warum keine Einigung erzielt wurde.



Output

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Erläuterung

Verantwortlich für die Aktivität: TSO

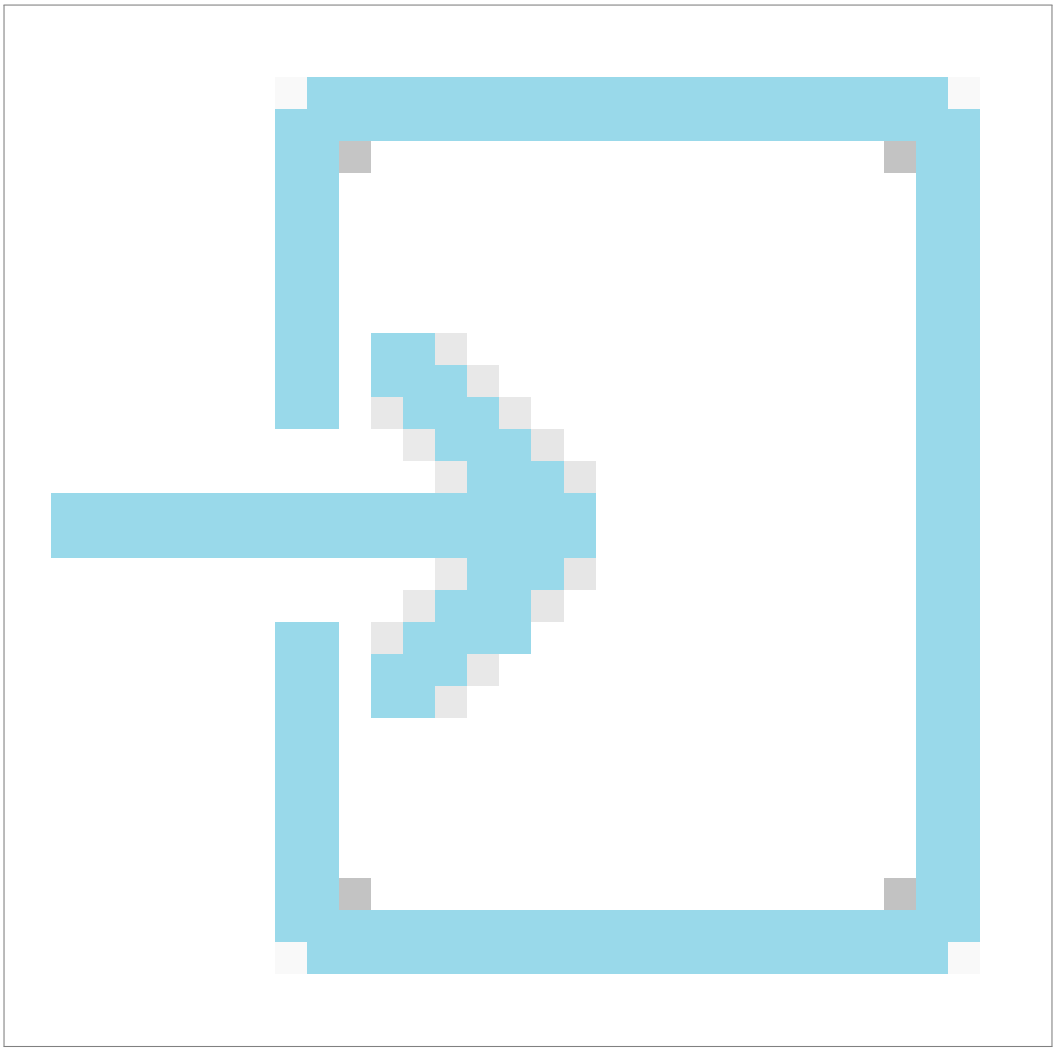
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu informieren: ACER, NCA

9.7 Absatz 6

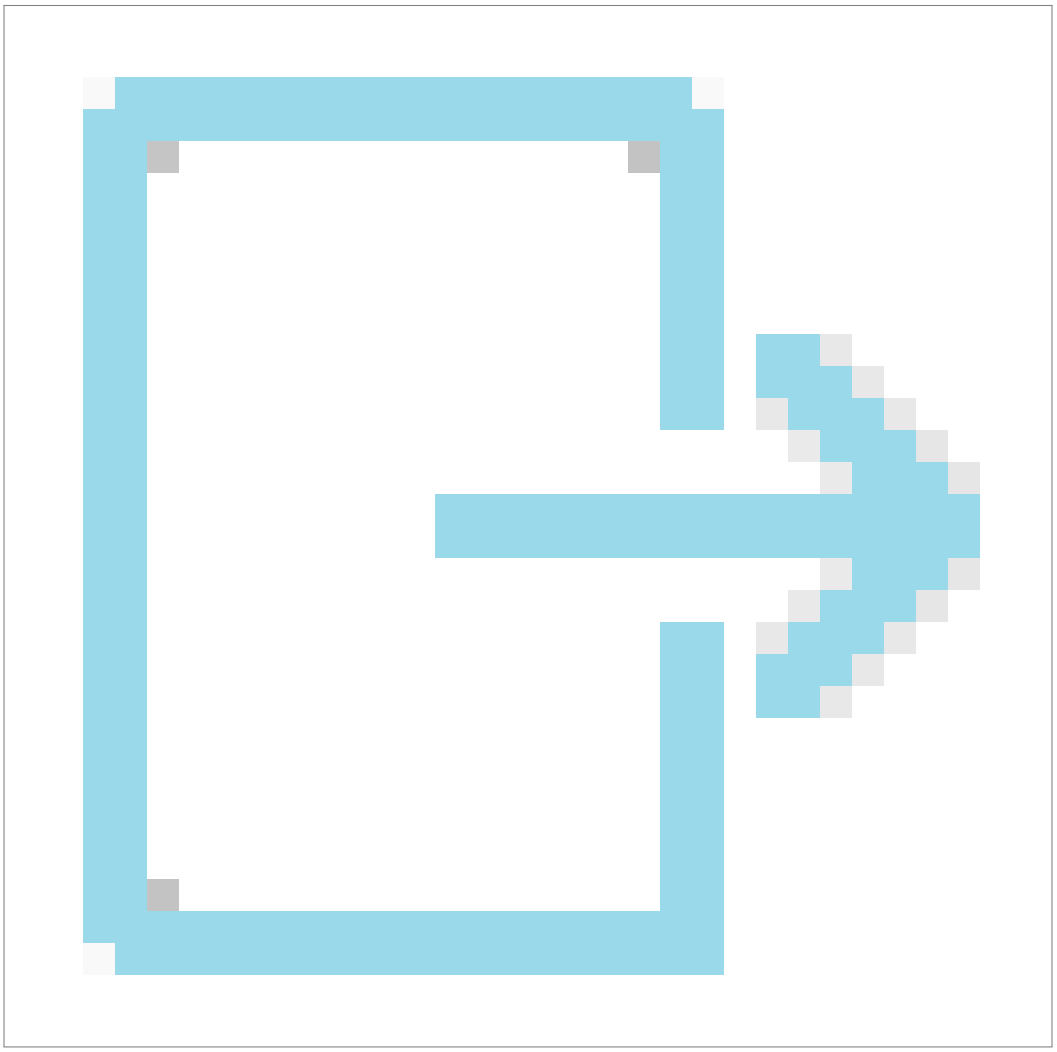
Die zuständigen Behörden treffen gemeinsam geeignete Maßnahmen für die Annahme der erforderlichen Modalitäten oder Methoden bzw. der erforderlichen Pläne. Dies kann z. B. durch Ersuchen um Änderungen der Entwürfe gemäß diesem Absatz, durch Überarbeitung und Vervollständigung dieser Entwürfe oder, falls keine Entwürfe vorgelegt wurden, durch Festlegung und Genehmigung der erforderlichen Modalitäten, Methoden oder Pläne erfolgen.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Erläuterung



Output

- Methoden zur Risikobewertung (genehmigt)
- Umfassender Risikobewertungsbericht (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen (genehmigt)
- Erweiterte Cybersicherheitskontrollen (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (genehmigt)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (genehmigt)

- Zuordnungsmatrix (genehmigt)
- Empfehlungen für die Beschaffung (genehmigt)
- Methodik zur Klassifizierung von Cyberangriffen (genehmigt)

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu informieren: TSO, ACER

Chapter 10

Artikel 8. : Einreichung von Vorschlägen bei den zuständigen Behörden

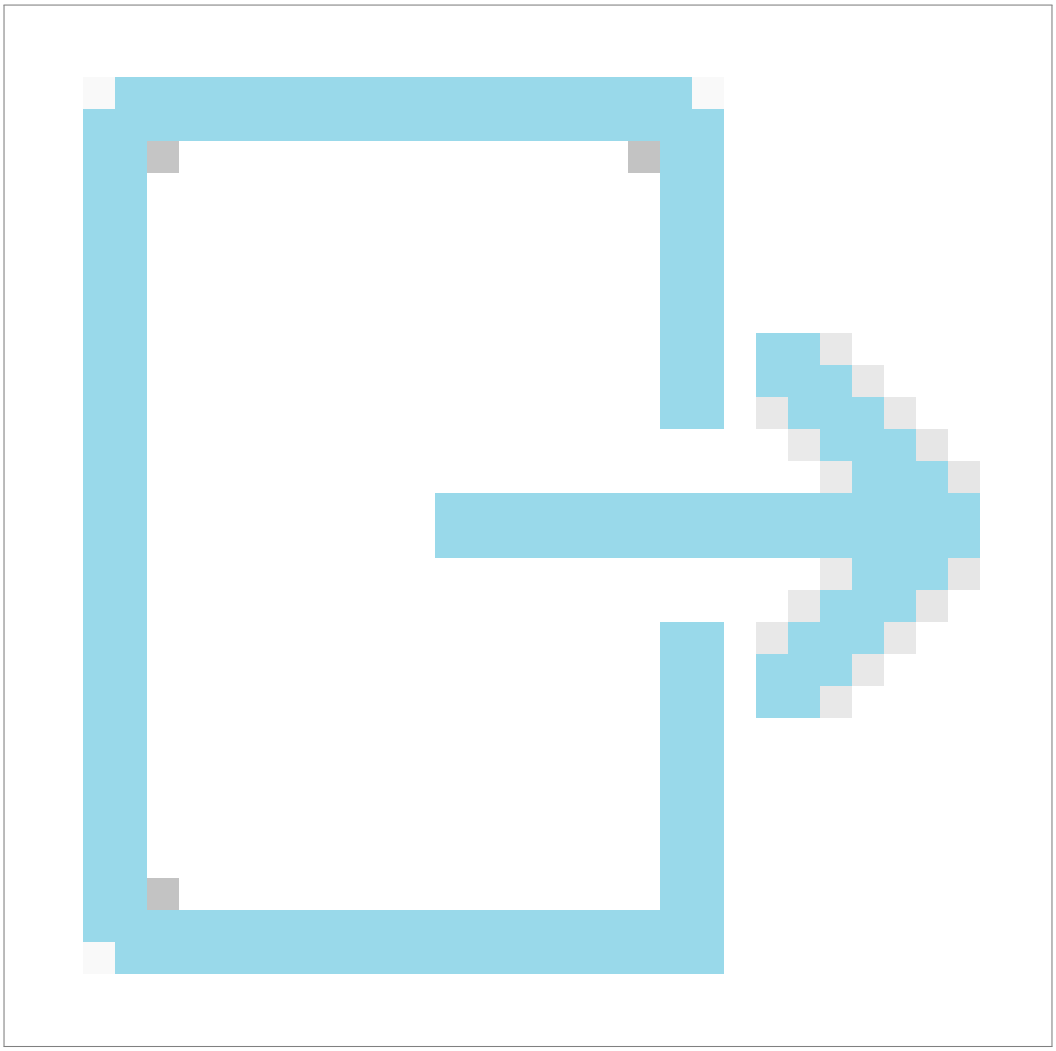
10.1 Absatz 1

Die ÜNB legen den jeweils zuständigen Behörden innerhalb der in den Artikeln 18, 23, 29, 33, 34, 35 und 37 festgelegten Fristen die Vorschläge für Modalitäten oder Methoden bzw. für Pläne zur Genehmigung vor.

Relevante NCCS-Artikel

- Artikel 18 (1)
- Artikel 23
- Artikel 29
- Artikel 34
- Artikel 33
- Artikel 35

- Artikel 37 (8)



Output

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)

- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)
- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Erläuterung

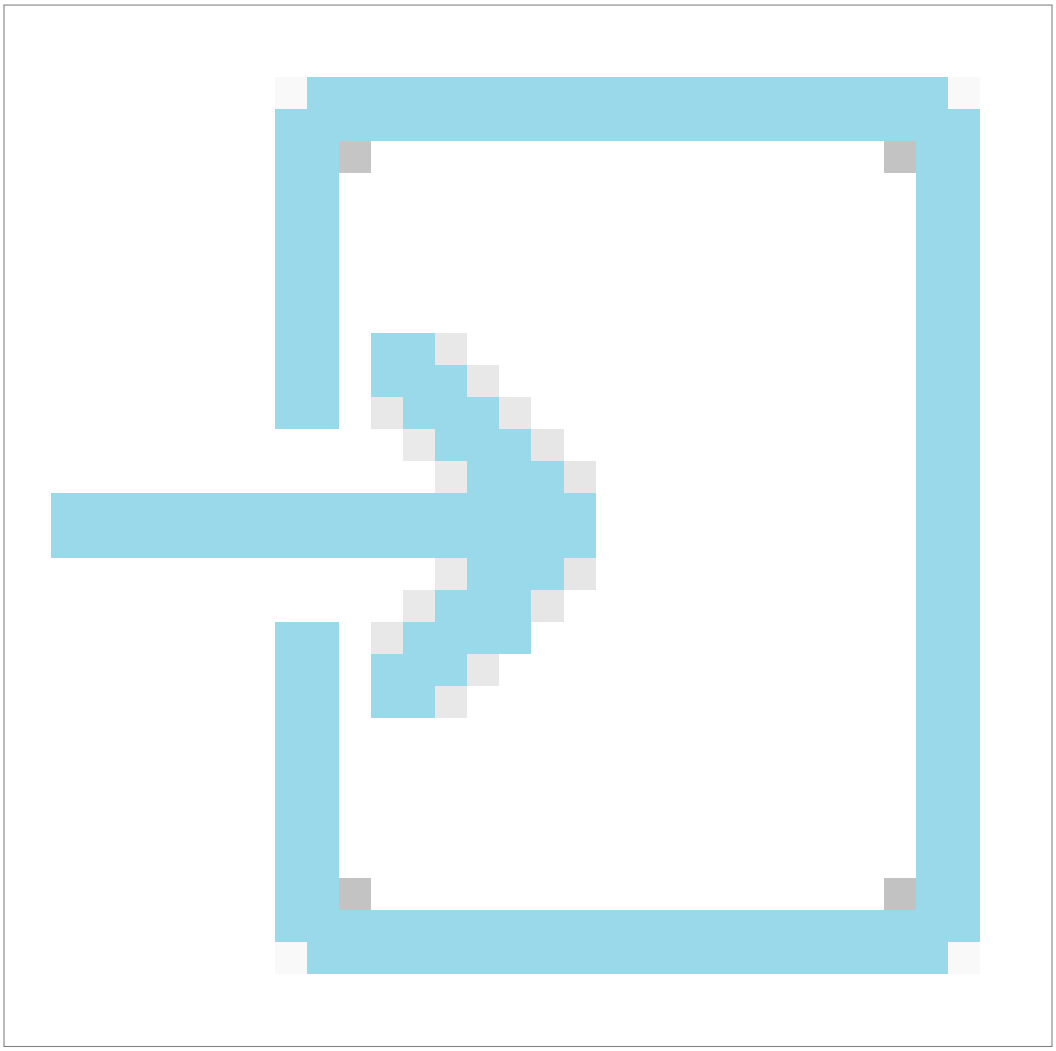
Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: TSO, NCA

10.2 Absatz 1

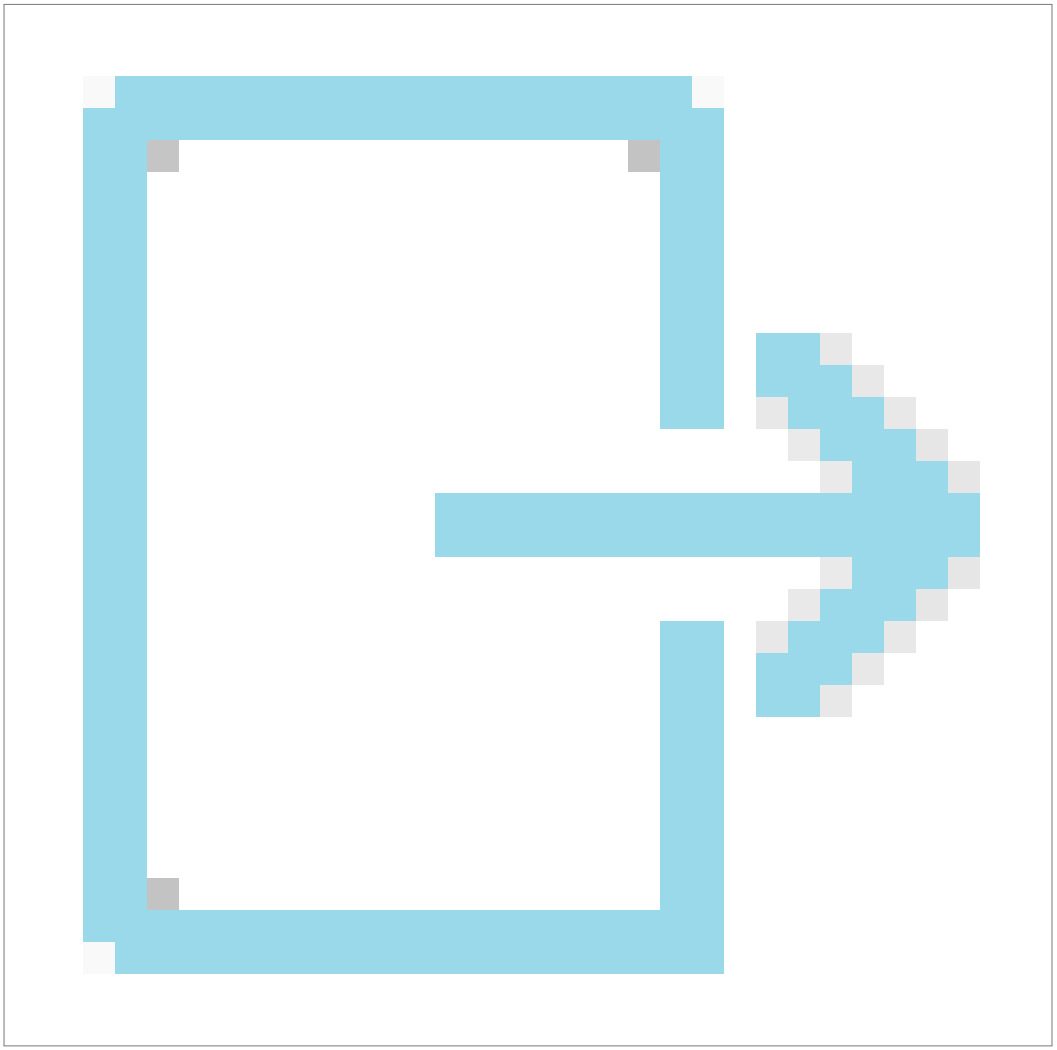
Die zuständigen Behörden können diese Fristen in Ausnahmefällen gemeinsam verlängern, insbesondere wenn eine Frist aufgrund von Umständen außerhalb des Verantwortungsbereichs der ÜNB oder der EU-VNBO nicht eingehalten werden kann.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)



Output

- Verlängerung

A

Verantwortlich für die Aktivität: NCA

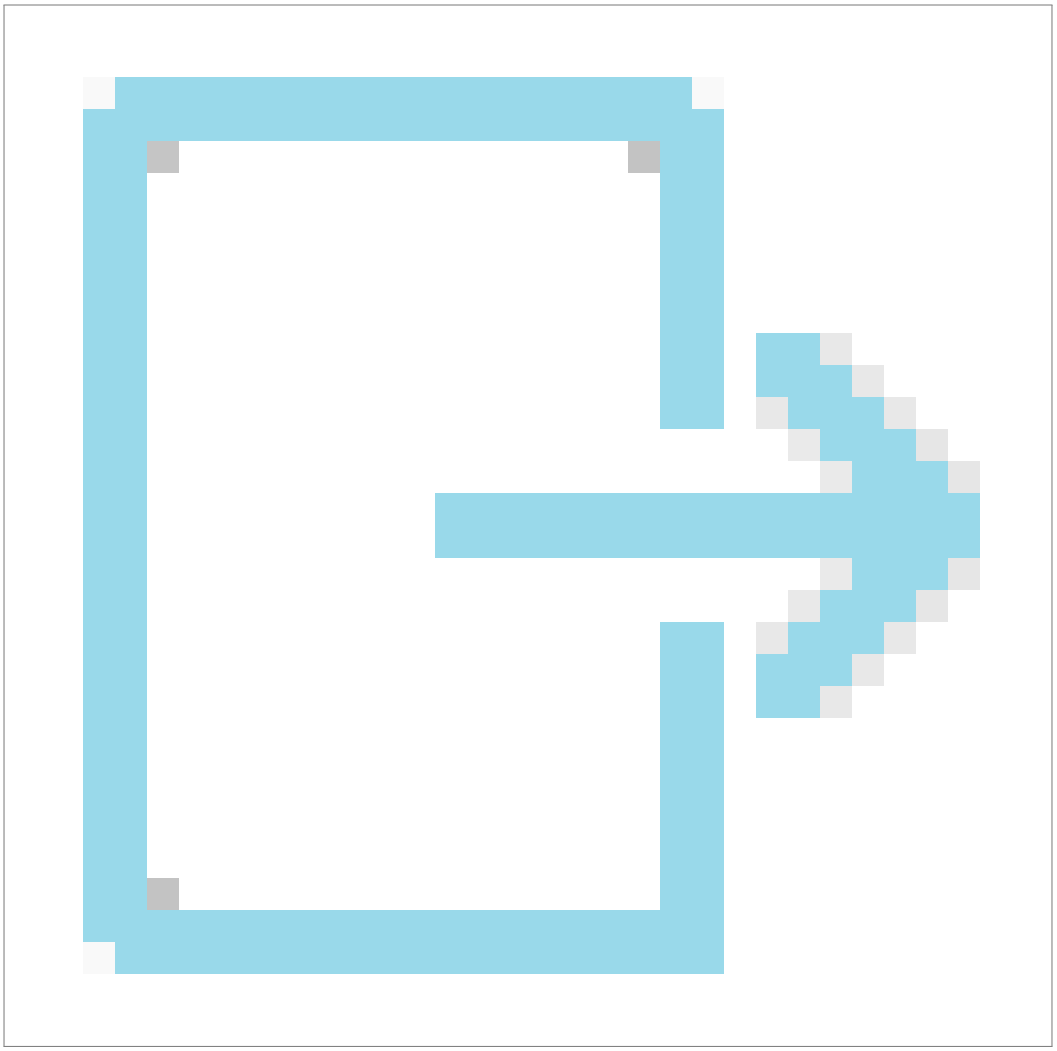
Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: NCA

10.3 Absatz 2

Vorschläge für Modalitäten, Methoden oder bzw. Pläne gemäß Absatz 1 werden zeitgleich mit der Übermittlung an die zuständigen Behörden auch der ACER zur Information vorgelegt.



Output

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)
- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)

Verantwortlich für die Aktivität: TSO

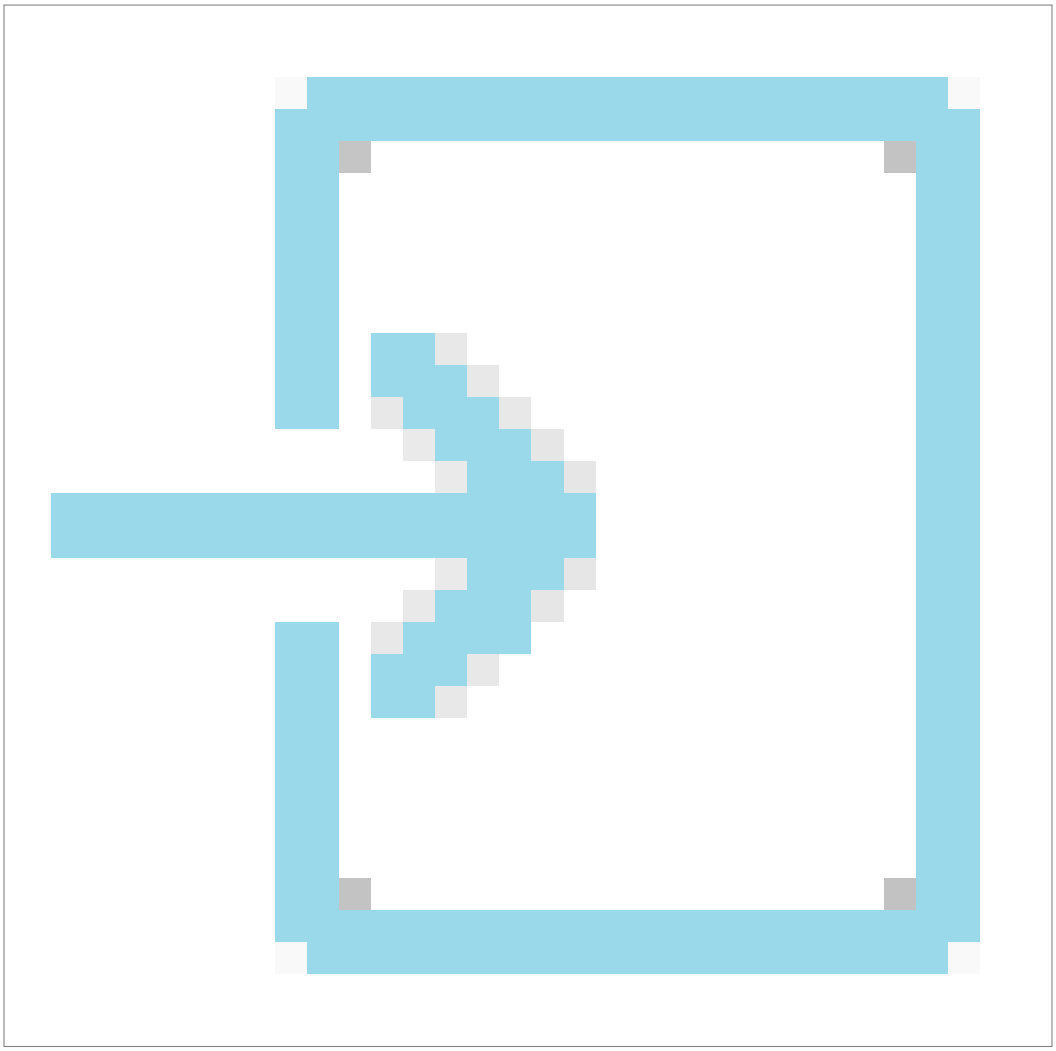
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: TSO

Zu informieren: ACER

10.4 Absatz 3

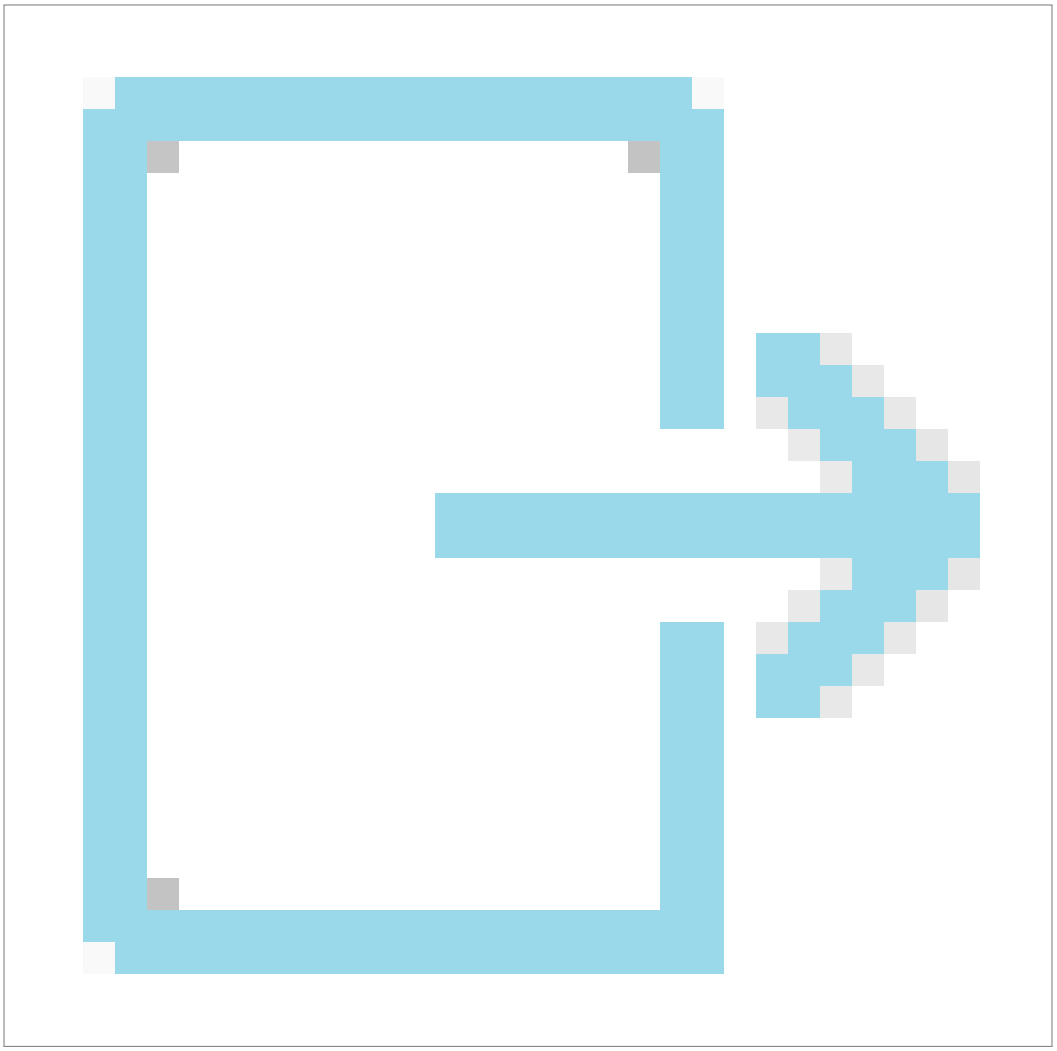
Auf gemeinsames Ersuchen der NRB gibt die ACER innerhalb von sechs Monaten nach Eingang des Vorschlags für Modalitäten oder Methoden oder für die Pläne eine Stellungnahme zu dem Vorschlag ab und übermittelt sie den NRB und den zuständigen Behörden.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Stellungnahme angefordert



Output

- Stellungnahme der ACER

GOOD TO KNOW

Zeitpunkt

> Innerhalb von 6 Monaten nach Erhalt der Empfehlungen zu Bedingungen oder Methoden sowie Plänen

Verantwortlich für die Aktivität: ACER

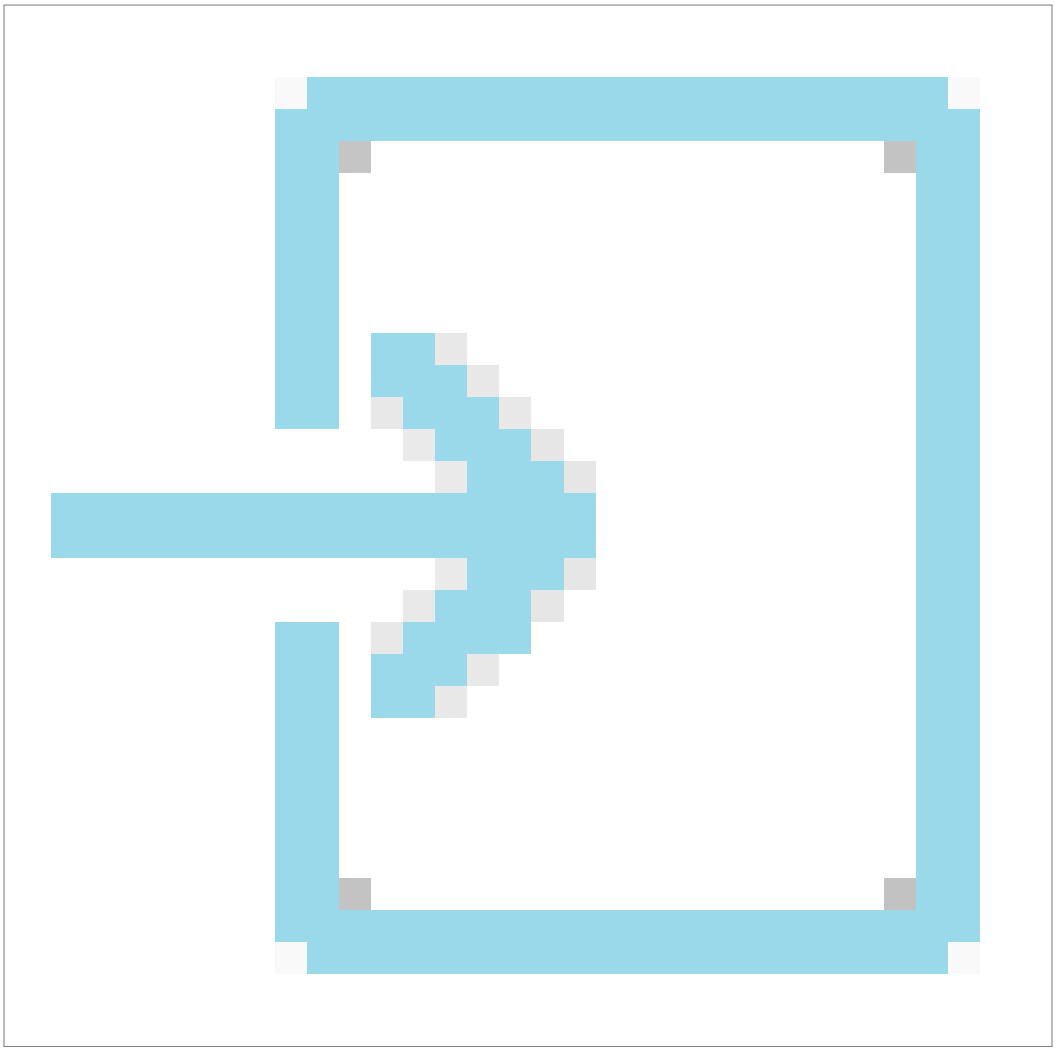
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ACER

Zu informieren: NCA, NRA

10.5 Absatz 3

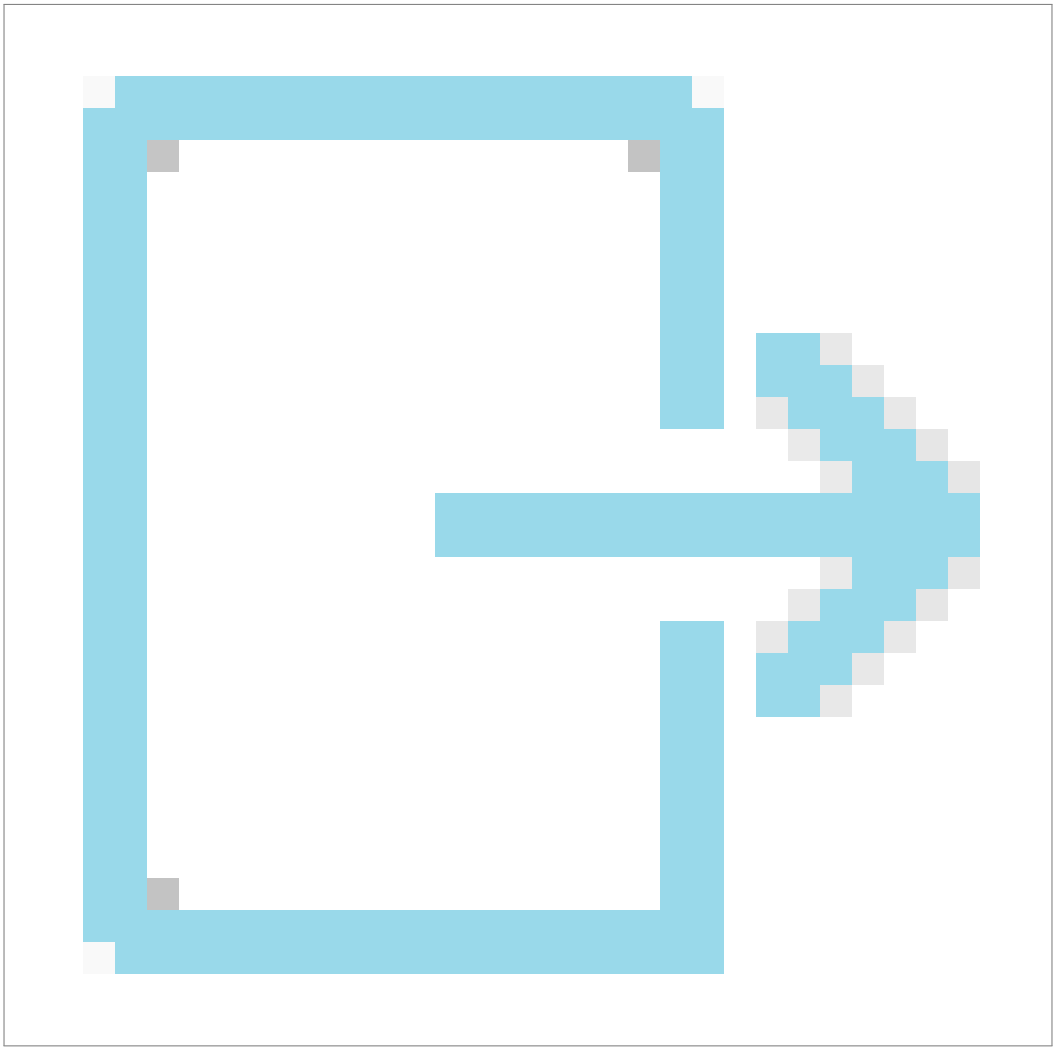
Die NRB, die CS-NCA und alle anderen als zuständige Behörden benannten Behörden stimmen sich untereinander ab, bevor die NRB die ACER um eine Stellungnahme ersuchen. Die ACER kann in dieser Stellungnahme Empfehlungen abgeben.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)



Output

- Stellungnahmeersuchen an ACER

Verantwortlich für die Aktivität: NRA

Beteiligte Stakeholder:

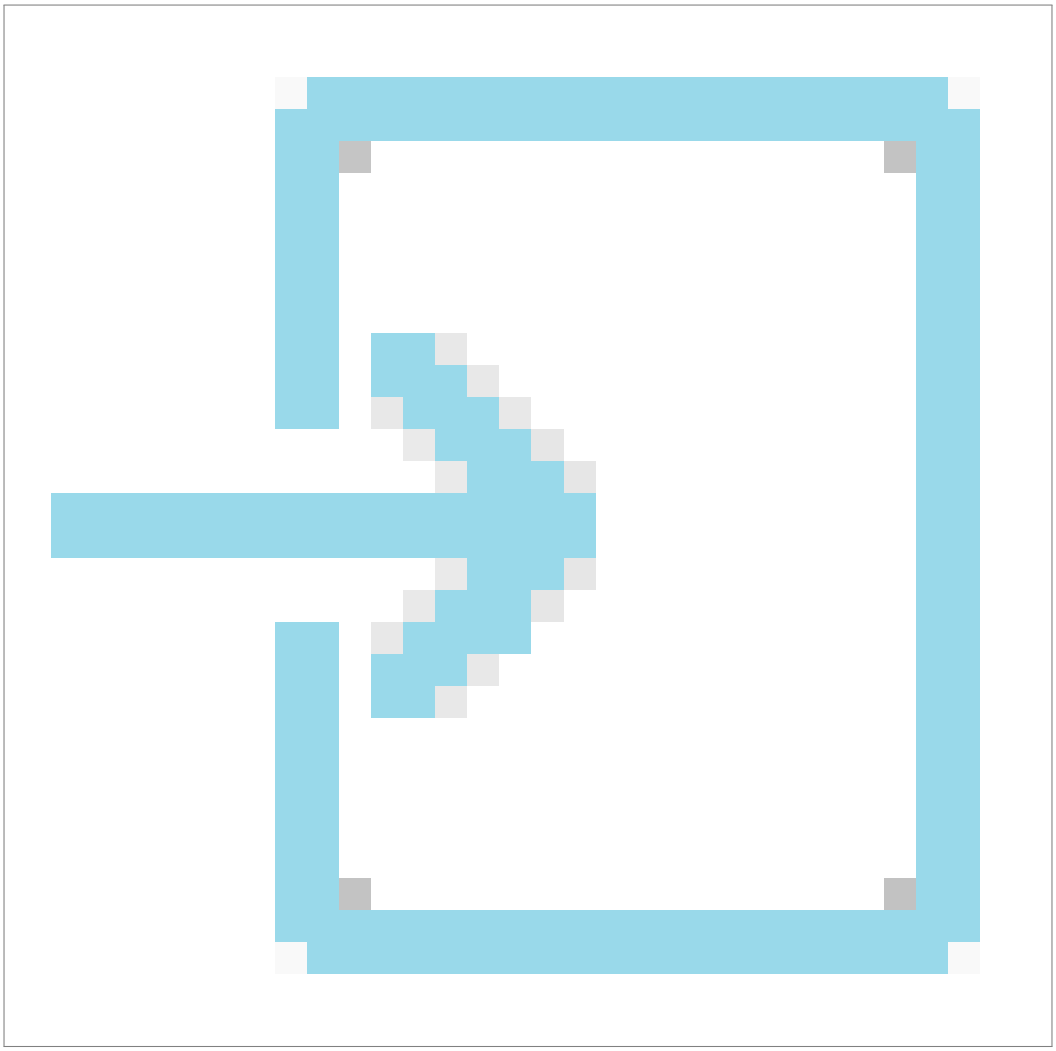
Beteiligt an der Aufgabenausführung: ACER, NCA, NRA, CS NCA

10.6 Absatz 3

Die ACER konsultiert die ENISA, bevor sie eine Stellungnahme zu den in Artikel 6 Absatz 2 aufgeführten Vorschlägen abgibt.

Relevante NCCS-Artikel

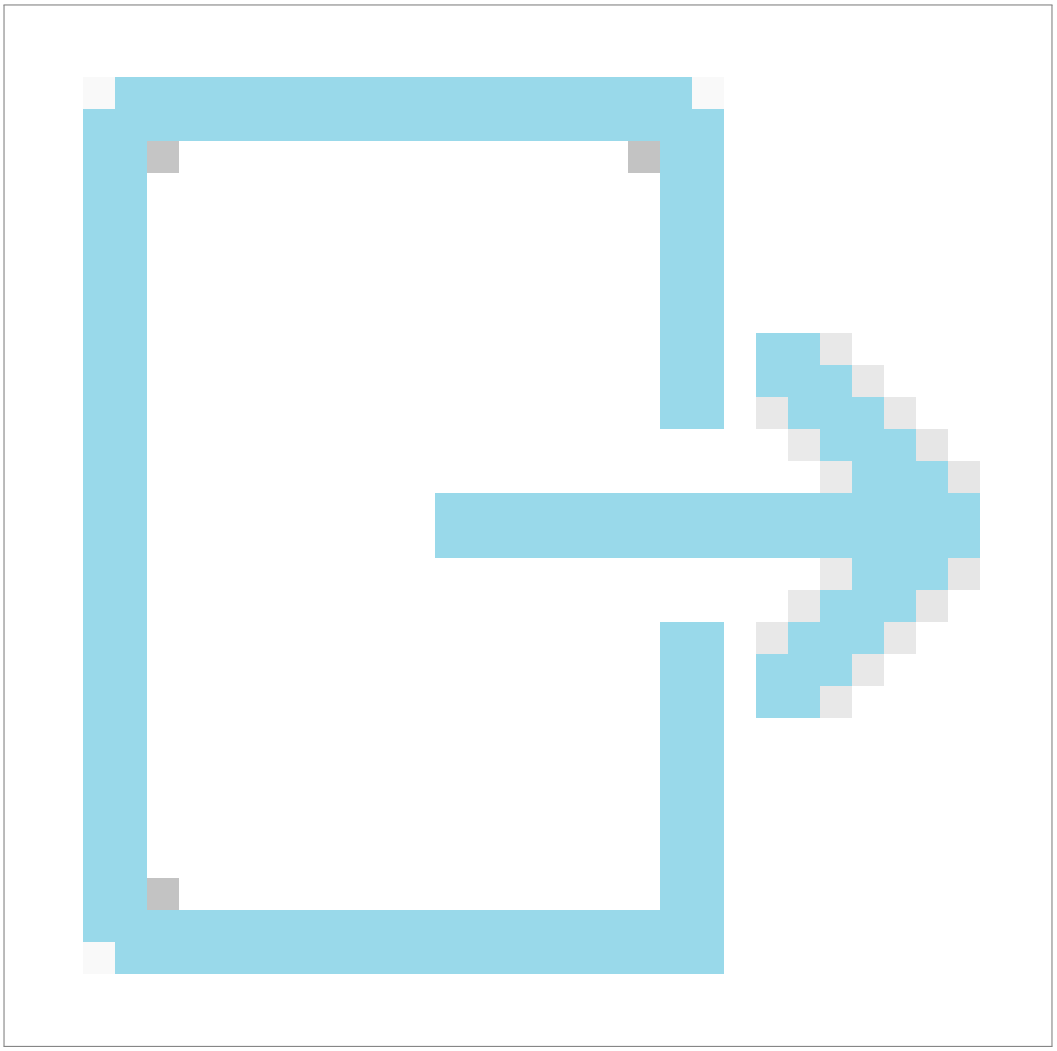
- Artikel 6 (2)



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Stellungnahme angefordert



Output

- Stellungnahme der ACER

GOOD TO KNOW

Zeitpunkt

> innerhalb von 6 Monaten

Verantwortlich für die Aktivität: ACER

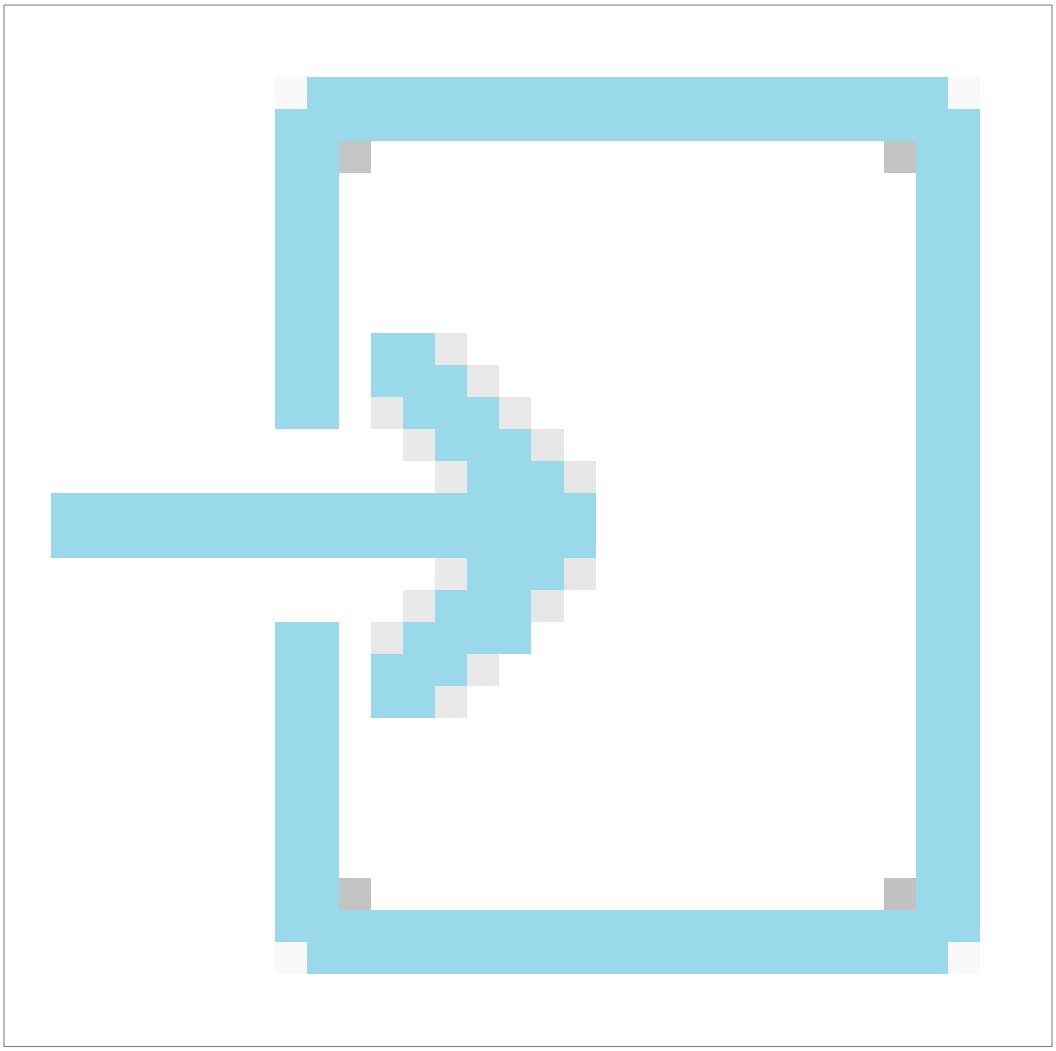
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ACER

Zu konsultieren: ENISA

10.7 Absatz 4

Die zuständigen Behörden konsultieren einander, arbeiten eng zusammen und stimmen sich untereinander ab, um zu einer Einigung über die vorgeschlagenen Modalitäten, Methoden oder Pläne zu gelangen. Vor der Genehmigung der Modalitäten oder Methoden oder der Pläne überarbeiten und ergänzen sie die Vorschläge nach Konsultation von ENTSO-E und der EU-VNBO erforderlichenfalls, um sicherzustellen, dass die Vorschläge mit dieser Verordnung im Einklang stehen und zu einem hohen gemeinsamen Cybersicherheitsniveau in der gesamten Union beitragen.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)

Verantwortlich für die Aktivität: NCA

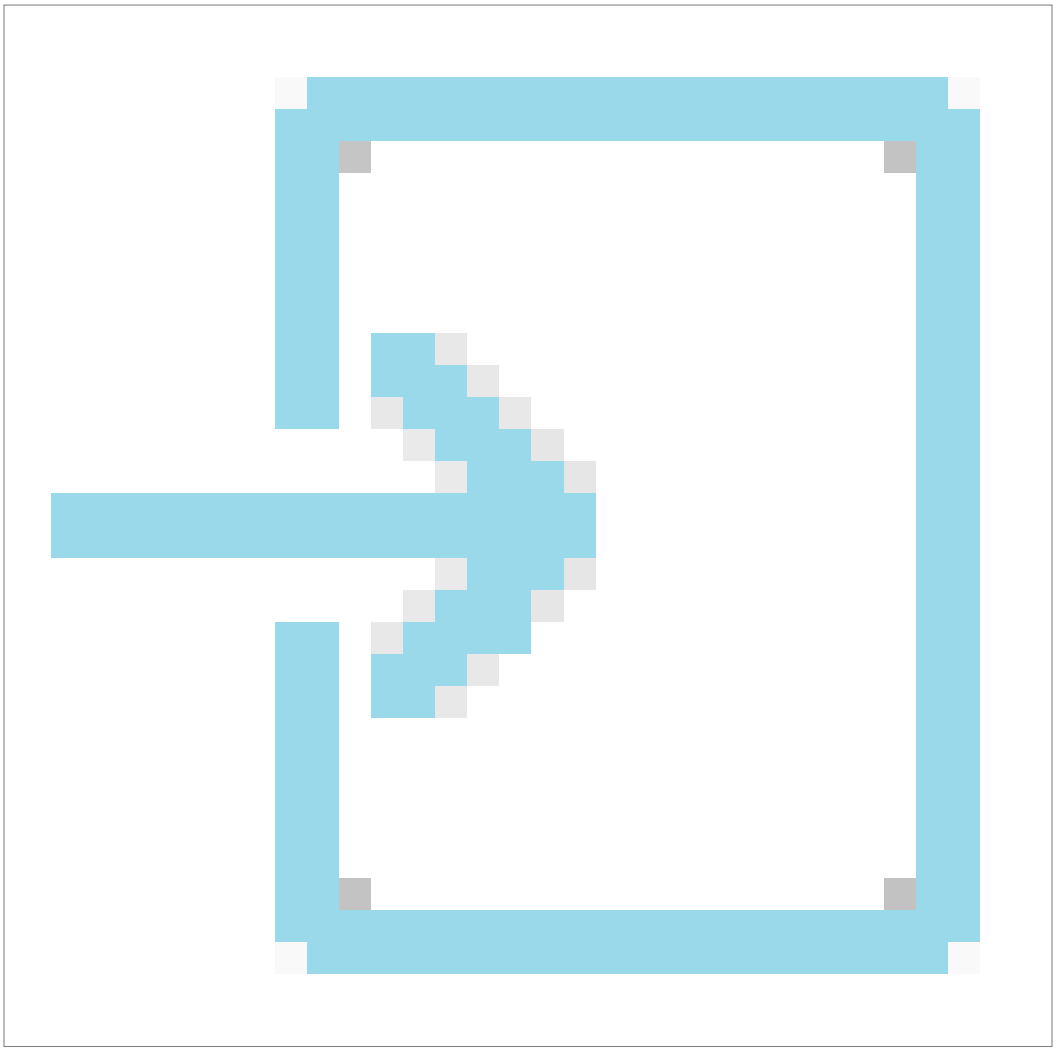
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu konsultieren: ENTSO-E, EU DSO

10.8 Absatz 5

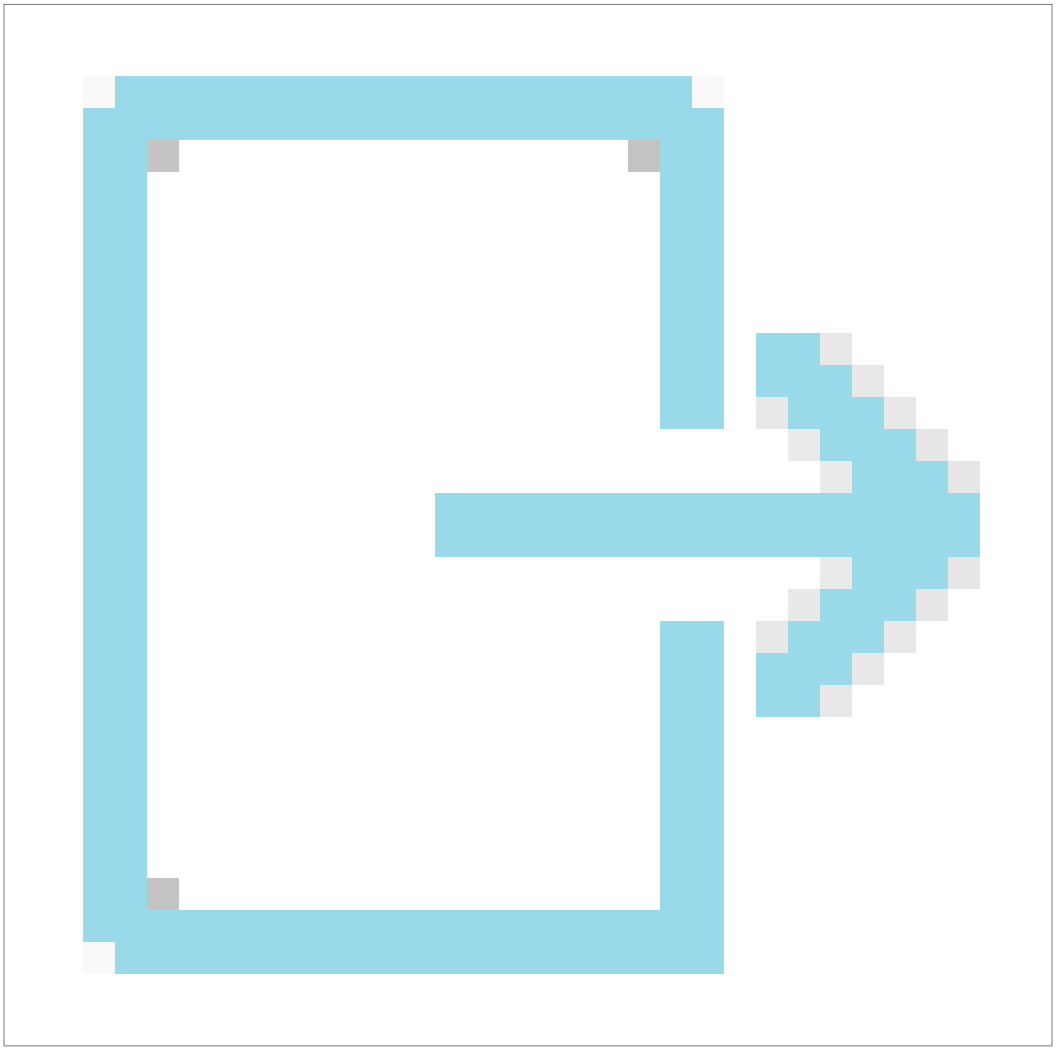
Die zuständigen Behörden entscheiden über die Modalitäten oder Methoden oder die Pläne innerhalb von sechs Monaten nach Eingang der Modalitäten oder Methoden bzw. der Pläne bei der jeweils zuständigen Behörde oder gegebenenfalls bei der letzten betroffenen zuständigen Behörde.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)



Output

- Entscheidung

GOOD TO KNOW

Zeitpunkt

> Innerhalb von 6 Monaten nach Erhalt der Empfehlungen zu Bedingungen oder Methoden sowie Plänen

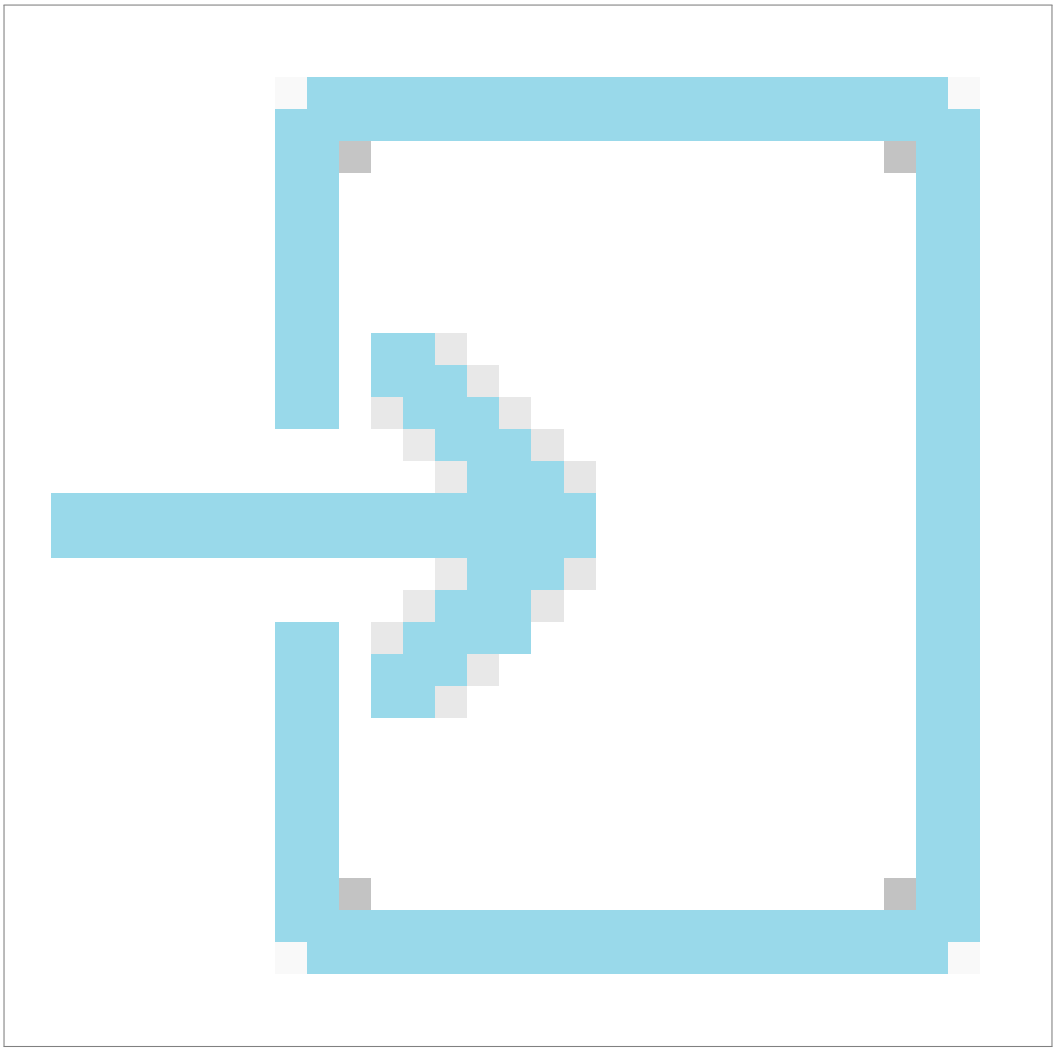
Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

10.9 Absatz 6

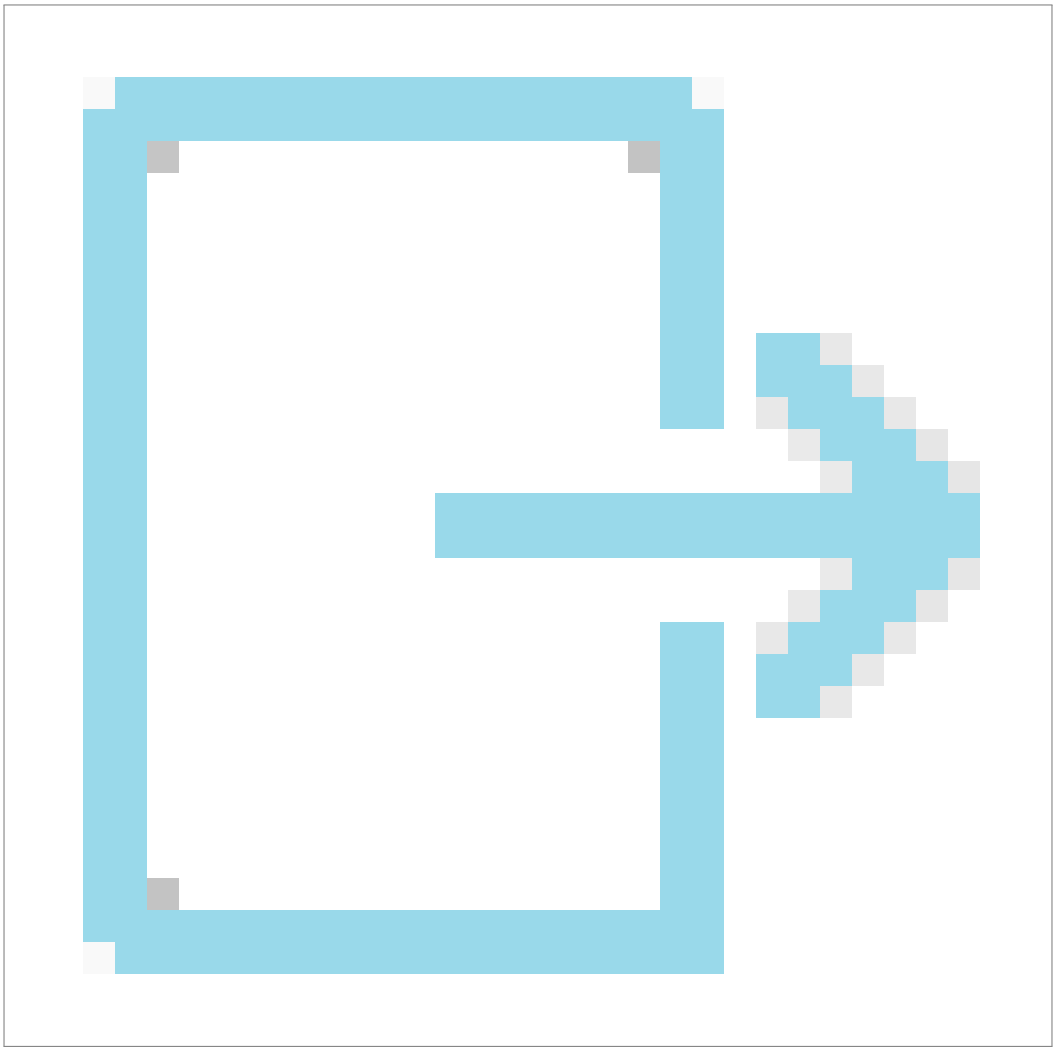
Gibt die ACER eine Stellungnahme ab, so tragen die jeweils zuständigen Behörden dieser Stellungnahme Rechnung und treffen ihre Entscheidungen innerhalb von sechs Monaten nach Eingang der Stellungnahme.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Stellungnahme von Acer



Output

- Entscheidung

GOOD TO KNOW

Zeitpunkt

> Innerhalb von 6 Monaten nach Erhalt der Stellungnahme der ACER

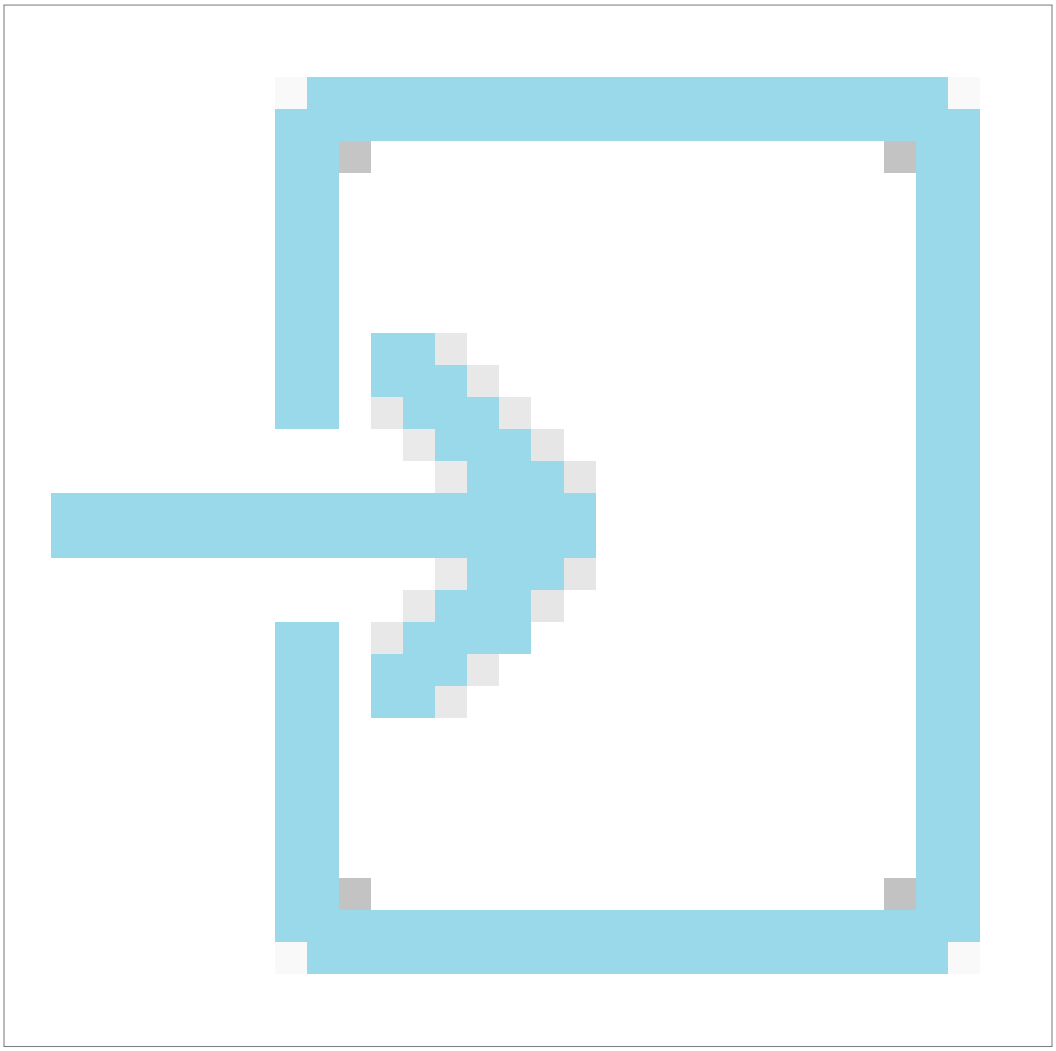
Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

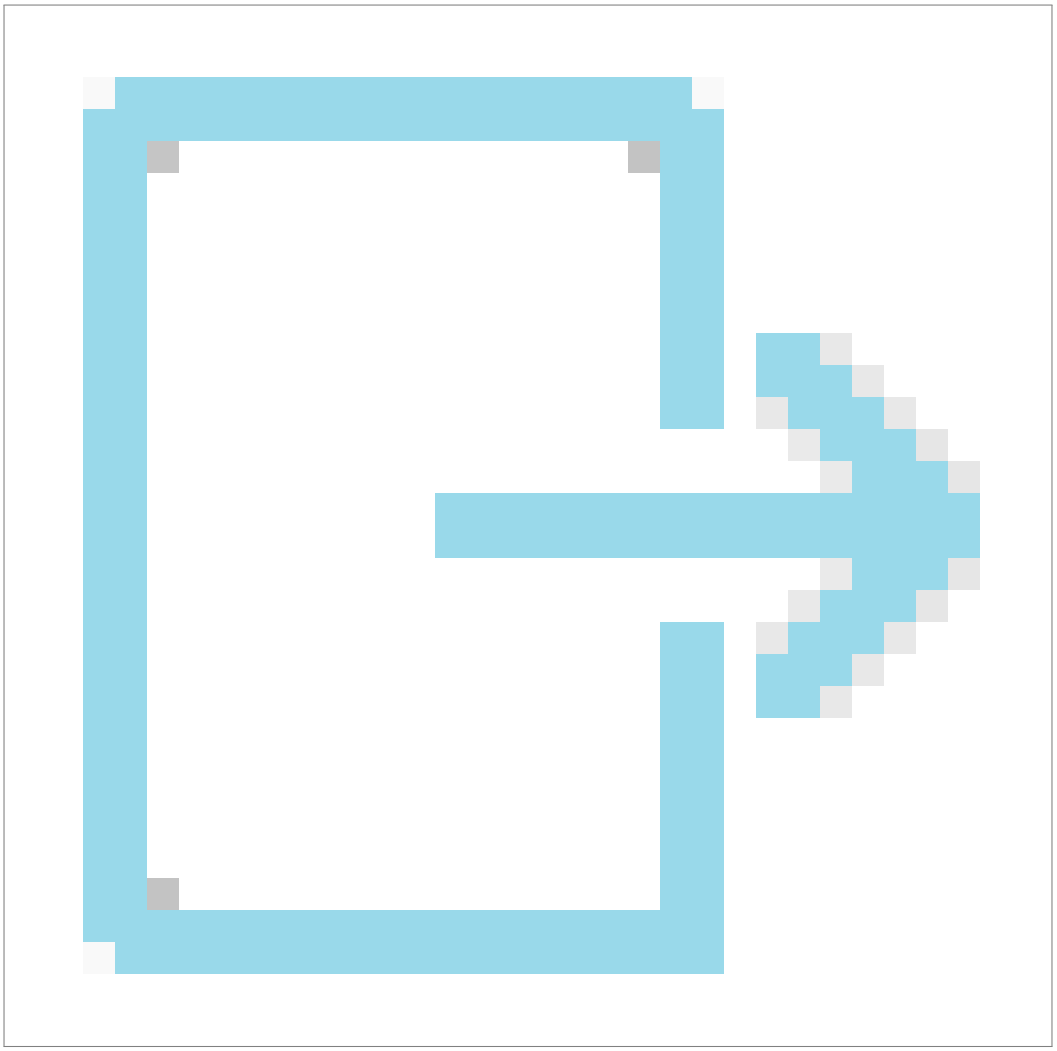
10.10 Absatz 7

Verlangen die zuständigen Behörden für ihre Genehmigung gemeinsam eine Änderung der vorgeschlagenen Modalitäten oder Methoden oder der Pläne, so entwickeln die ÜNB in Zusammenarbeit mit der EU-VNBO einen Vorschlag für eine solche Änderung der Modalitäten oder Methoden bzw. der Pläne. Die ÜNB legen den zuständigen Behörden den geänderten Vorschlag innerhalb von zwei Monaten nach deren Aufforderung zur Genehmigung vor.



Input

- Stellungnahme



Output

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Stellungnahme von Acer

> GOOD TO KNOW
>
> **Zeitpunkt**
>
> innerhalb von 2 Monaten nach der Anfrage

Verantwortlich für die Aktivität: TSO

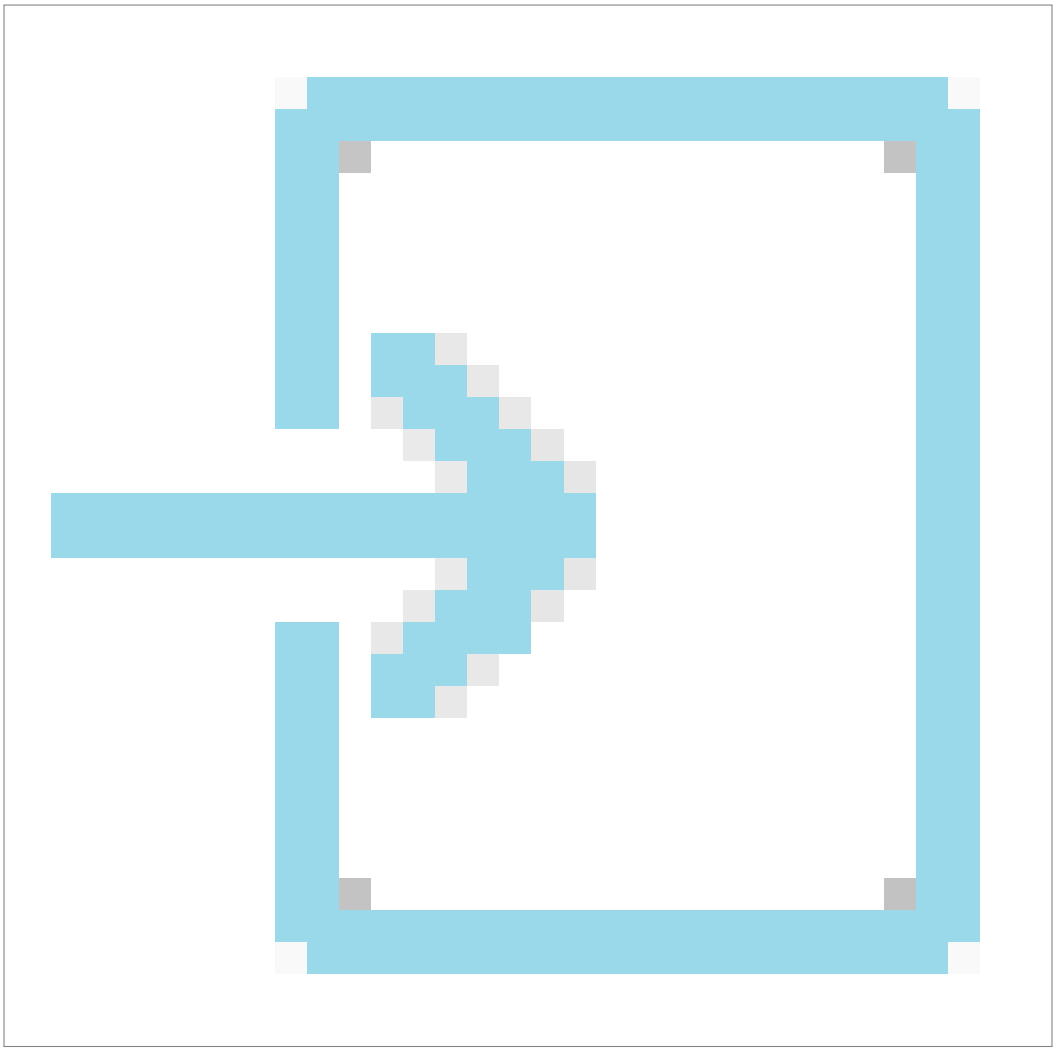
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu informieren: NCA

10.11 Absatz 7

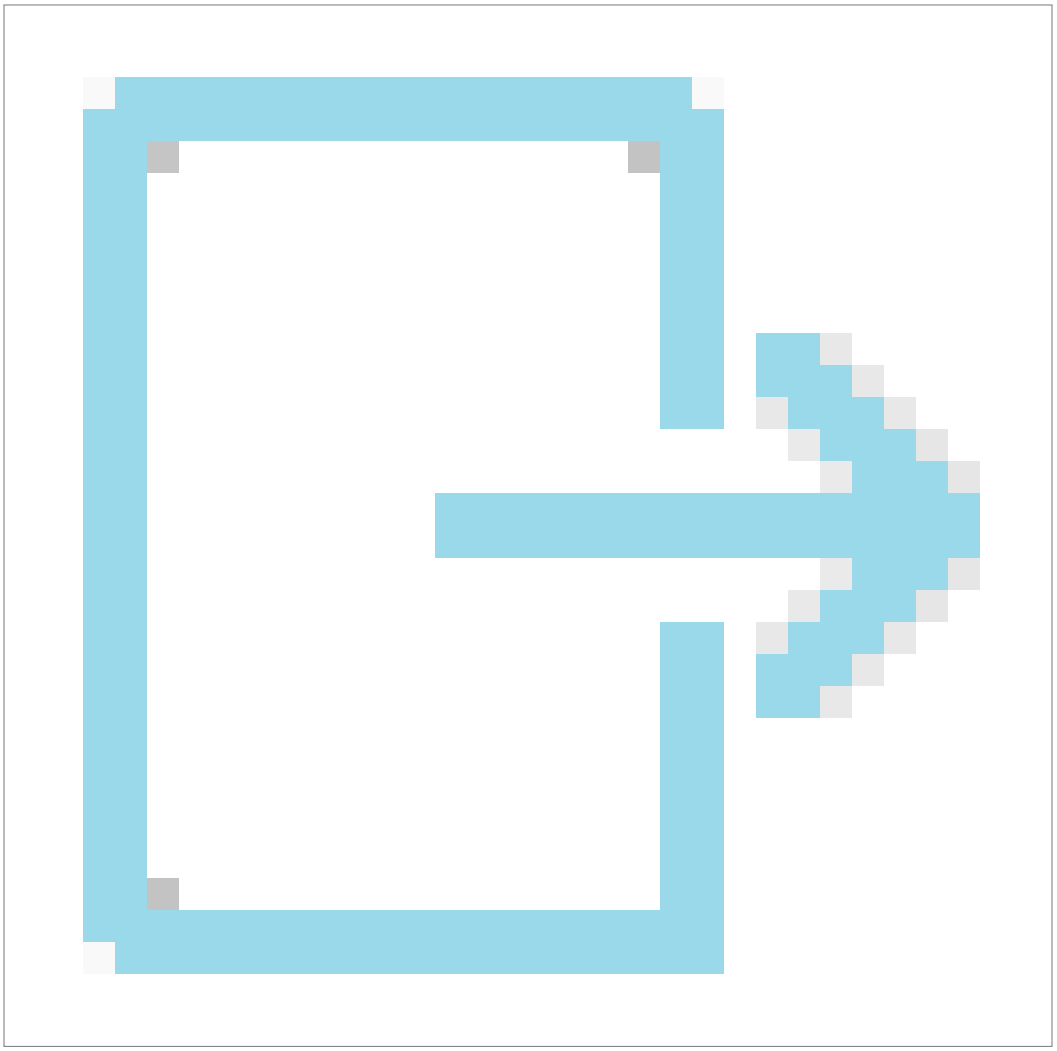
Die zuständigen Behörden entscheiden über die geänderten Modalitäten oder Methoden oder Pläne innerhalb von zwei Monaten nach deren Vorlage.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Stellungnahme von Acer



Output

- Entscheidung

GOOD TO KNOW

Zeitpunkt

> Innerhalb von 2 Monaten nach Einreichung

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

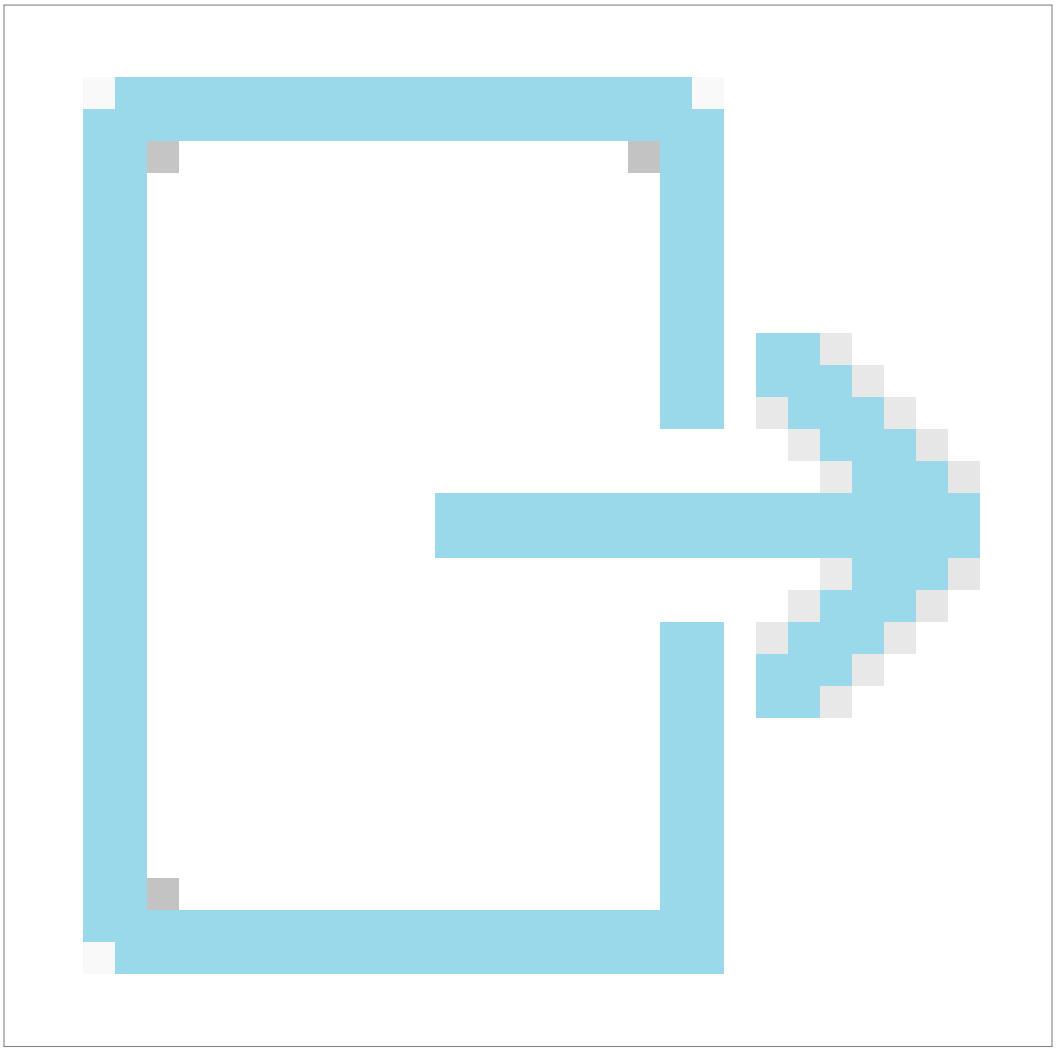
Beteiligt an der Aufgabenausführung: NCA

10.12 Absatz 8

Konnten die zuständigen Behörden innerhalb der in Absatz 5 oder Absatz 7 genannten Frist keine Einigung erzielen, so unterrichten sie die Kommission.

Relevante NCCS-Artikel

- Artikel 8 (5)
- Artikel 8 (7)



Output

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Stellungnahme von Acer
- Benachrichtigung

Verantwortlich für die Aktivität: NCA

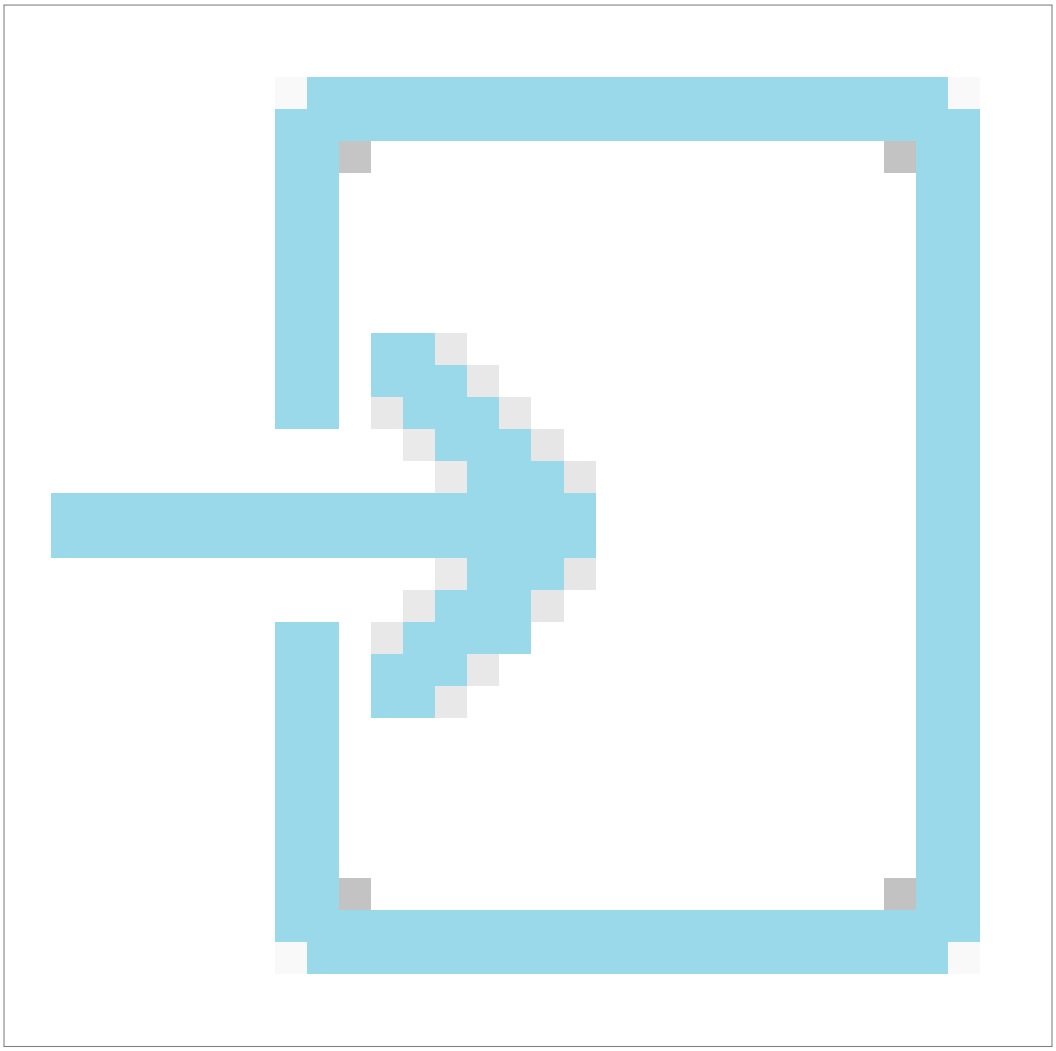
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu informieren: EC

10.13 Absatz 8

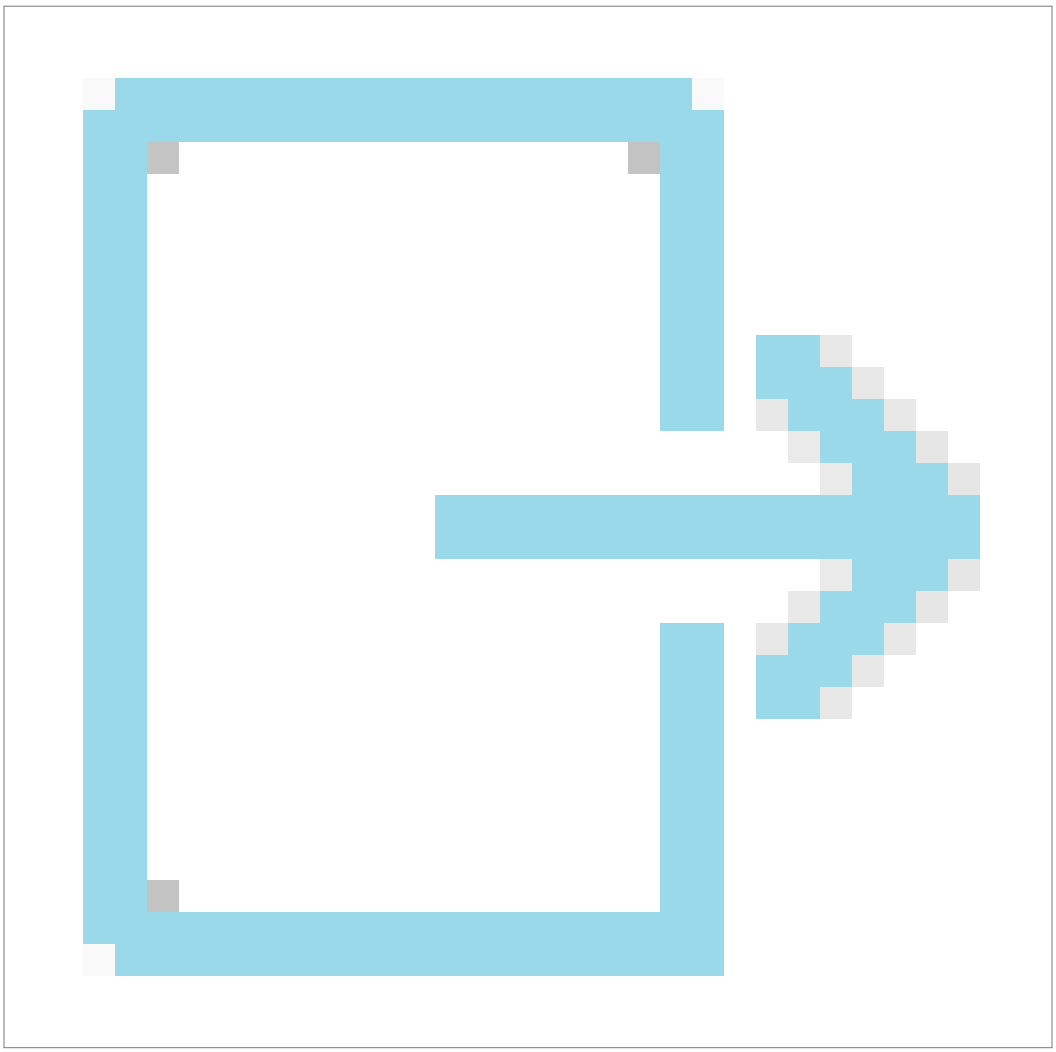
Die Kommission kann geeignete Maßnahmen ergreifen, um die Annahme der erforderlichen Modalitäten, Methoden oder Pläne zu ermöglichen.



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Stellungnahme von Acer
- Benachrichtigung



Output

- Entscheidung

Verantwortlich für die Aktivität: EC

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: EC

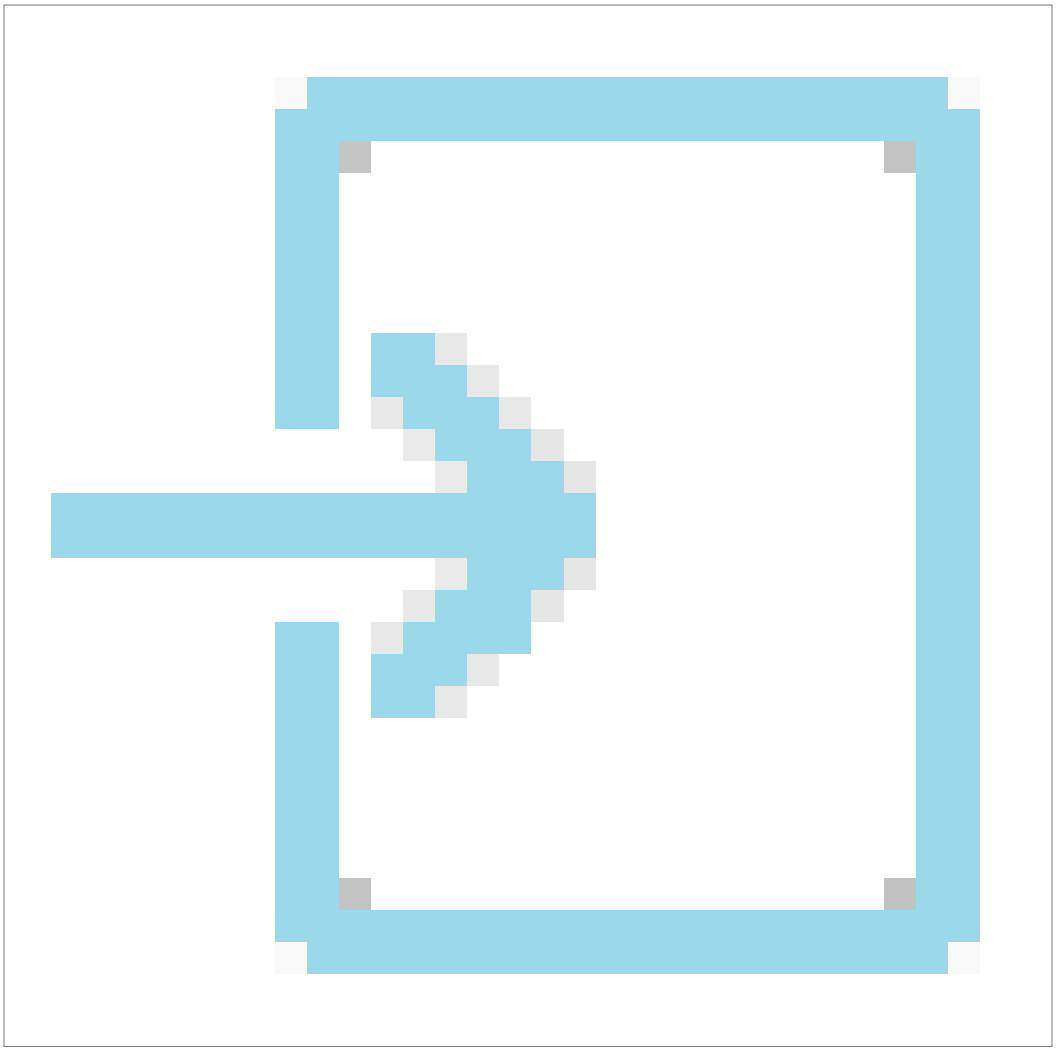
Zu informieren: NCA

10.14 Absatz 9

Die ÜNB veröffentlichen mit Unterstützung von ENTSO-E und der EU-VNBO die Modalitäten oder Methoden oder die Pläne nach der Genehmigung durch die jeweils zuständigen Behörden auf ihren Websites, soweit diese Informationen nicht gemäß Artikel 47 als vertraulich betrachtet werden.

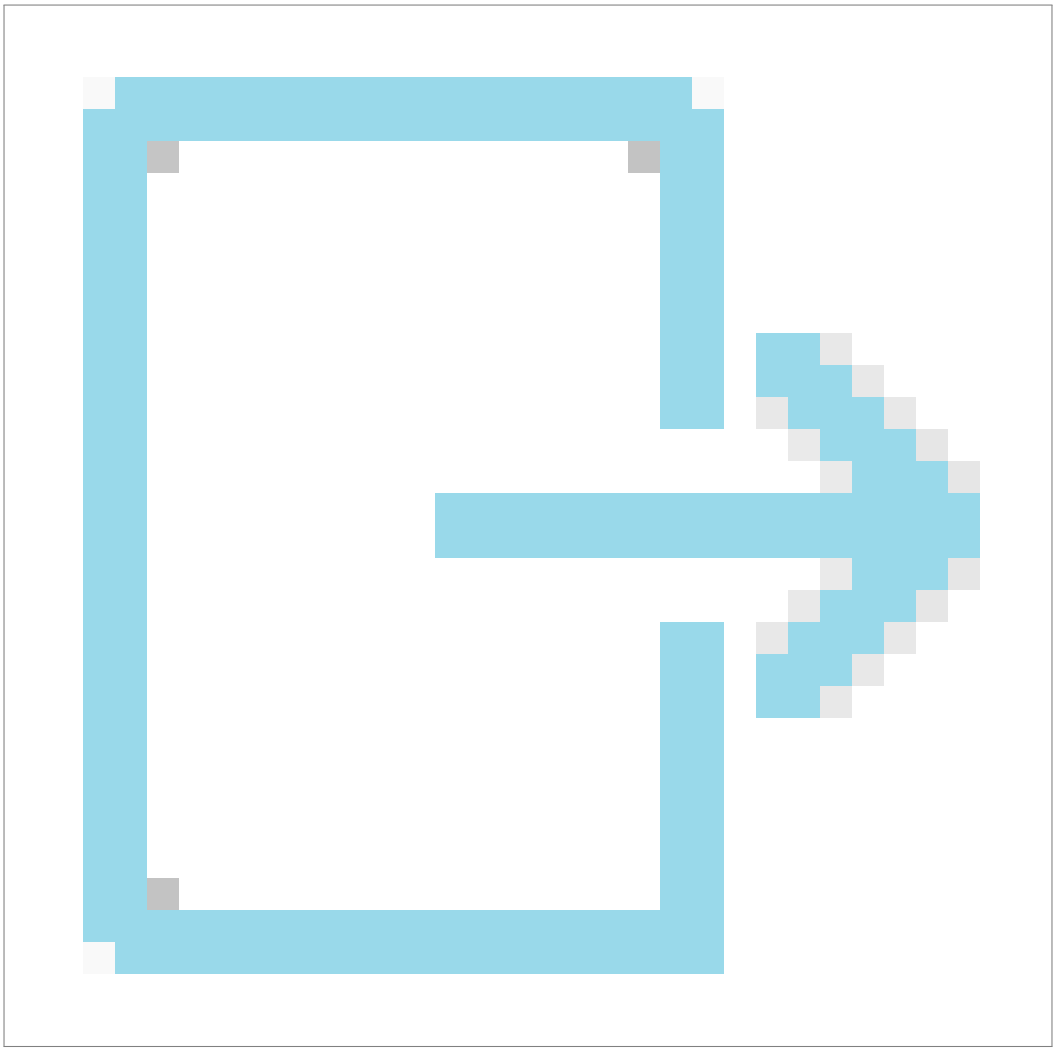
Relevante NCCS-Artikel

- Artikel 47



Input

- Entscheidung



Output

- Methoden zur Risikobewertung (genehmigt)
- Umfassender Risikobewertungsbericht (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen (genehmigt)
- Erweiterte Cybersicherheitskontrollen (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (genehmigt)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (genehmigt)
- Zuordnungsmatrix (genehmigt)
- Empfehlungen für die Beschaffung (genehmigt)

- Methodik zur Klassifizierung von Cyberangriffen (genehmigt)

Verantwortlich für die Aktivität: TSO

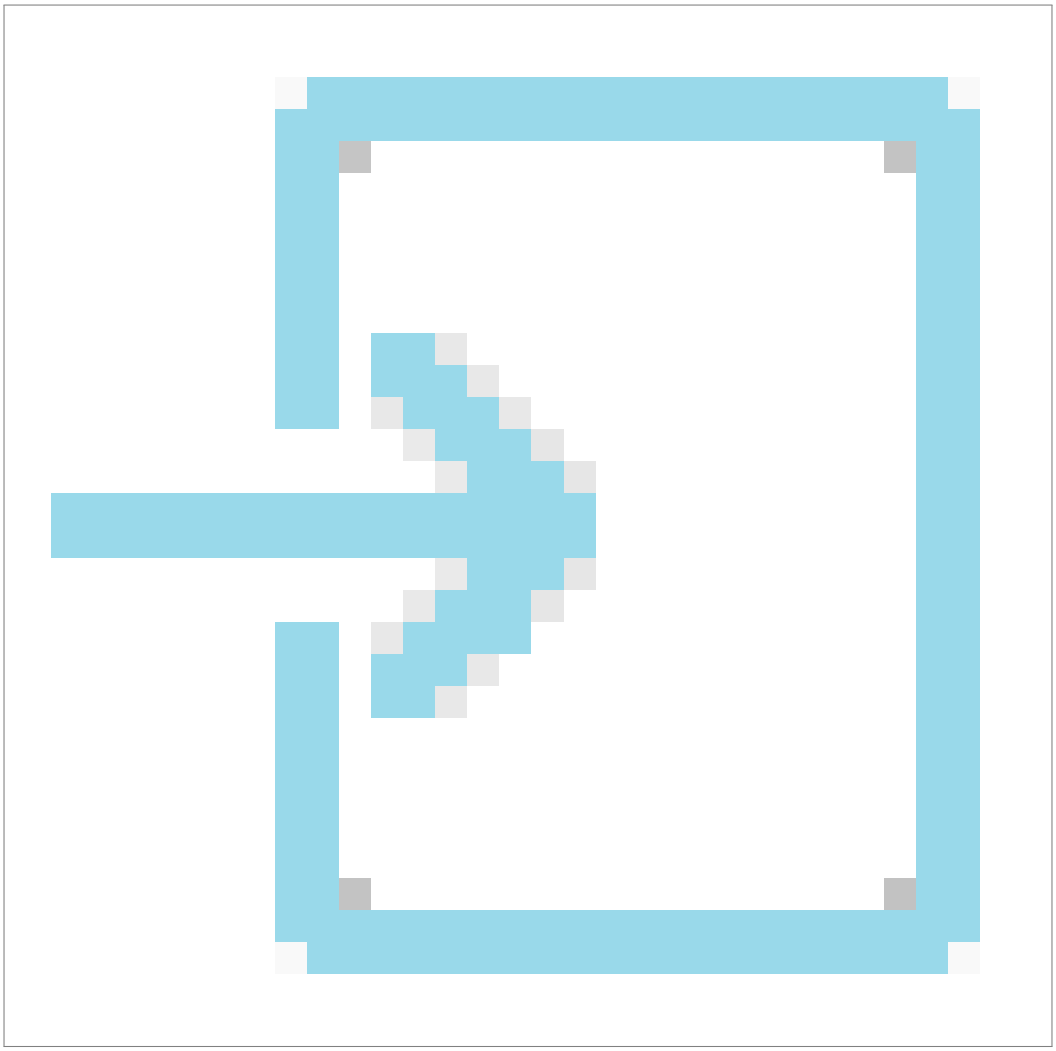
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO, NCA

Zu informieren: HIE, CIE

10.15 Absatz 10

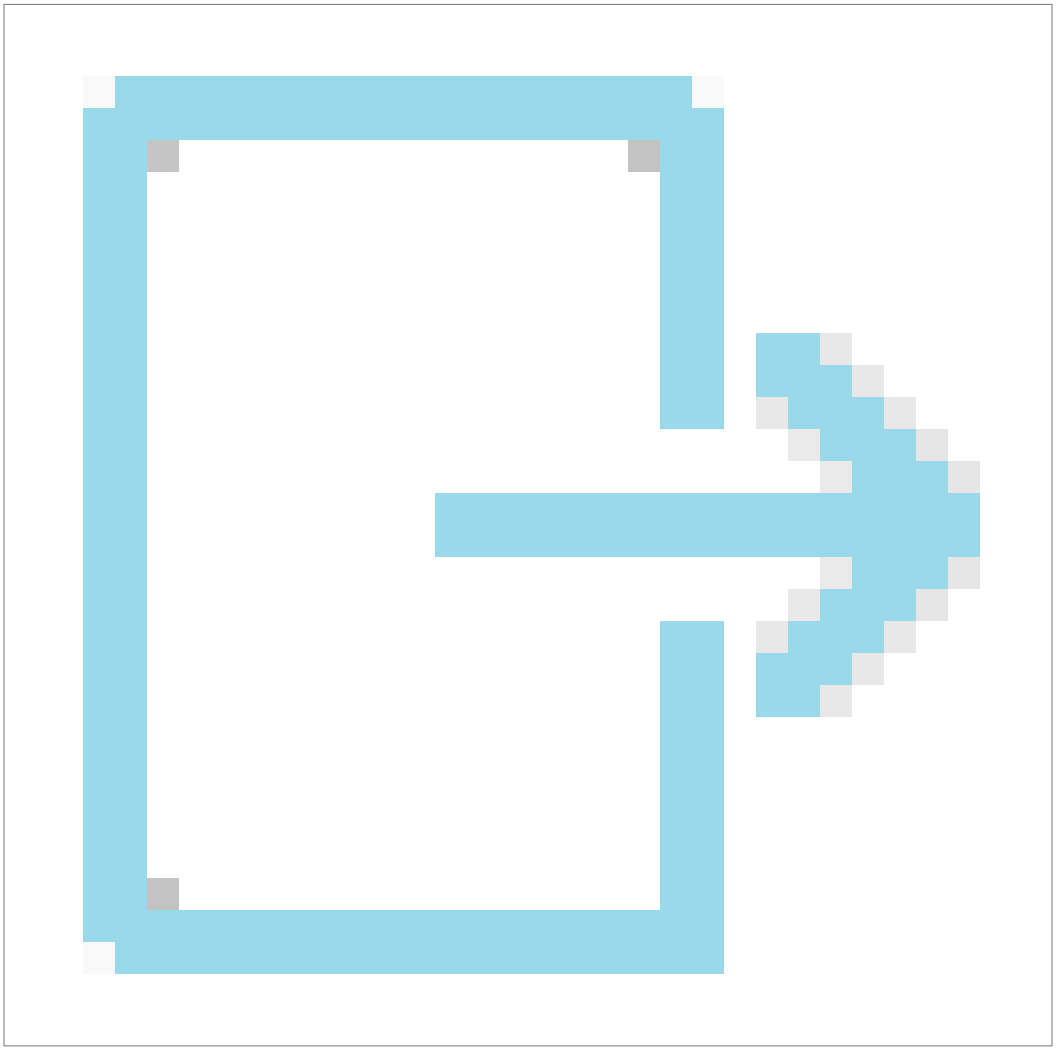
Die zuständigen Behörden können von den ÜNB und der EU-VNBO gemeinsam Vorschläge für Änderungen der genehmigten Modalitäten oder Methoden oder der genehmigten Pläne anfordern und eine Frist für die Einreichung dieser Vorschläge festlegen.



Input

- Methoden zur Risikobewertung (genehmigt)
- Umfassender Risikobewertungsbericht (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen (genehmigt)
- Erweiterte Cybersicherheitskontrollen (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (genehmigt)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (genehmigt)
- Zuordnungsmatrix (genehmigt)
- Empfehlungen für die Beschaffung (genehmigt)

- Methodik zur Klassifizierung von Cyberangriffen (genehmigt)



Output

- Änderungsantrag

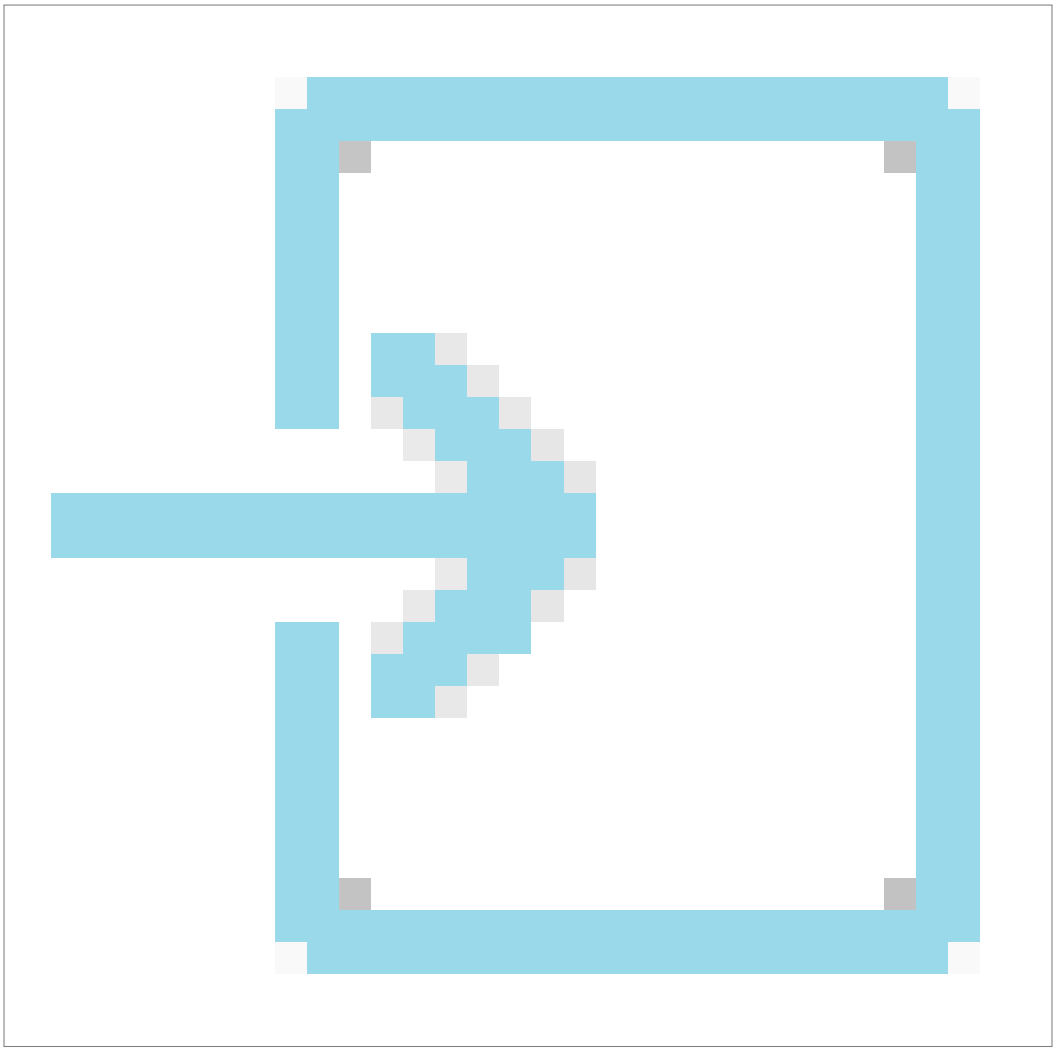
Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO, NCA

10.16 Absatz 10

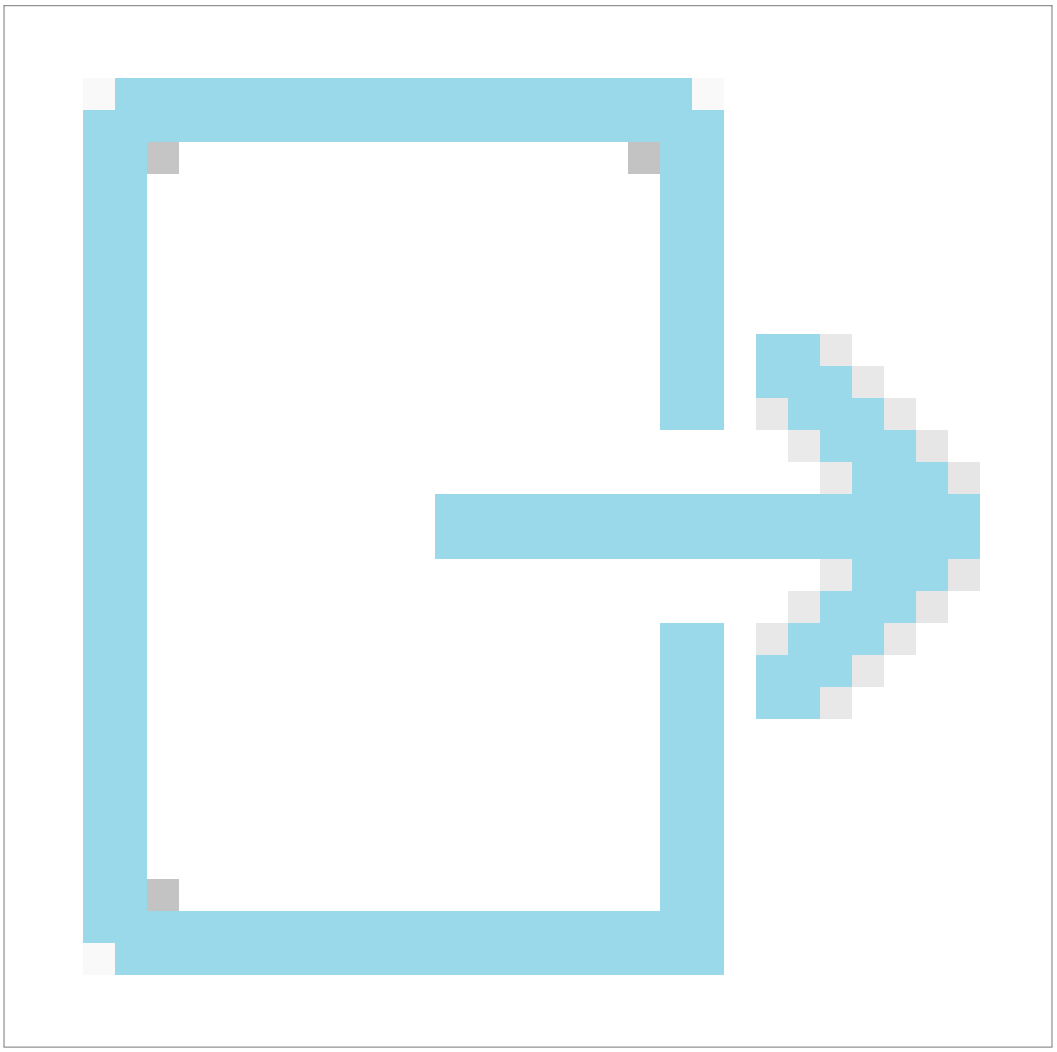
Die ÜNB können den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO auch auf eigene Initiative Änderungen vorschlagen. Die Vorschläge zur Änderung der Modalitäten oder Methoden bzw. zur Änderung der Pläne werden nach dem Verfahren dieses Artikels entwickelt und genehmigt.



Input

- Methoden zur Risikobewertung (genehmigt)
- Umfassender Risikobewertungsbericht (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen (genehmigt)
- Erweiterte Cybersicherheitskontrollen (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (genehmigt)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (genehmigt)
- Zuordnungsmatrix (genehmigt)
- Empfehlungen für die Beschaffung (genehmigt)

- Methodik zur Klassifizierung von Cyberangriffen (genehmigt)



Output

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)

- Empfehlungen für die Beschaffung (Entwurf)
- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Stellungnahme von Acer

Verantwortlich für die Aktivität: TSO

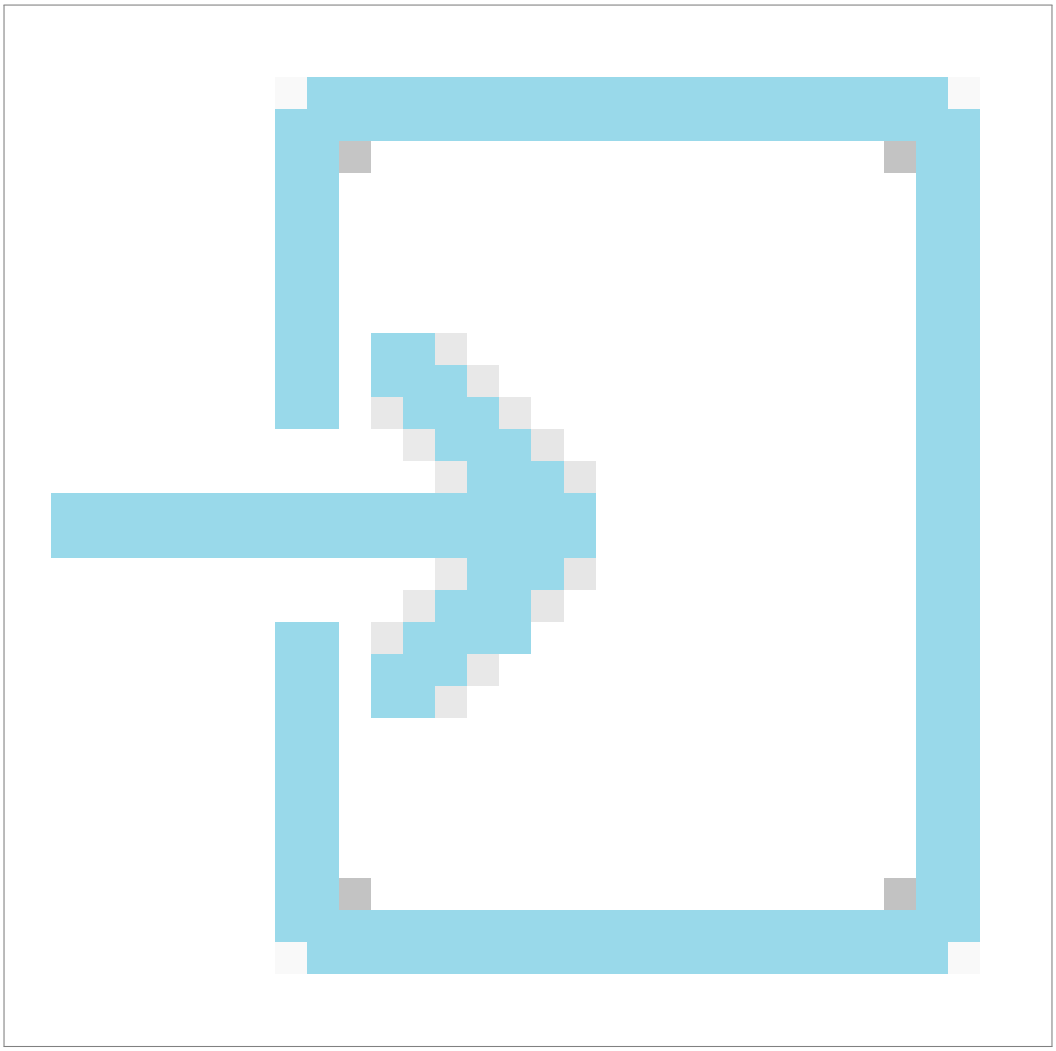
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu informieren: NCA

10.17 Absatz 11

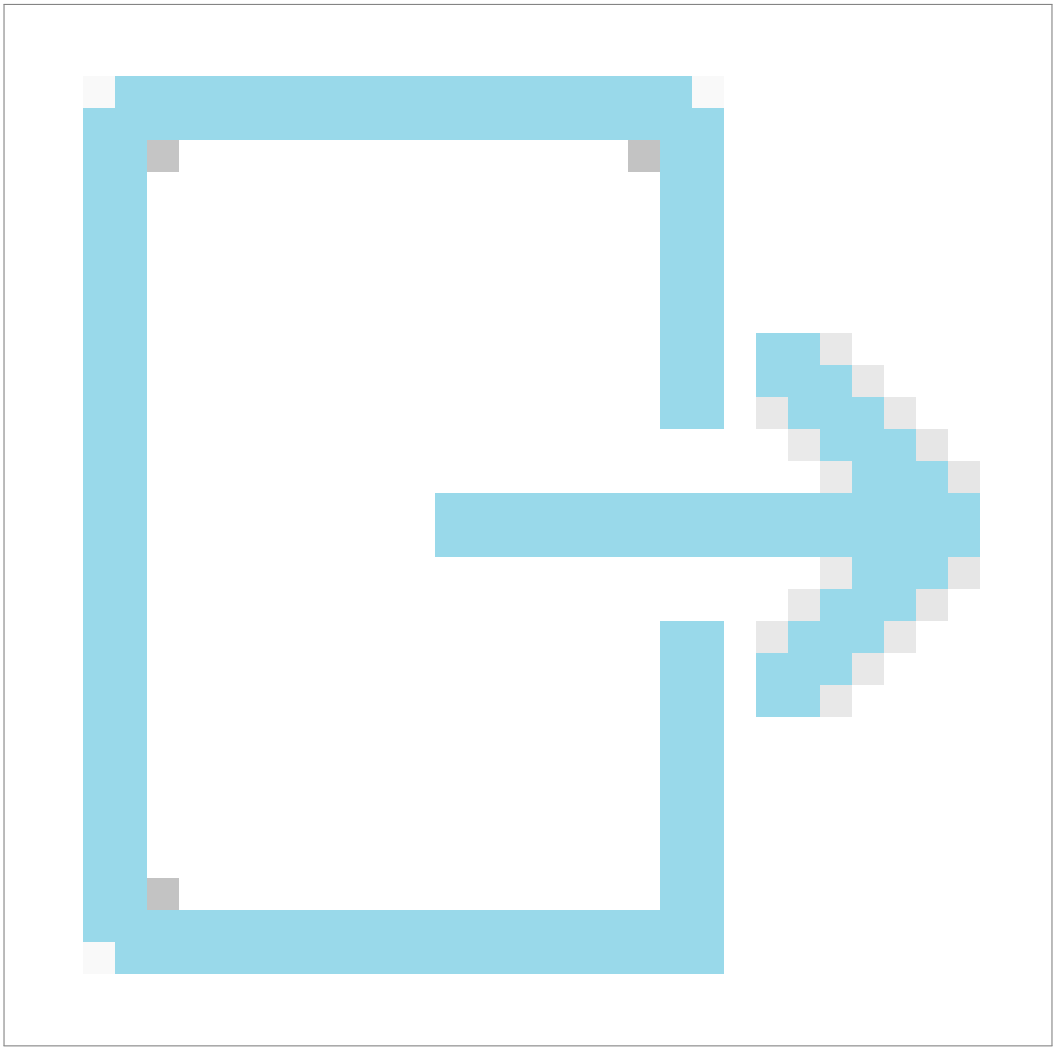
Mindestens alle drei Jahre nach der ersten Annahme der jeweiligen Modalitäten oder Methoden bzw. der Annahme der jeweiligen Pläne überprüfen die ÜNB in Zusammenarbeit mit der EU-VNBO die Wirksamkeit der angenommenen Modalitäten oder Methoden bzw. der angenommenen Pläne und teilen den zuständigen Behörden und der ACER die Ergebnisse der Überprüfung unverzüglich mit.



Input

- Methoden zur Risikobewertung (genehmigt)
- Umfassender Risikobewertungsbericht (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen (genehmigt)
- Erweiterte Cybersicherheitskontrollen (genehmigt)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (genehmigt)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (genehmigt)
- Zuordnungsmatrix (genehmigt)
- Empfehlungen für die Beschaffung (genehmigt)

- Methodik zur Klassifizierung von Cyberangriffen (genehmigt)



Output

- Überprüfungsbericht

GOOD TO KNOW

Zeitpunkt

> innerhalb von 3 Jahren

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu informieren: ACER

Chapter 11

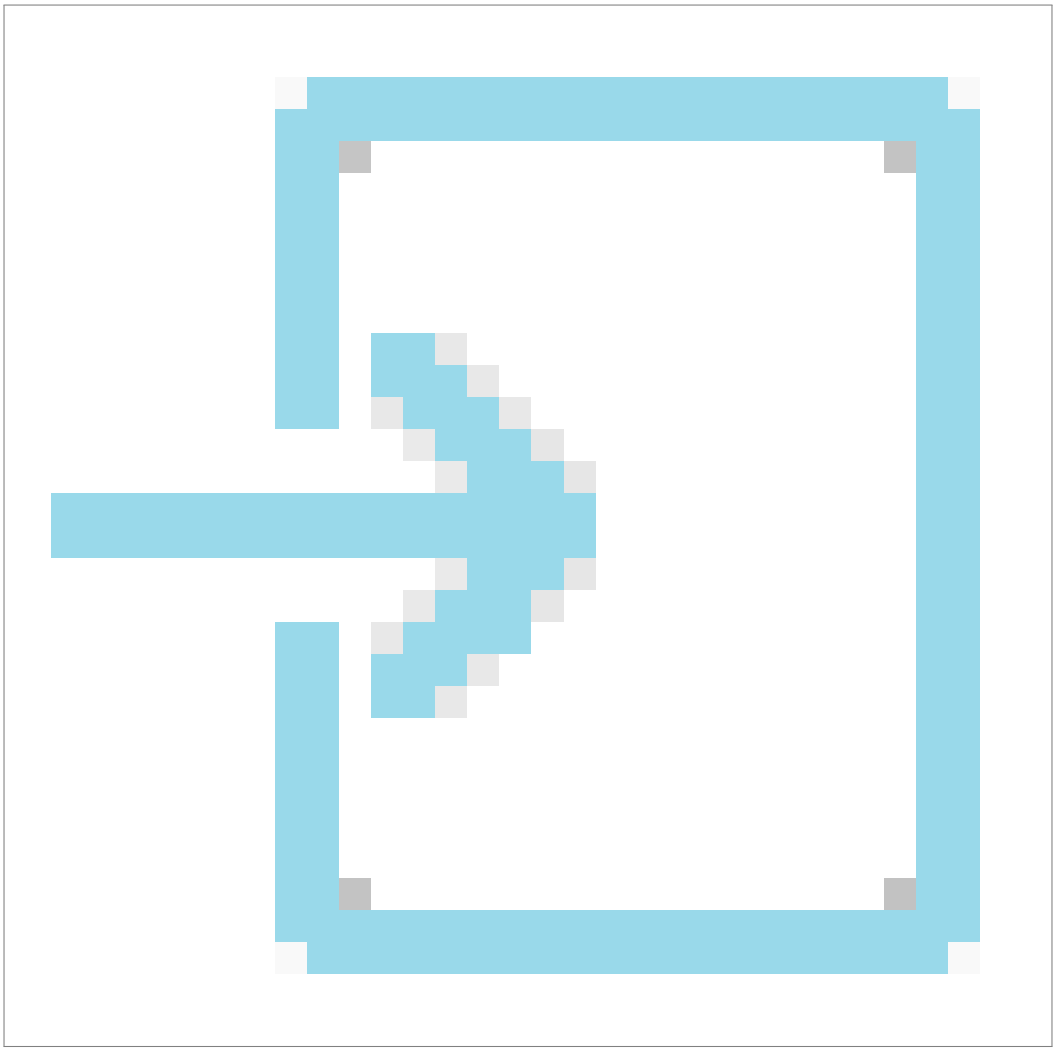
Artikel 9. : Konsultationen

11.1 Absatz 1

Die ÜNB konsultieren mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO die Interessenträger, einschließlich der ACER, der ENISA und der zuständigen Behörde jedes Mitgliedstaats, zu den Entwürfen von Vorschlägen für die in Artikel 6 Absatz 2 genannten Modalitäten oder Methoden und für die in Artikel 6 Absatz 3 genannten Pläne. Die Konsultation dauert mindestens einen Monat.

Relevante NCCS-Artikel

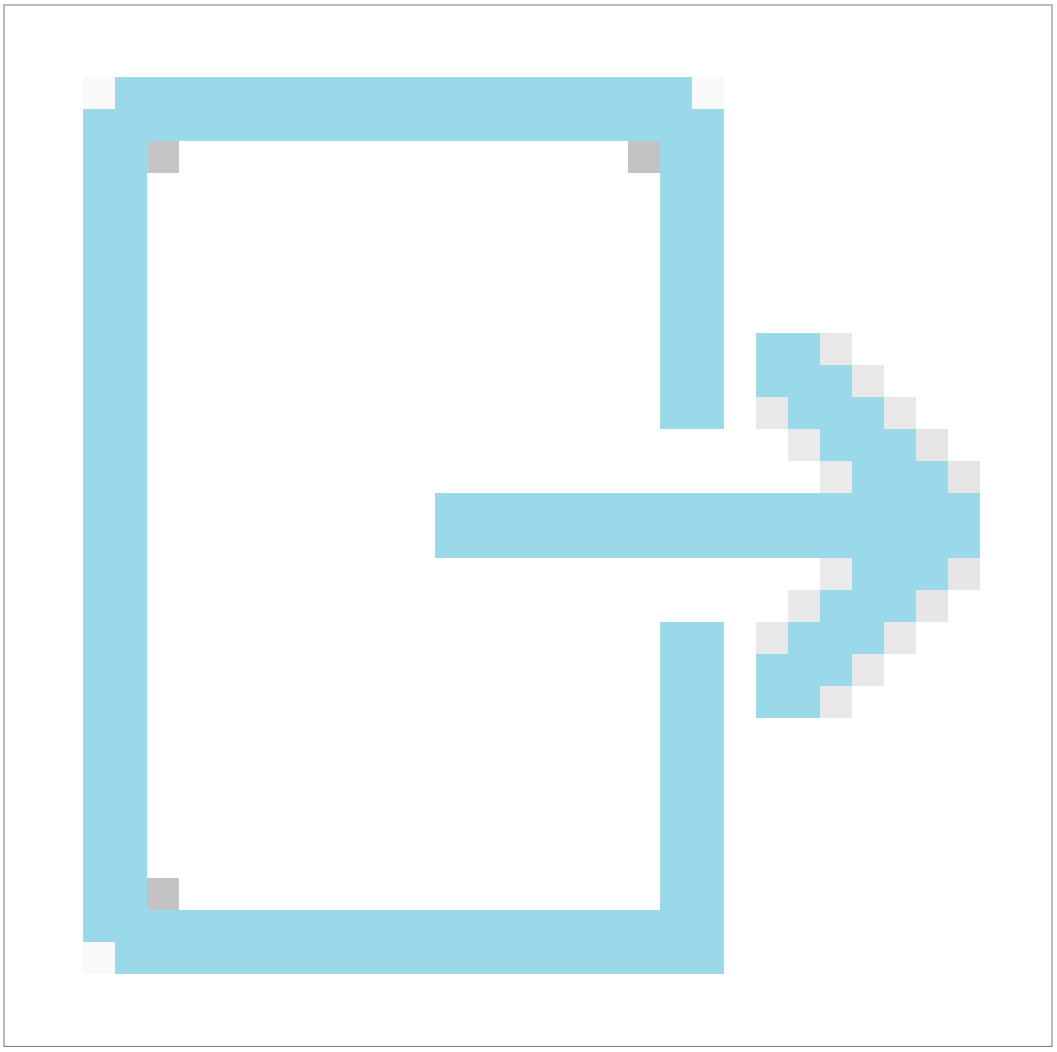
- Artikel 6 (2)
- Artikel 6 (3)



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Regionaler Plan zur Risikominderung (Entwurf)



Output

- Kommentare

GOOD TO KNOW

Zeitpunkt

> Min. 1 Monat

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: ACER, ENISA

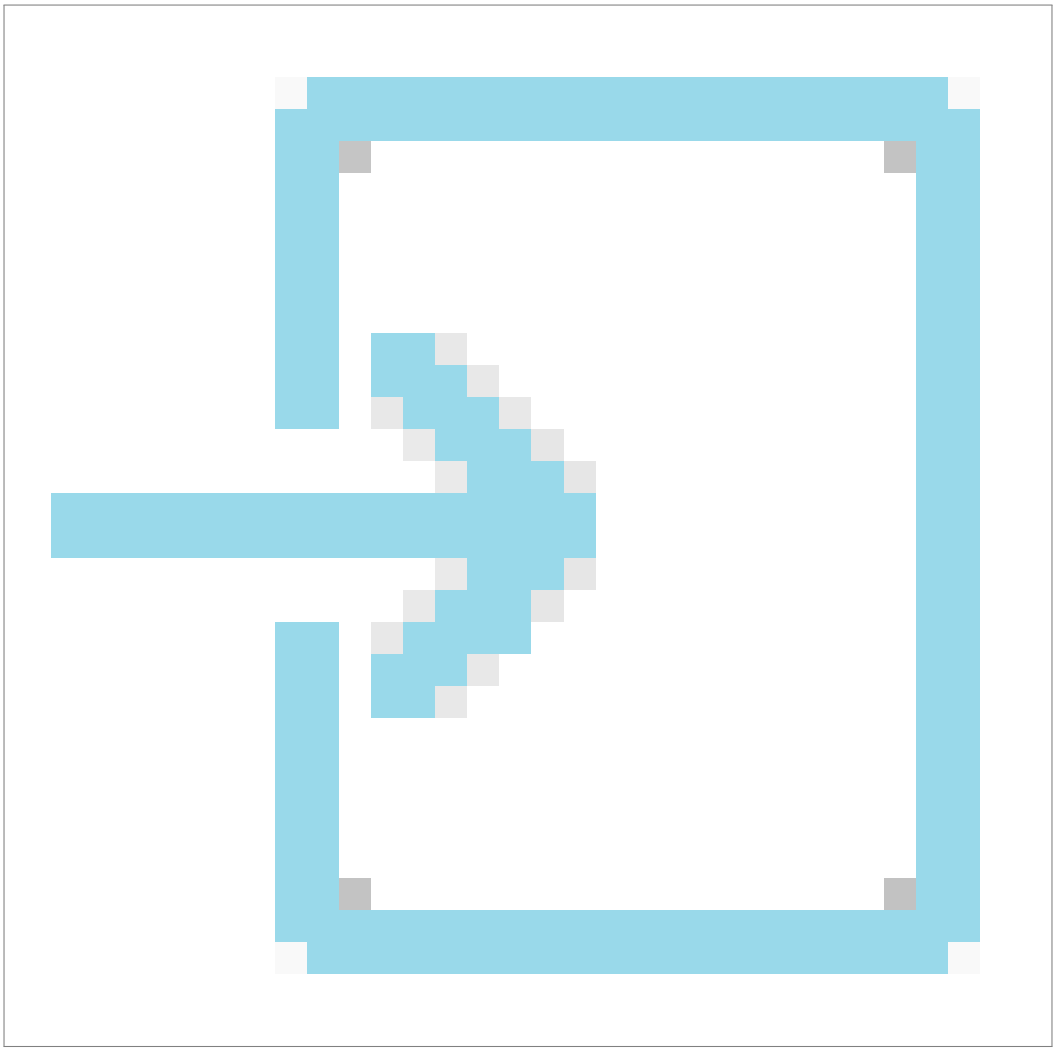
11.2 Absatz 2

Die in Artikel 6 Absatz 2 genannten Vorschläge für Modalitäten oder Methoden, die von den ÜNB in Zusammenarbeit mit der EU-VNBO vorgelegt wurden, werden veröffentlicht und auf Unionsebene einer Konsultation unterzogen. Die von den relevanten ÜNB in Zusammenarbeit mit der EU-VNBO auf regionaler Ebene vorgelegten Vorschläge für Pläne gemäß Artikel 6 Absatz 3 werden mindestens auf regionaler Ebene einer Konsultation unterzogen.

>

Relevante NCCS-Artikel

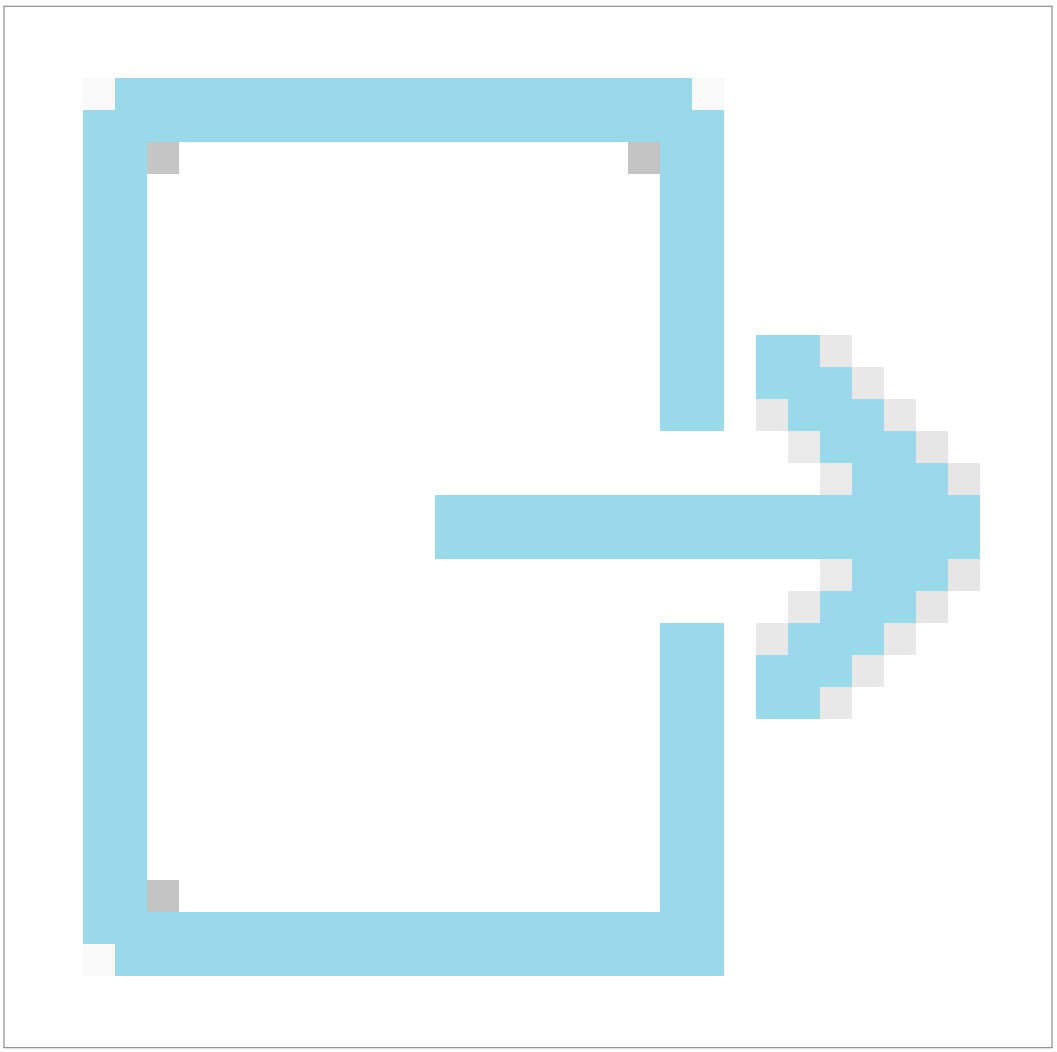
- Artikel 6 (2)
- Artikel 6 (3)



Input

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Regionaler Plan zur Risikominderung (Entwurf)



Output

- Kommentare

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

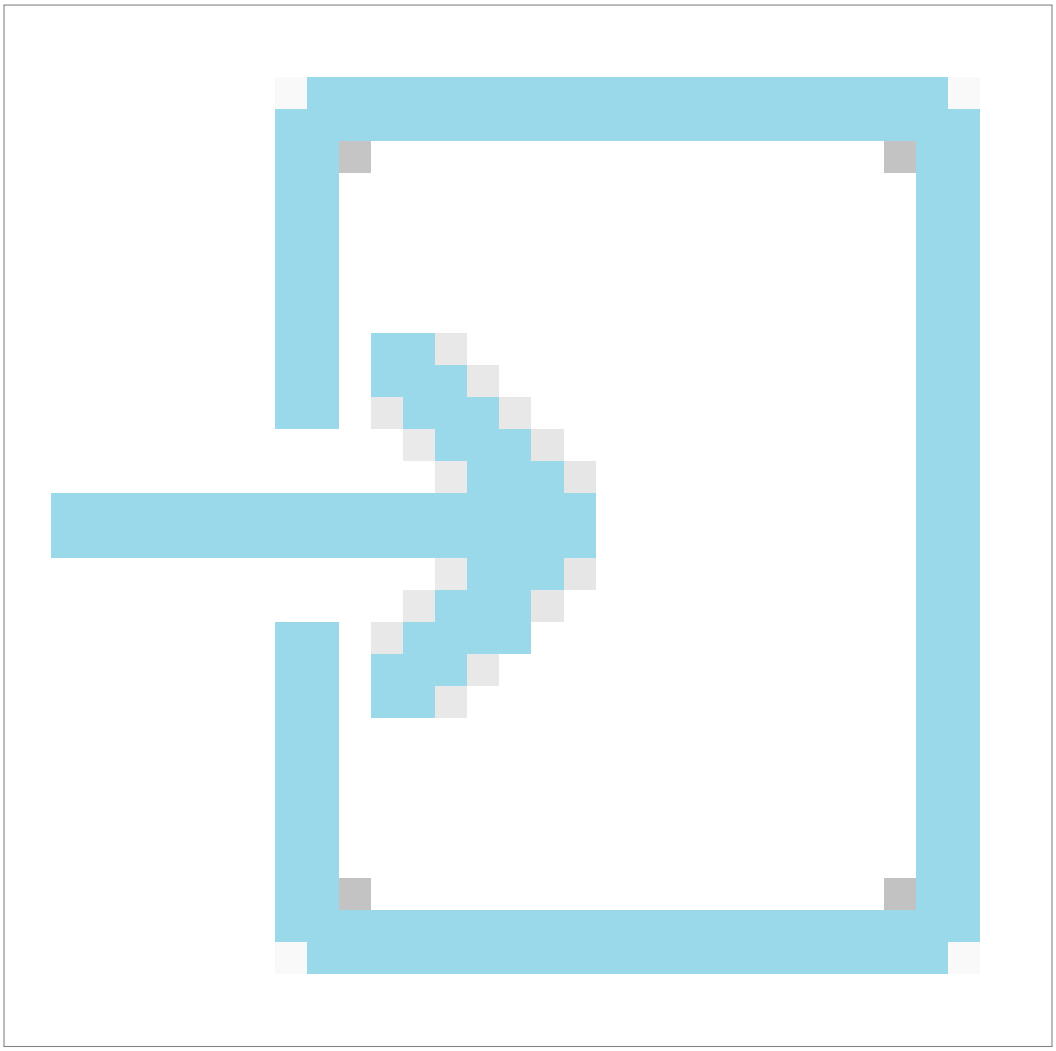
Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

11.3 Absatz 3

Die ÜNB, unterstützt von ENTSO-E, und die für den Vorschlag für Modalitäten, Methoden oder Pläne zuständige EU-VNBO tragen den in den gemäß Absatz 1 durchgeführten Konsultationen geäußerten Ansichten der Interessenträger, gebührend Rechnung, bevor sie die Vorschläge zur regulatorischen Genehmigung vorlegen. In allen Fällen ist zusammen mit dem Vorschlag eine fundierte Begründung vorzulegen, weshalb die aus der Konsultation hervorgegangenen Stellungnahmen berücksichtigt bzw. nicht berücksichtigt wurden, und rechtzeitig — vor oder gleichzeitig mit dem Vorschlag für Modalitäten oder Methoden — zu veröffentlichen.

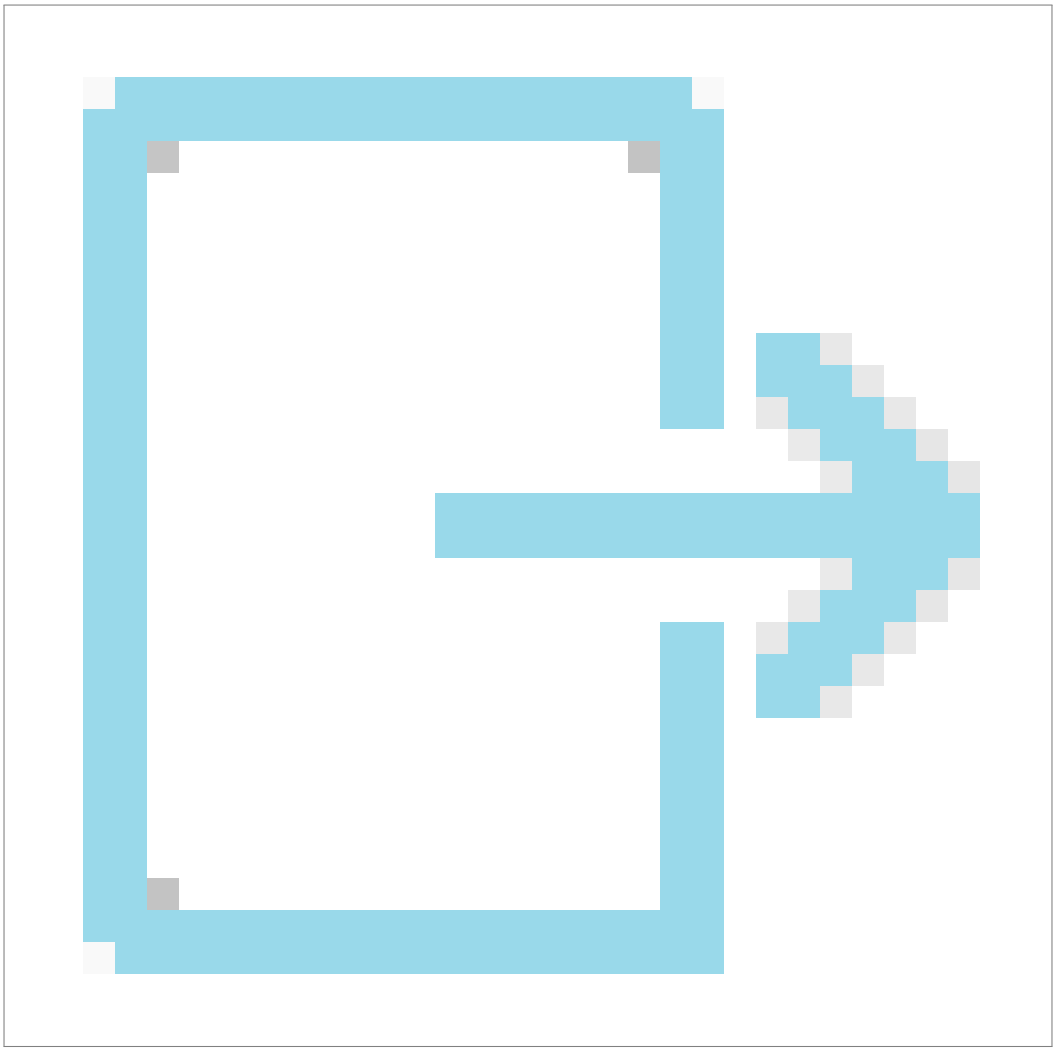
Relevante NCCS-Artikel

- Artikel 9 (1)



Input

- Kommentare



Output

- Methoden zur Risikobewertung (Entwurf)
- Umfassender Risikobewertungsbericht (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen (Entwurf)
- Erweiterte Cybersicherheitskontrollen (Entwurf)
- Mindestanforderungen an Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)
- Zuordnungsmatrix (Entwurf)
- Empfehlungen für die Beschaffung (Entwurf)

- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Regionaler Risikominderungsplan (Entwurf)

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

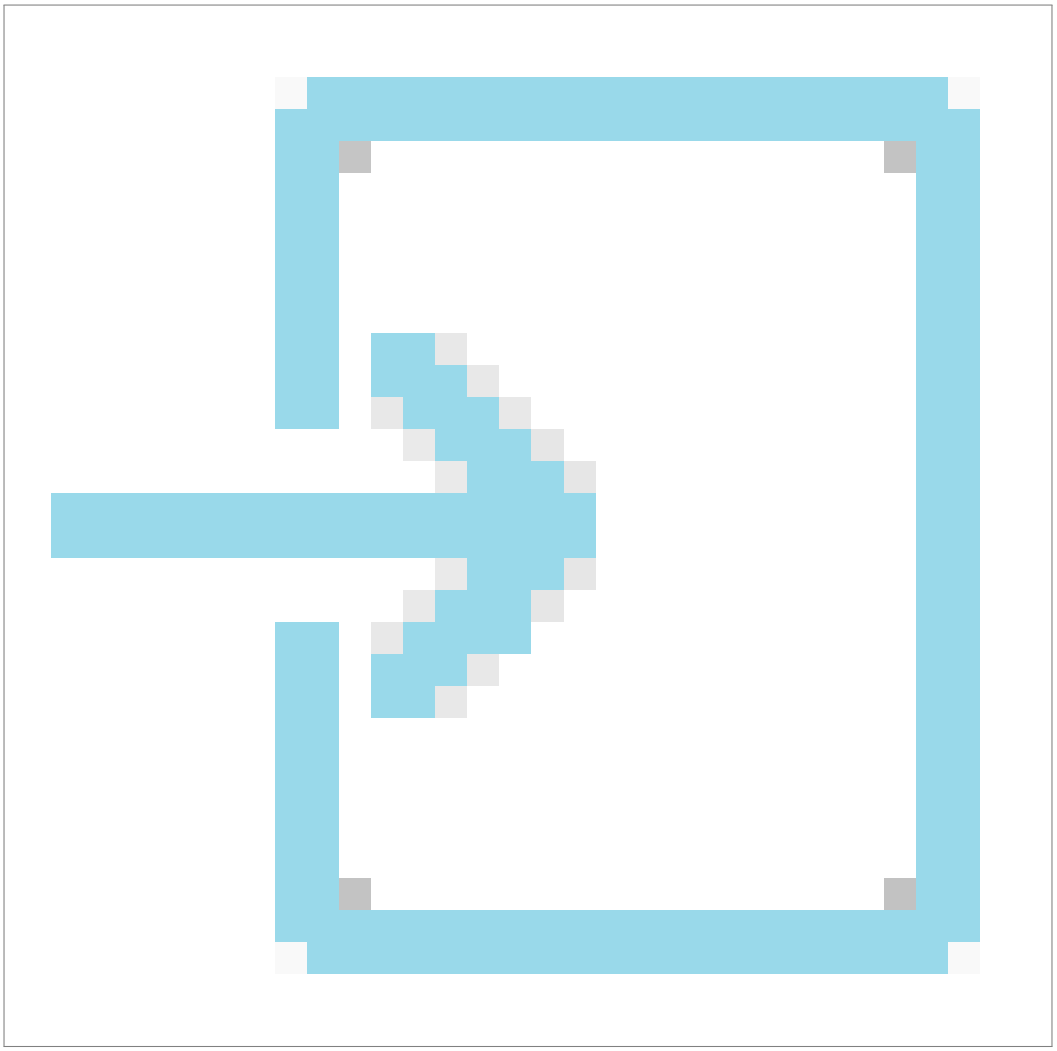
Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Chapter 12

Artikel 10. : Einbeziehung der Interessenträger

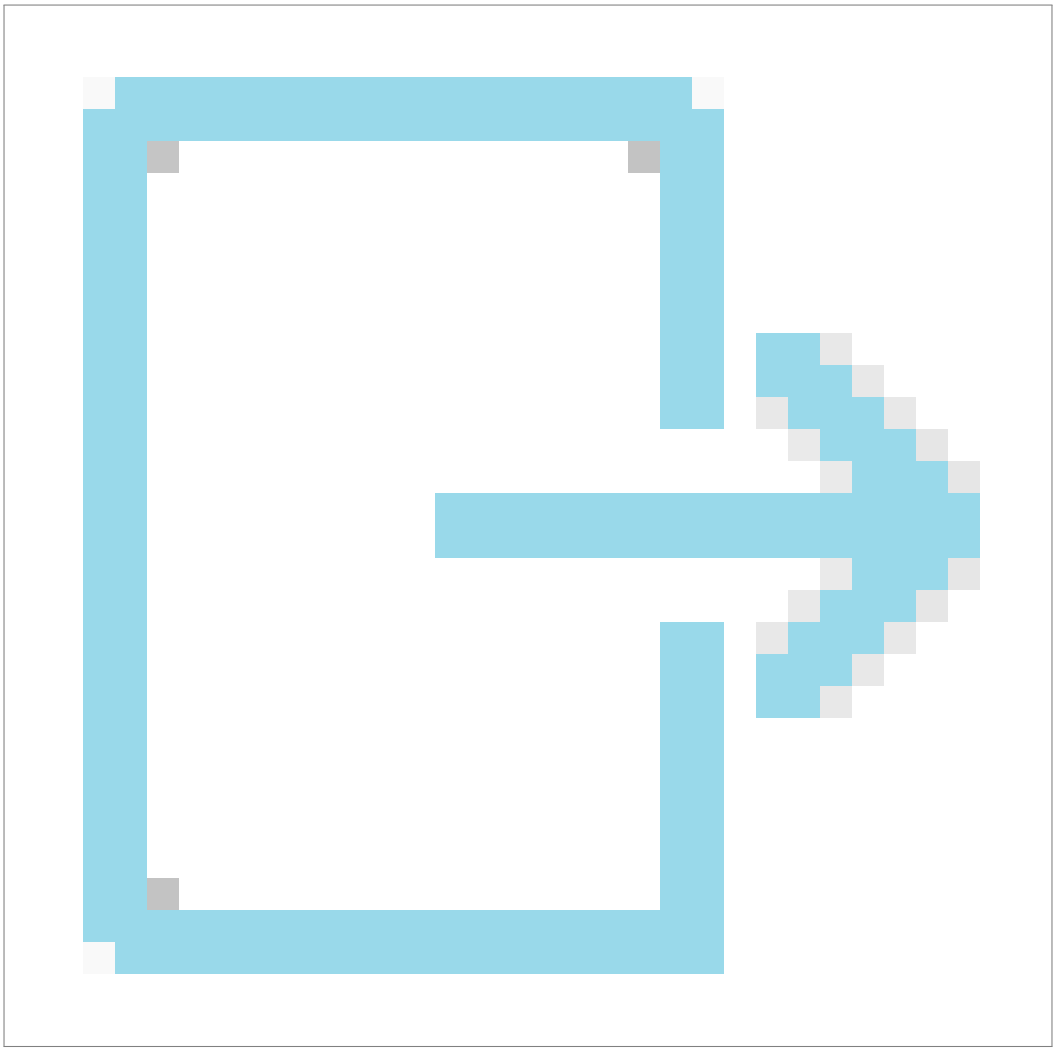
12.1 Absatz

Die ACER organisiert in enger Zusammenarbeit mit ENTSO-E und der EU-VNBO die Einbeziehung der Interessenträger, einschließlich regelmäßiger Treffen mit Interessenträgern, um Probleme zu ermitteln und Verbesserungen im Zusammenhang mit der Durchführung dieser Verordnung vorzuschlagen.



Input

- Kommentare



Output

- Überprüfungsbericht

A

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: ENTSO-E, ACER, EU DSO

Chapter 13

Artikel 11. : Kostenerstattung

13.1 Absatz 1

Die Kosten, die aufgrund der Verpflichtungen aus dieser Verordnung bei ÜNB und VNB anfallen, die der Netzentgeltregulierung unterliegen, einschließlich der Kosten von ENTSO-E und der EU-VNBO, werden von der zuständigen NRB jedes Mitgliedstaats geprüft.

Verantwortlich für die Aktivität: NRA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO, DSO, NRA

13.2 Absatz 2

Als angemessen, effizient und verhältnismäßig bewertete Kosten werden durch Netzentgelte oder andere geeignete Mechanismen gedeckt, die von der zuständigen NRB festgelegt werden.

Verantwortlich für die Aktivität: NRA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NRA

13.3 Absatz 3

Auf Verlangen der zuständigen NRB stellen die in Absatz 1 genannten ÜNB und VNB innerhalb einer von der NRB festgelegten angemessenen Frist die erforderlichen Informationen bereit, um die Prüfung der entstandenen Kosten zu erleichtern.

Relevante NCCS-Artikel

- Artikel 11 (1)

Verantwortlich für die Aktivität: NRA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: TSO, DSO, NRA

Chapter 14

Artikel 12. : Überwachung

14.1 Absatz 1

Die ACER überwacht die Durchführung dieser Verordnung gemäß Artikel 32 Absatz 1 der Verordnung (EU) 2019/943 und Artikel 4 Absatz 2 der Verordnung (EU) 2019/942. Bei der Durchführung der Überwachung kann die ACER mit der ENISA zusammenarbeiten und ENTSO-E und die EU-VNBO um Unterstützung ersuchen. Die ACER unterrichtet die Koordinierungsgruppe „Strom“ und die NIS-Kooperationsgruppe regelmäßig über die Durchführung dieser Verordnung. Article 32(1) of Regulation (EU) 2019/943 [a] Article 4(2) of Regulation (EU) 2019/942 [b]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943&qid=1733993709560#d1e3462-54-1

[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942#d1e519-22-1

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, ACER, ENISA, EU DSO

Zu informieren: NIS CG, ECG

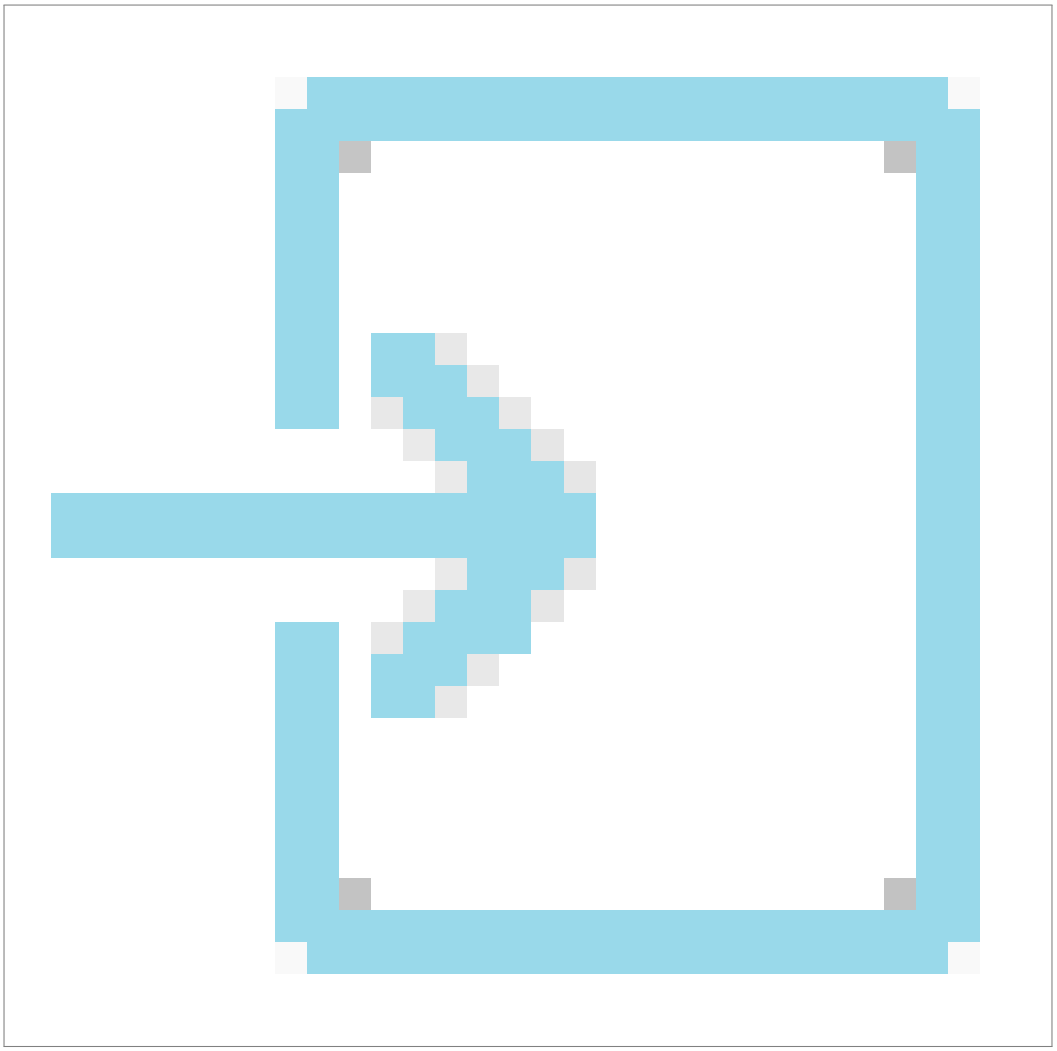
14.2 Absatz 2

Die ACER veröffentlicht nach dem Inkrafttreten dieser Verordnung mindestens alle drei Jahre einen Bericht, um

a. den Stand der Umsetzung der anwendbaren Risikomanagementmaßnahmen im Bereich der Cybersicherheit durch Einrichtungen mit erheblichen Auswirkungen und Einrichtungen mit kritischen Auswirkungen zu überprüfen;

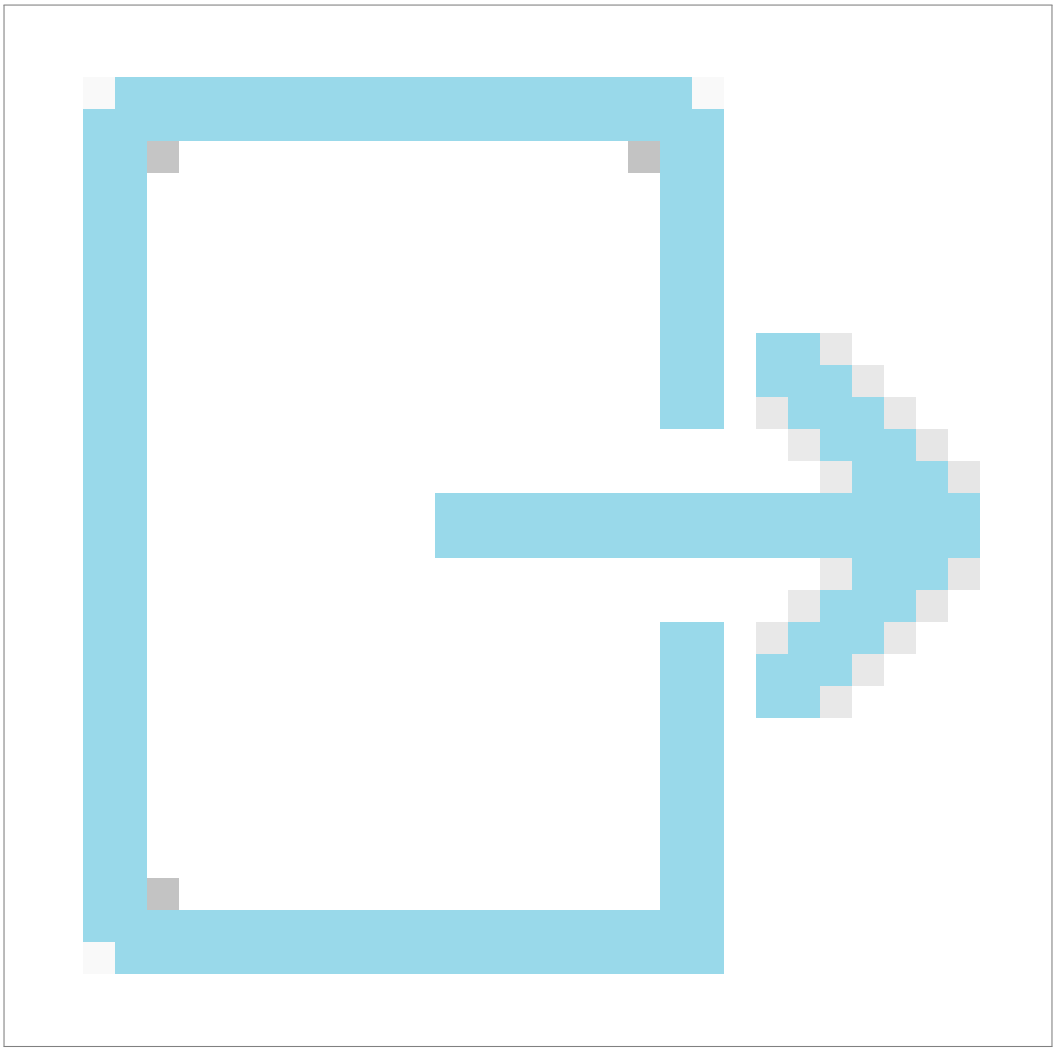
b. zu ermitteln, ob zur Prävention von Risiken für den Elektrizitätssektor zusätzliche Vorschriften über gemeinsame Anforderungen, Planung, Beobachtung, Berichterstattung und Krisenbewältigung erforderlich sein könnten, und

c. Verbesserungsbedarf für die Überarbeitung dieser Verordnung zu bestimmen oder nicht abgedeckte Bereiche und neue Prioritäten zu ermitteln, die sich aufgrund technischer Entwicklungen ergeben können.



Input

- Überwachungsdaten



Output

- Statusbericht

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Oktober 2026

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

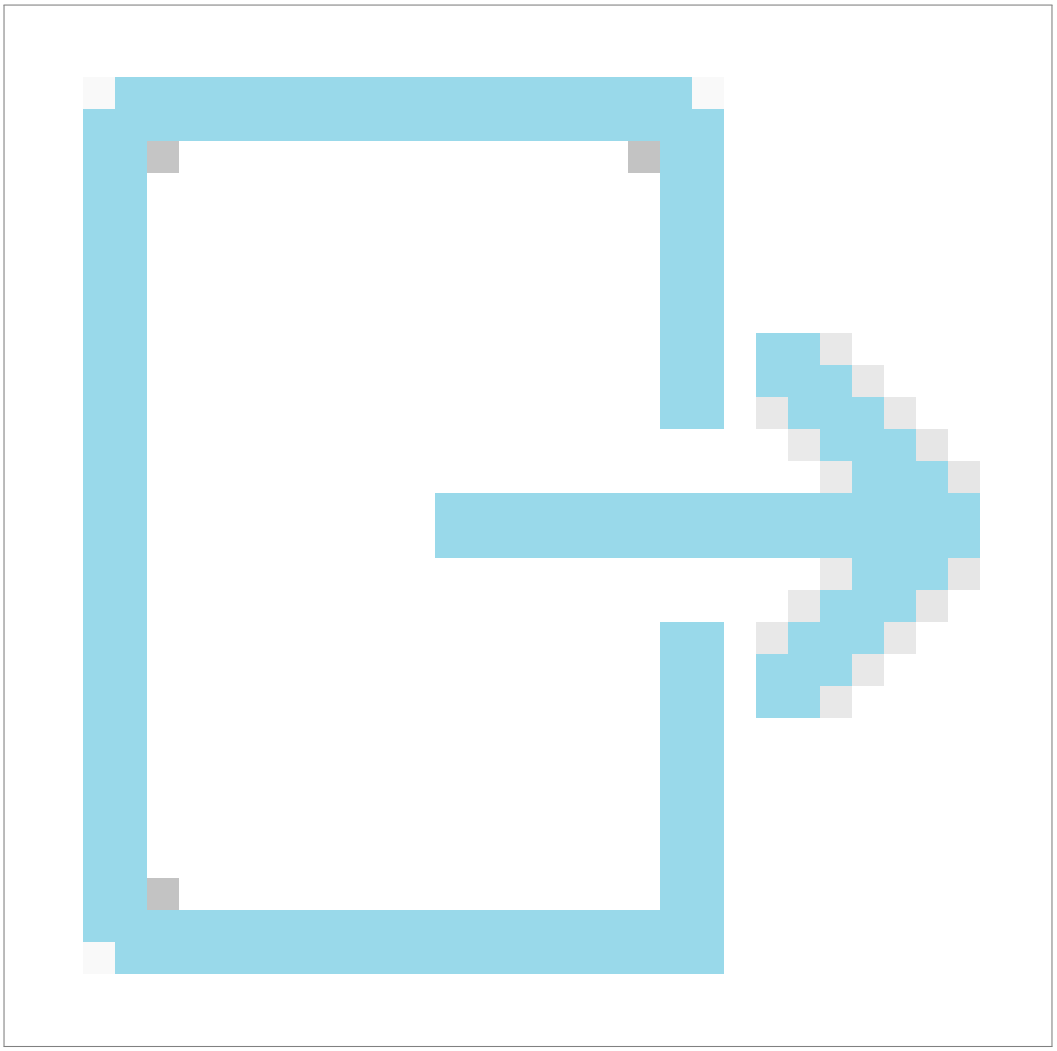
Beteiligt an der Aufgabenausführung: ACER

14.3 Absatz 3

Bis zum 13 Juni 2025 kann die ACER in Zusammenarbeit mit der ENISA und nach Konsultation von ENTSO-E und der EU-VNBO auf der Grundlage der gemäß Absatz 5 festgelegten Leistungsindikatoren Leitlinien zu den relevanten Informationen, die der ACER zu Überwachungszwecken zu übermitteln sind, sowie zu dem Verfahren und der Häufigkeit der Einholung der Informationen vorlegen.

Relevante NCCS-Artikel

- Artikel 12 (5)



Output

- Anleitung

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Juni 2025

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ACER, ENISA

Zu konsultieren: ENTSO-E, EU DSO

14.4 Absatz 4

Die zuständigen Behörden können Zugang zu den einschlägigen Informationen erhalten, die sich im Besitz der ACER befinden und gemäß diesem Artikel erhoben wurden.

Verantwortlich für die Aktivität: ACER

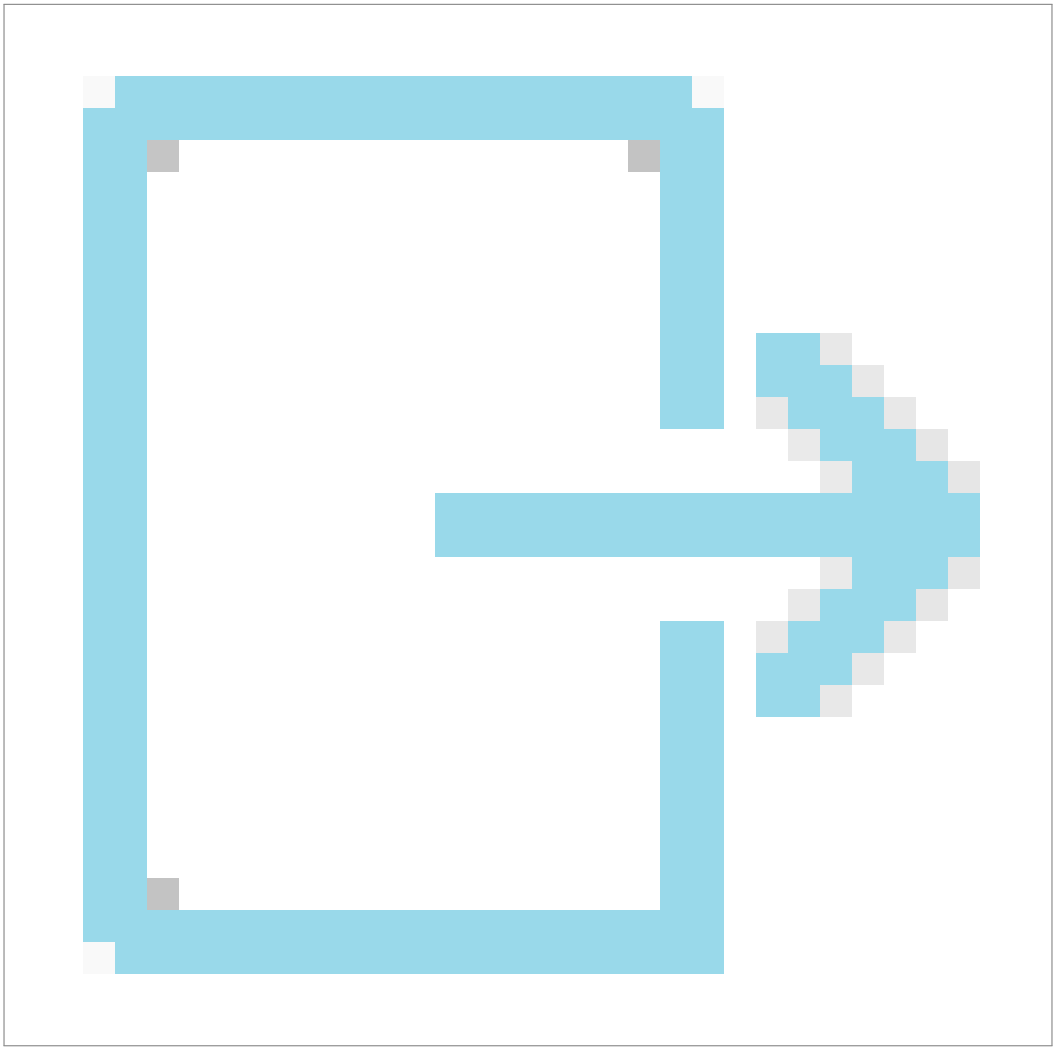
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ACER

Zu informieren: NCA

14.5 Absatz 5

Die ACER legt in Zusammenarbeit mit der ENISA und mit Unterstützung von ENTSO-E und der EU-VNBO in Bezug auf Cybersicherheitsaspekte grenzüberschreitender Stromflüsse unverbindliche Leistungsindikatoren für die Bewertung der betrieblichen Zuverlässigkeit vor.



Output

- ORPI

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Juni 2027

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

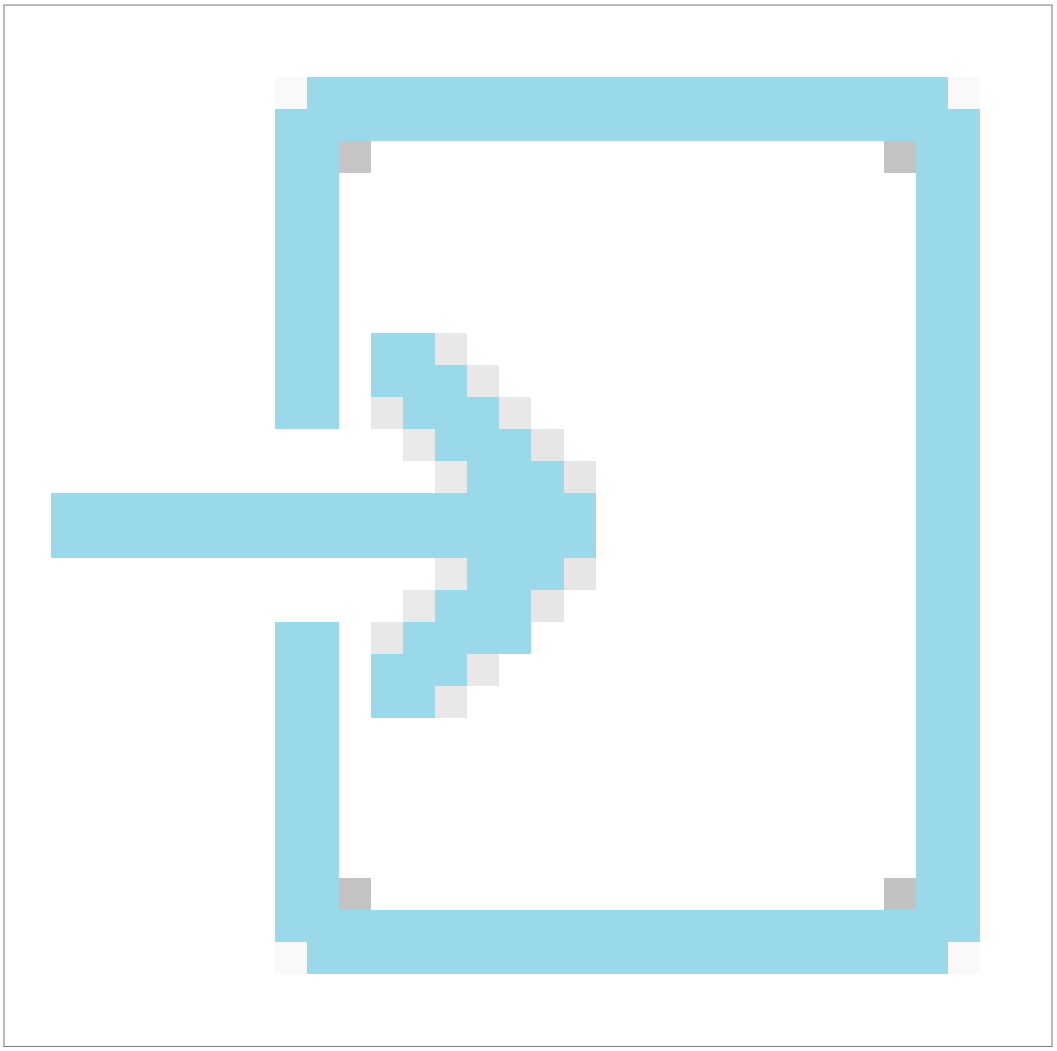
Beteiligt an der Aufgabenausführung: ENTSO-E, ACER, ENISA, EU DSO

14.6 Absatz 6

Die in Artikel 2 Absatz 1 dieser Verordnung aufgeführten Einrichtungen übermitteln der ACER die Informationen, die diese zur Wahrnehmung der in Absatz 2 genannten Aufgaben benötigt.

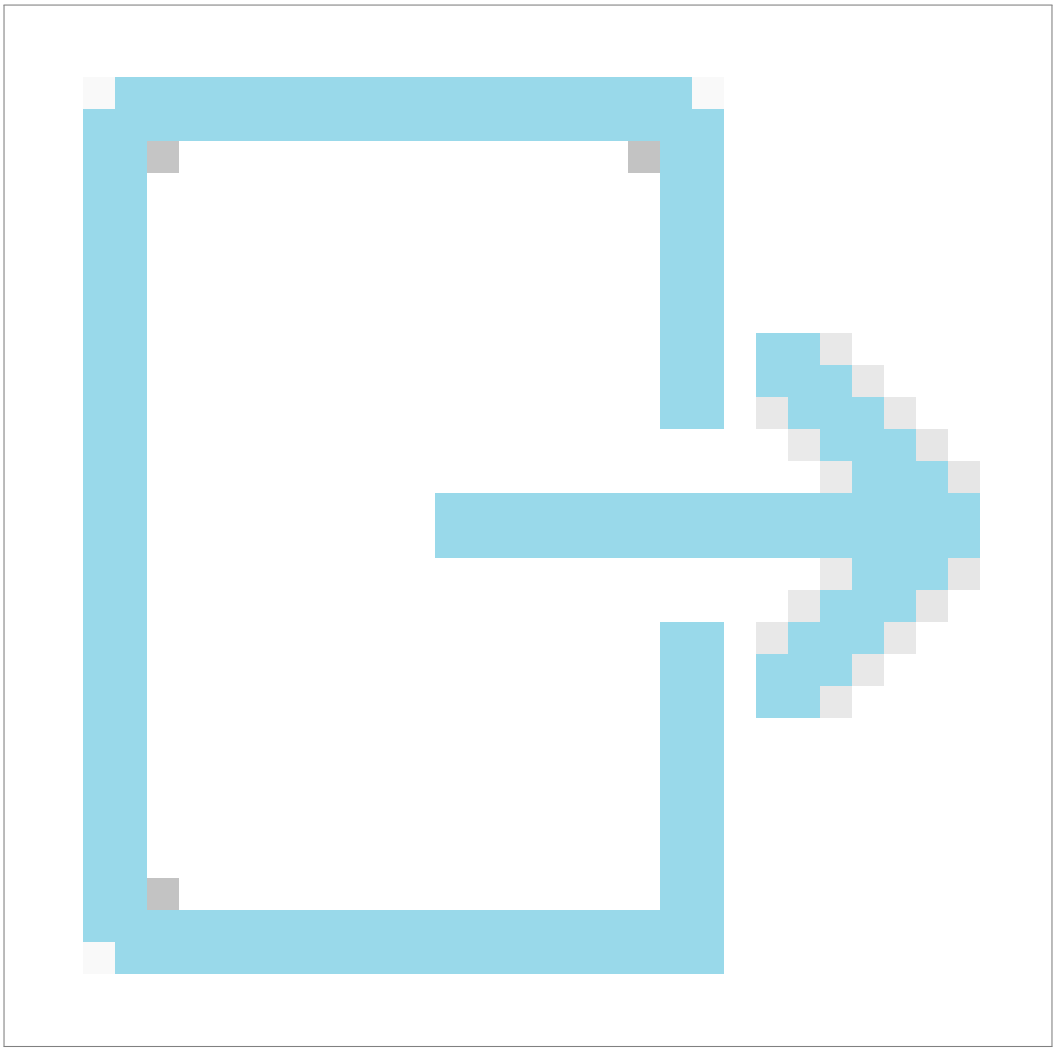
Relevante NCCS-Artikel

- Artikel 2 (1)
- Artikel 2 (2)



Input

- Anleitung
- ORPI



Output

- Überwachungsdaten

A

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Zu informieren: ACER

Chapter 15

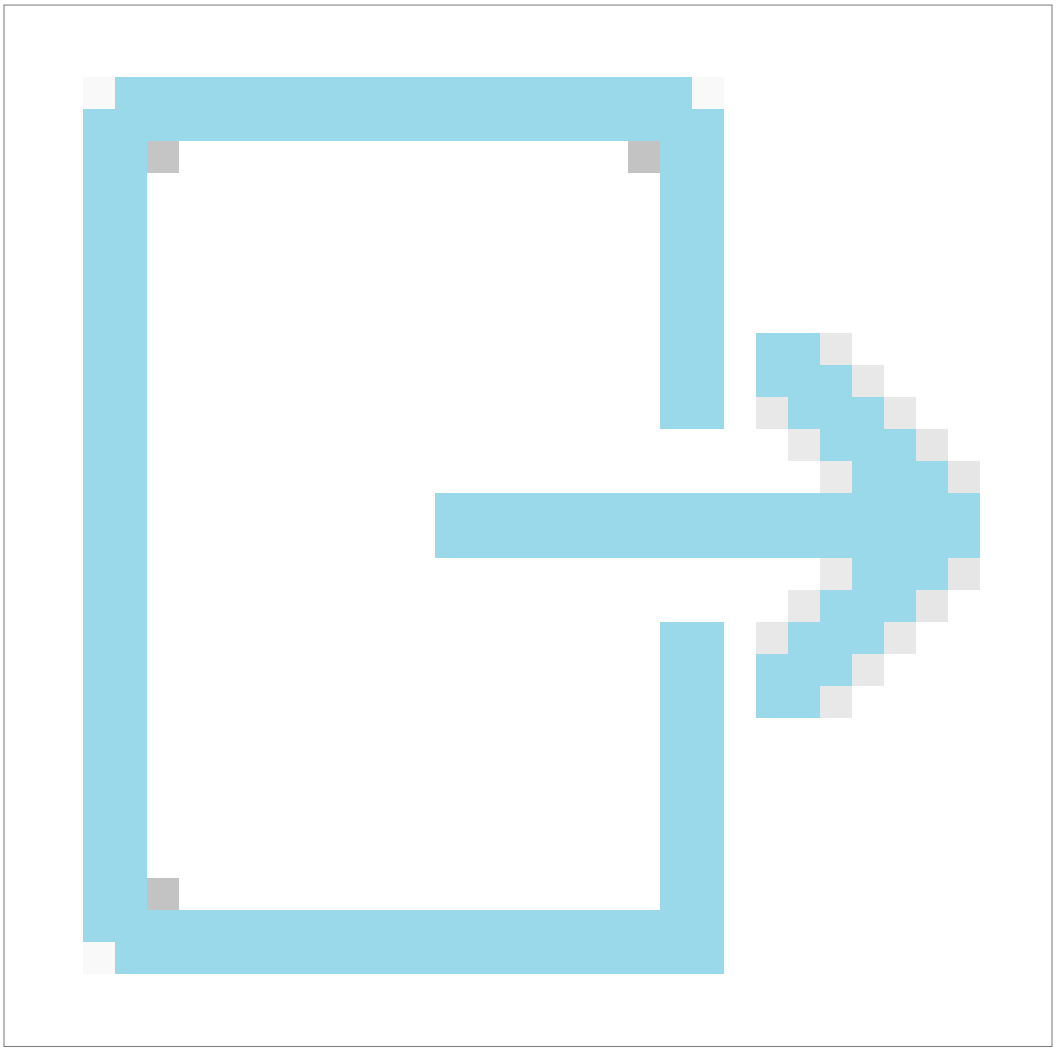
Artikel 13. : Benchmarking

15.1 Absatz 1

Bis zum 13 Juni 2025 erstellt die ACER in Zusammenarbeit mit der ENISA einen unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit. In dem Leitfaden für die NRB werden die Grundsätze des Benchmarkings der durchgeführten Cybersicherheitskontrollen gemäß Absatz 2 erläutert, wobei die Kosten für die Durchführung der Kontrollen und die Wirksamkeit von Prozessen, Produkten, Diensten, Systemen und Lösungen, die zur Durchführung dieser Kontrollen genutzt werden, zu berücksichtigen sind. Die ACER berücksichtigt bei der Erstellung des unverbindlichen Leitfadens für das Benchmarking im Bereich der Cybersicherheit vorhandene Benchmarking-Berichte. Die ACER übermittelt den unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit den NRB zur Information.

Relevante NCCS-Artikel

- Artikel 13 (2)



Output

- Unverbindliche Leitlinien zum Cybersicherheits-Benchmarking

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Juni 2025

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ACER, ENISA

Zu informieren: NRA

15.2 Absatz 2

Innerhalb von 12 Monaten nach Erstellung des Benchmarking-Leitfadens gemäß Absatz 1 führen die NRB eine Benchmarking-Analyse durch, um zu bewerten, ob die aktuellen Investitionen in die Cybersicherheit

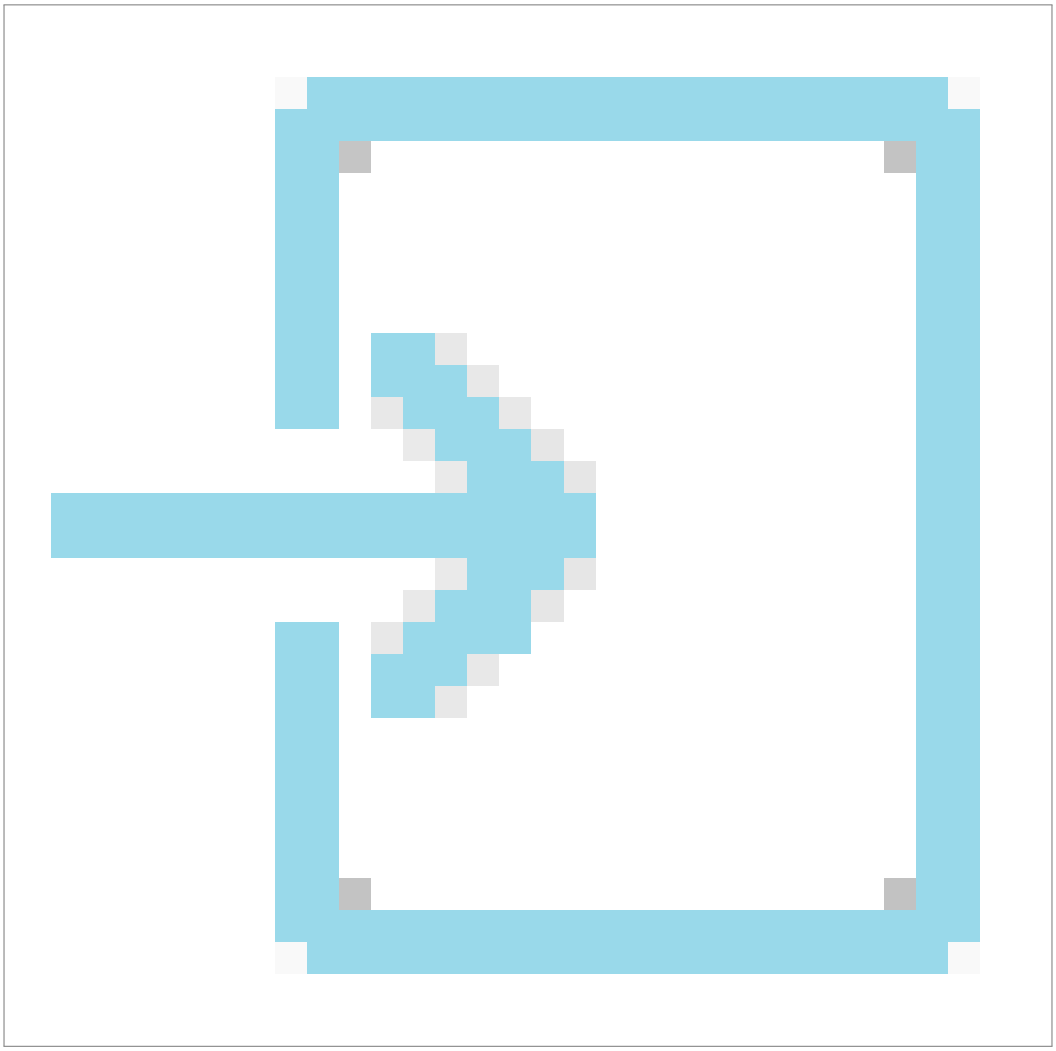
a. Risiken mit Auswirkungen auf grenzüberschreitende Stromflüsse mindern;

b. zu den gewünschten Ergebnissen führen und die Effizienz bei der Entwicklung des Elektrizitätssystems verbessern;

c. effizient sind und in die allgemeine Auftragsvergabe für Vermögenswerte und Dienstleistungen integriert werden.

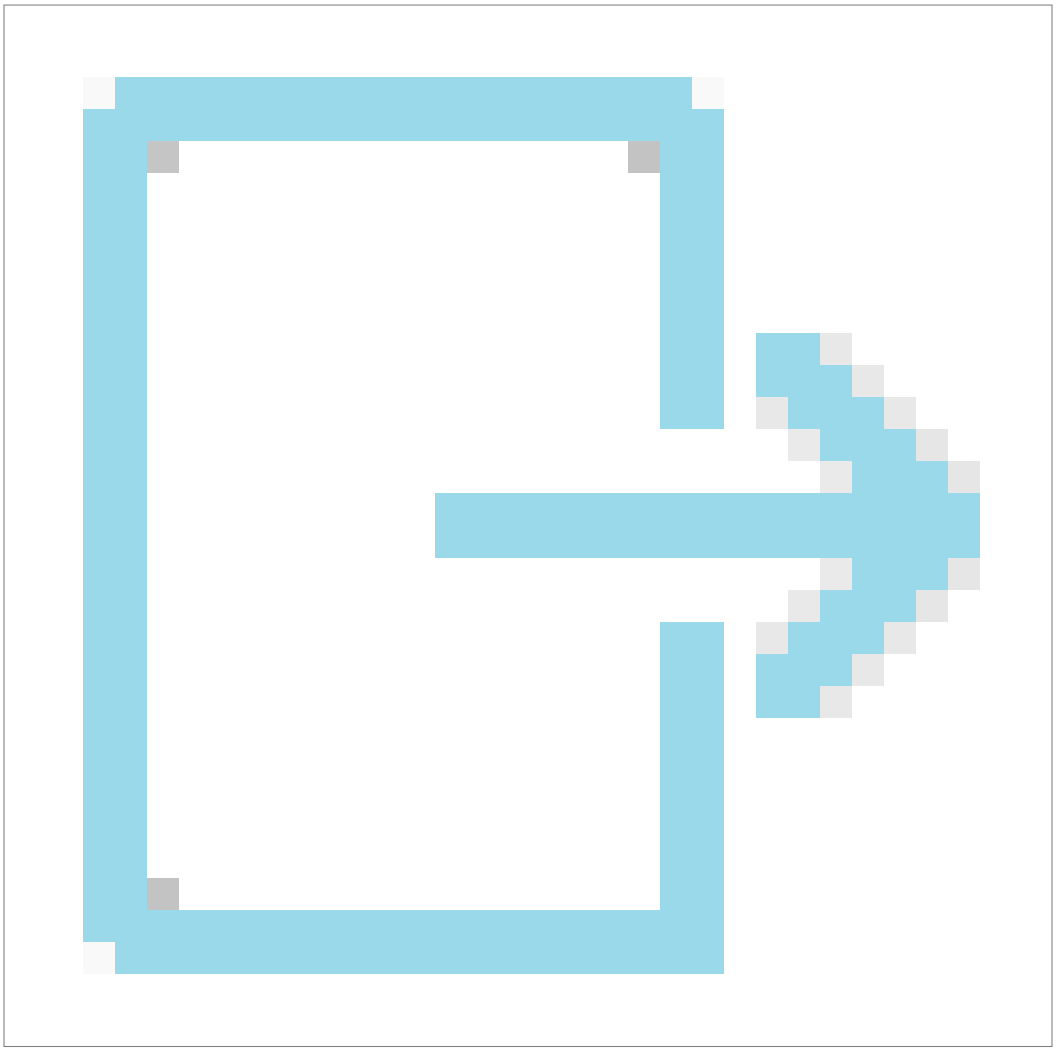
Relevante NCCS-Artikel

- Artikel 13 (1)



Input

- Unverbindliche Leitlinien zum Cybersicherheits-Benchmarking



Output

- Benchmarking Analyse

GOOD TO KNOW

Zeitpunkt

By 13 June 2026

Verantwortlich für die Aktivität: NRA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NRA

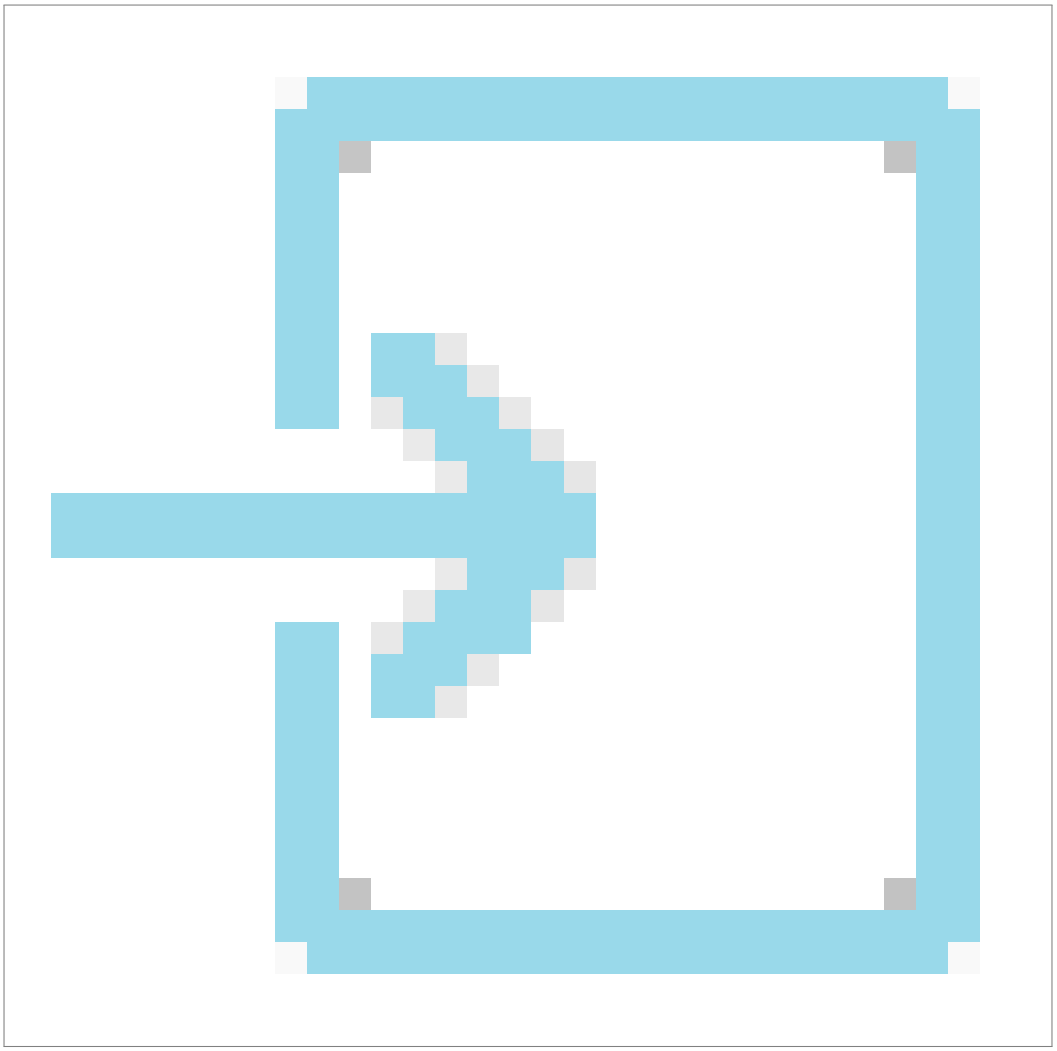
15.3 Absatz 3

Bei der Benchmarking-Analyse können die NRB den von der ACER erstellten unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit berücksichtigen, wobei sie insbesondere Folgendes bewerten:

a. die durchschnittlichen Ausgaben für die Cybersicherheit zur Minderung von Risiken, die sich auf grenzüberschreitende Stromflüsse auswirken, insbesondere bei Einrichtungen mit erheblichen oder kritischen Auswirkungen;

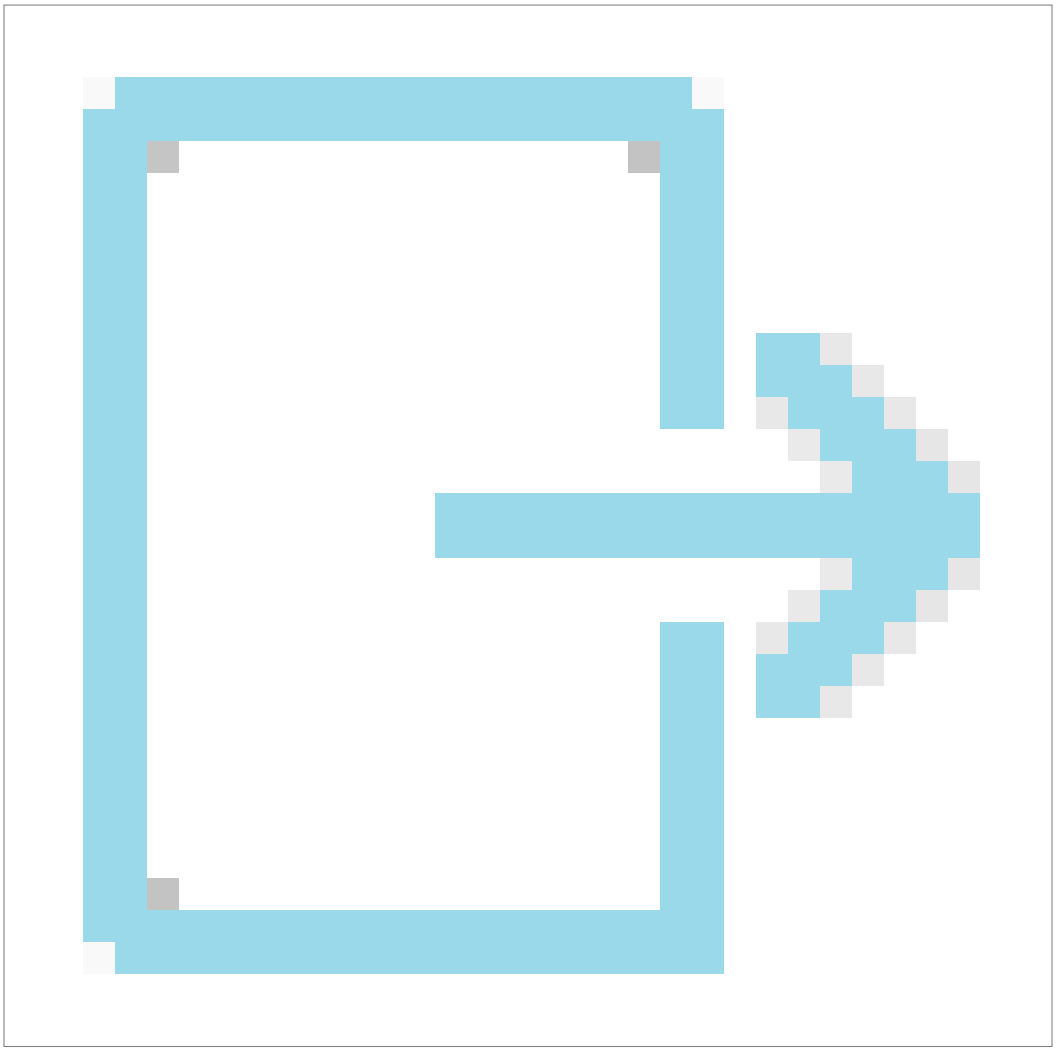
b. in Zusammenarbeit mit ENTSO-E und der EU-VNBO die Durchschnittspreise für Cybersicherheitsdienste, -systeme und -produkte, die in hohem Maß zur Verbesserung und Aufrechterhaltung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit in den verschiedenen Netzbetriebsregionen beitragen;

c. das Vorhandensein von Cybersicherheitsdiensten, -systemen und -lösungen, die sich für die Durchführung dieser Verordnung eignen, sowie die Vergleichbarkeit der damit verbundenen Kosten und Funktionen, wobei sie mögliche Maßnahmen ermitteln, die zur Verbesserung der Effizienz der Ausgaben erforderlich sind, insbesondere wenn Investitionen in die Cybersicherheitstechnik erforderlich sein könnten.



Input

- Unverbindliche Leitlinien zum Cybersicherheits-Benchmarking



Output

- Benchmarking Analyse

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Juni 2026

Verantwortlich für die Aktivität: NRA

Beteiligte Stakeholder:

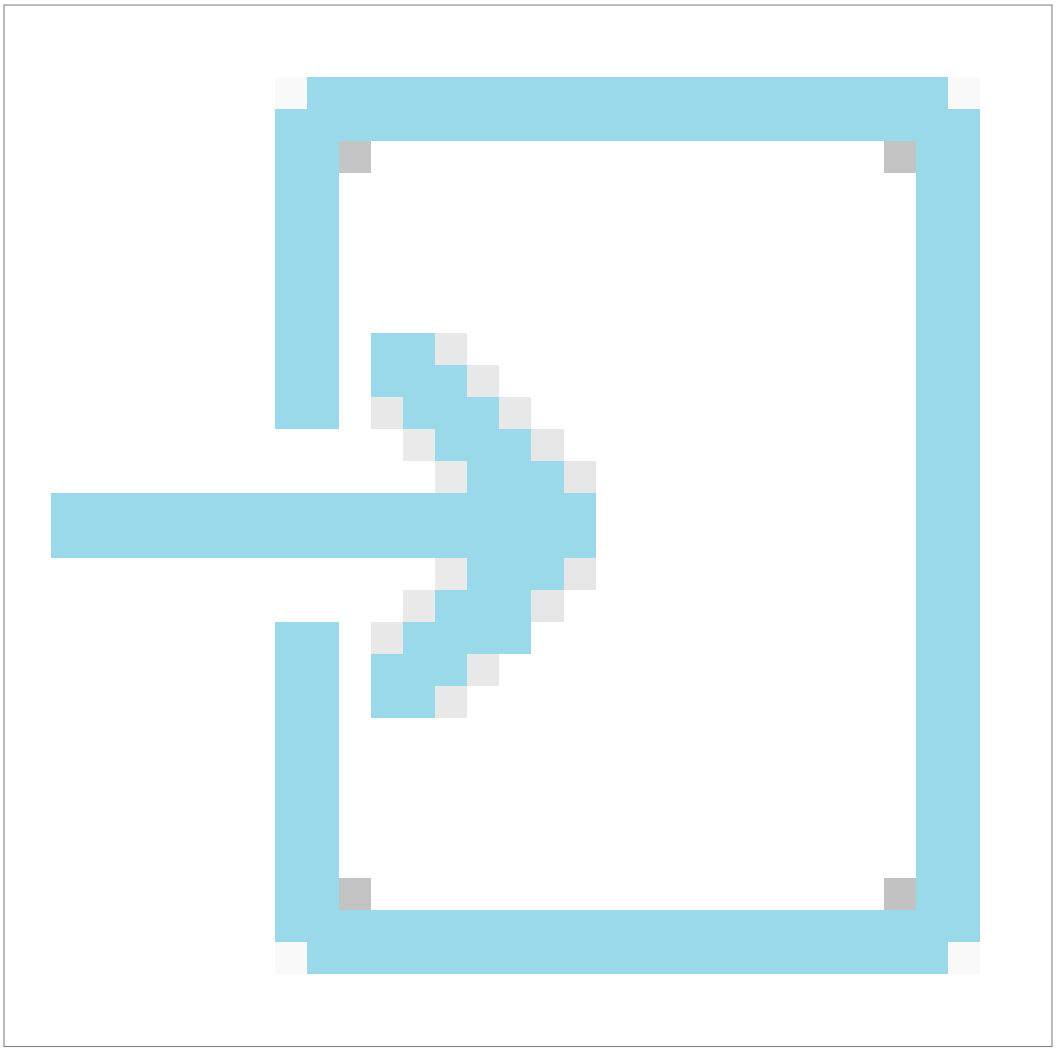
Beteiligt an der Aufgabenausführung: ENTSO-E, ACER, EU DSO, NRA

15.4 Absatz 4

Alle Informationen zu Benchmarking-Analysen werden gemäß den Anforderungen dieser Verordnung an dieDatenklassifizierung, die Mindest-Cybersicherheitskontrollen und den Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gehandhabt und verarbeitet. Die in den Absätzen 2 und 3 genannte Benchmarking-Analyse wird nicht veröffentlicht.

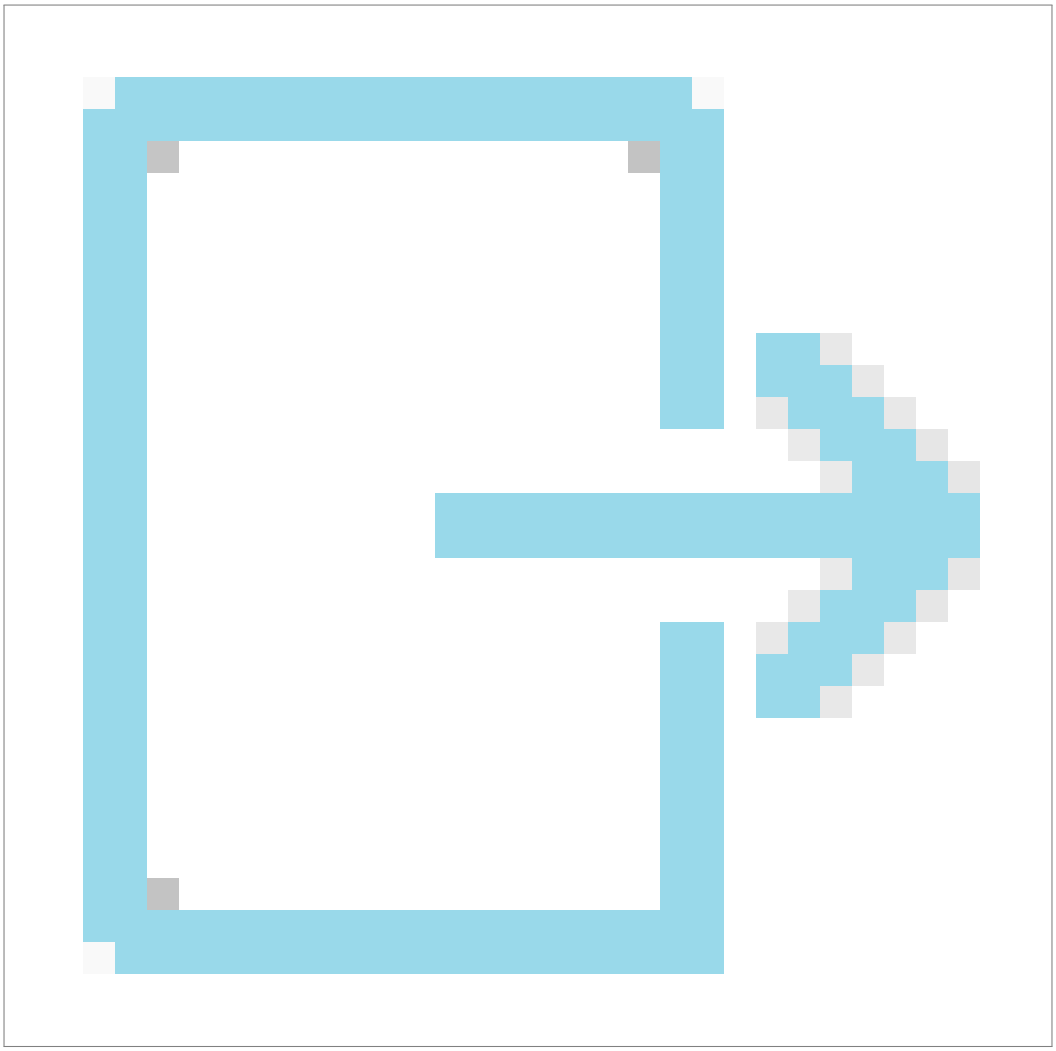
Relevante NCCS-Artikel

- Artikel 13 (2)
- Artikel 13 (3)



Input

- Cybersicherheitskontrollen



Output

- Benchmarking Analyse

A

Verantwortlich für die Aktivität: NRA

Beteiligte Stakeholder:

R

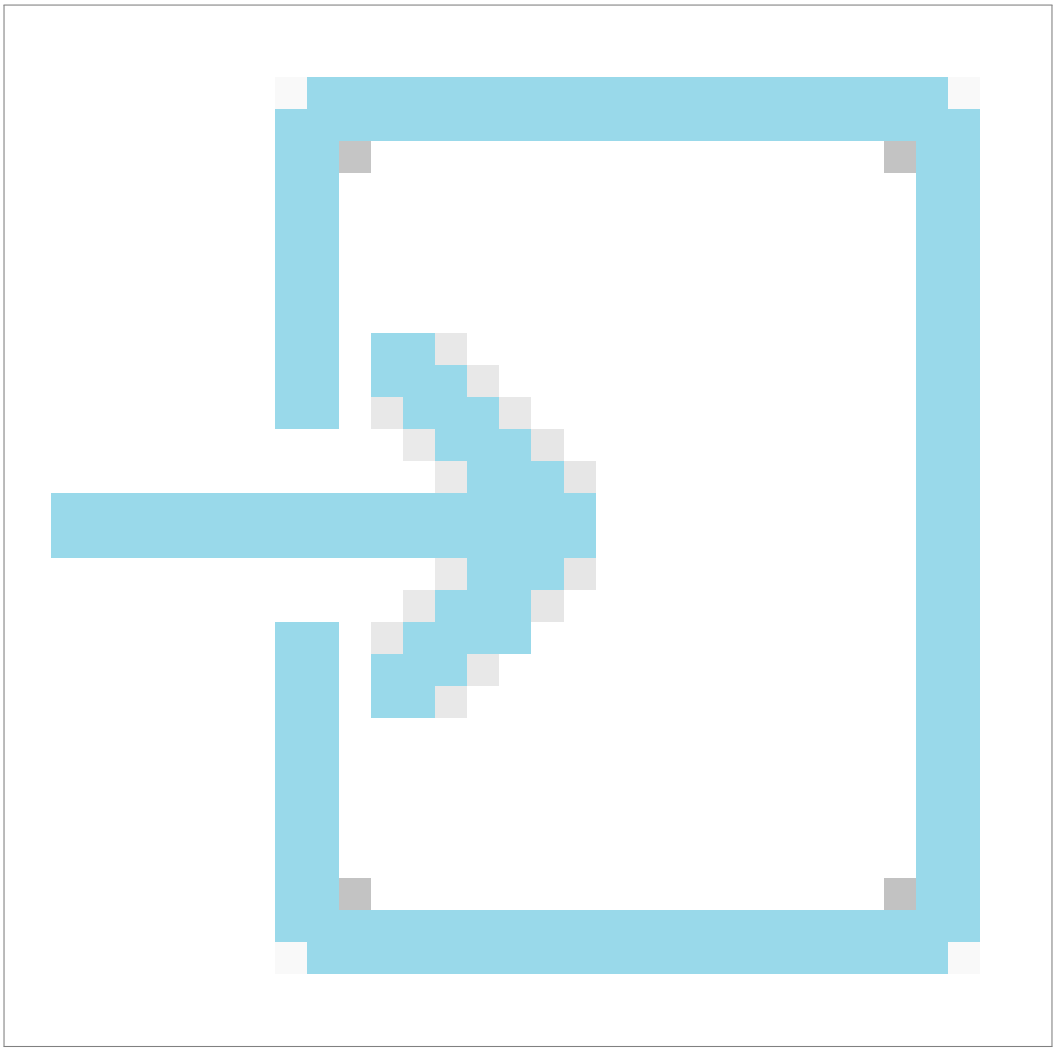
Beteiligt an der Aufgabenausführung: ENTSO-E, ACER, EU DSO, NRA

15.5 Absatz 5

Unbeschadet der Vertraulichkeitsbestimmungen in Artikel 47 und der Notwendigkeit, die Sicherheit von Einrichtungen zu schützen, die den Bestimmungen dieser Verordnung unterliegen, wird die in den Absätzen 2 und 3 dieses Artikels genannte Benchmarking-Analyse allen NRB, allen zuständigen Behörden, der ACER, der ENISA und der Kommission übermittelt.

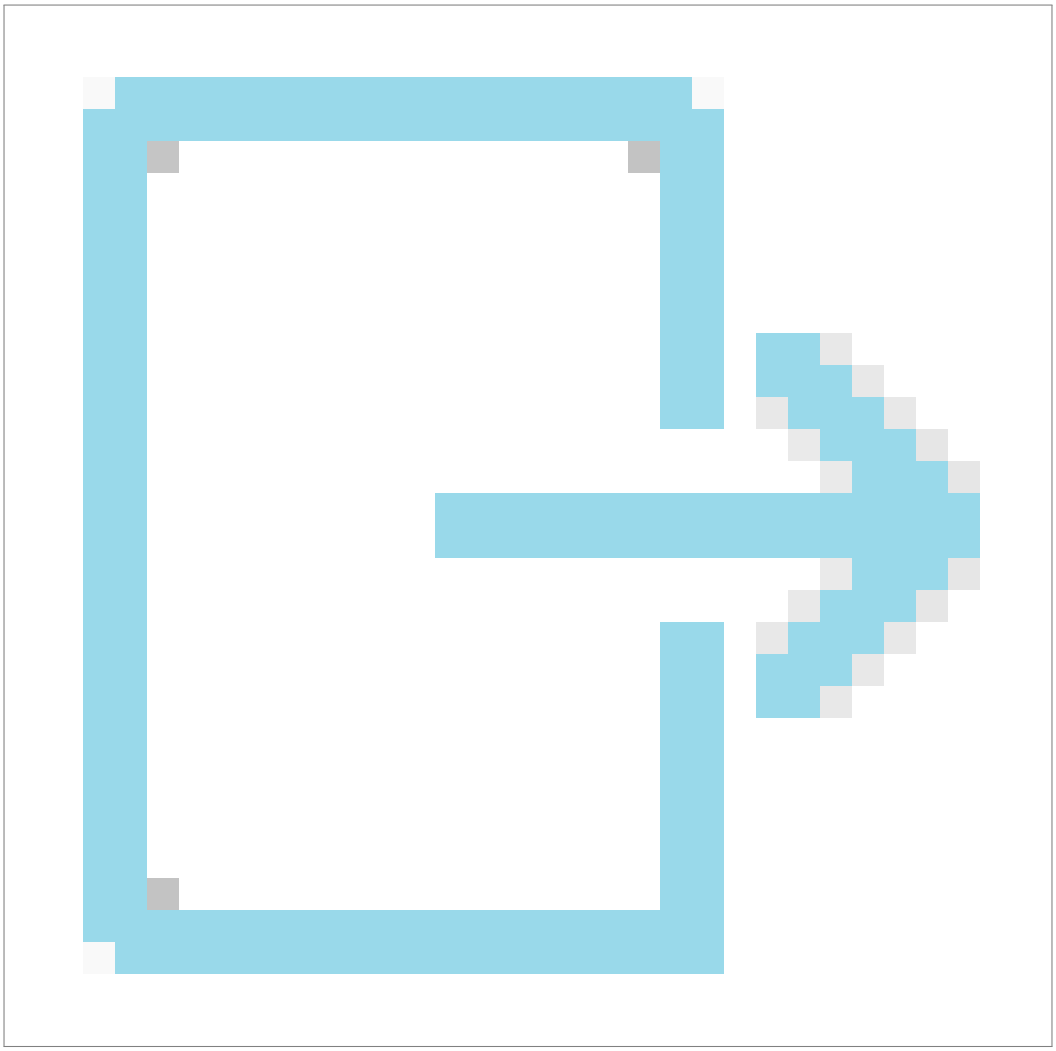
Relevante NCCS-Artikel

- Artikel 13 (2)
- Artikel 13 (3)
- Artikel 47



Input

- Cybersicherheitskontrollen
- Richtlinie zum Informationsaustausch



Output

- Benchmarking Analyse

A

Verantwortlich für die Aktivität: NRA

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: NRA

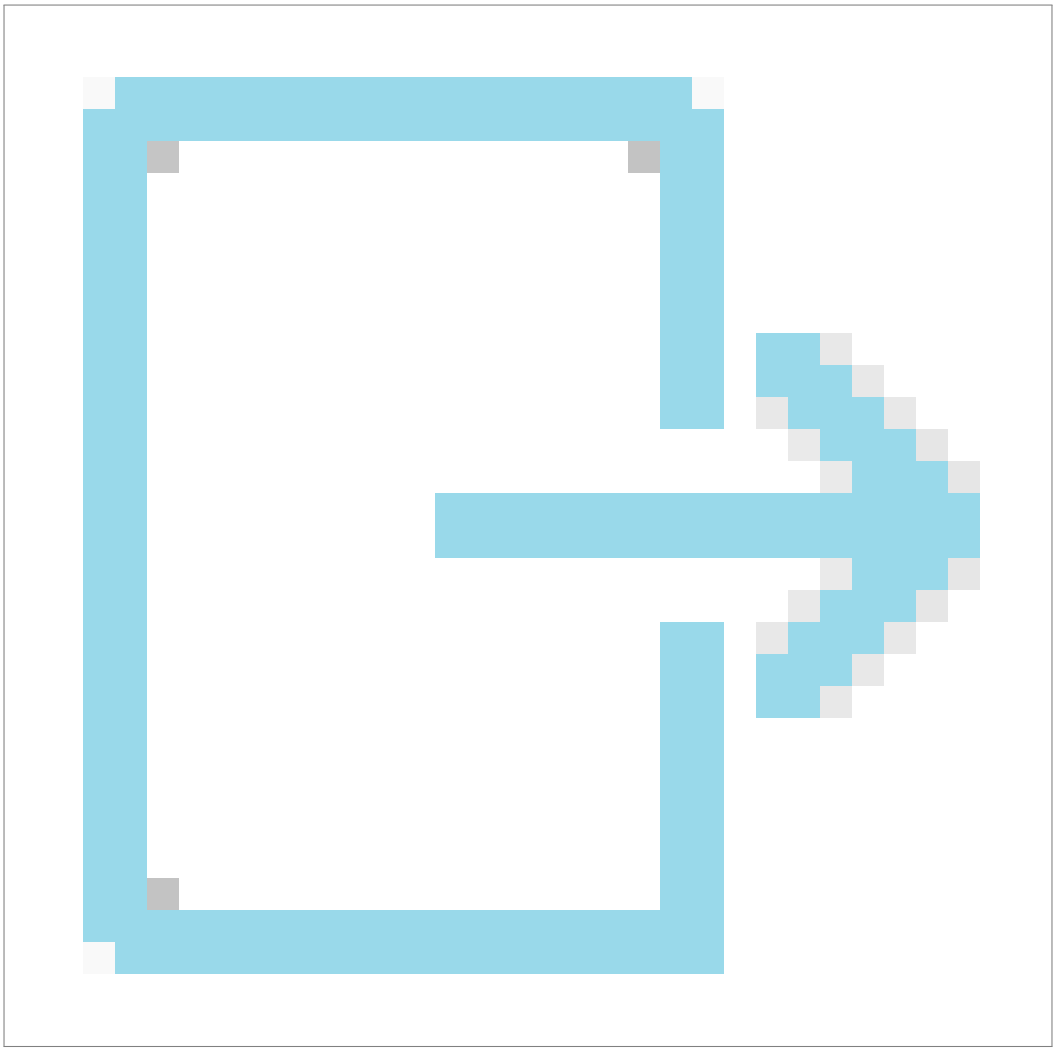
Zu informieren: EC, ACER, ENISA

Chapter 16

Artikel 14. : Vereinbarungen mit ÜNB von Drittländern

16.1 Absatz 1

Innerhalb von 18 Monaten nach dem Inkrafttreten dieser Verordnung bemühen sich die ÜNB einer Netzbetriebsregion, die an ein Drittland angrenzt, um den Abschluss von Vereinbarungen mit ÜNB des benachbarten Drittlands, die mit dem einschlägigen Unionsrecht im Einklang stehen, die Grundlage für die Zusammenarbeit zum Cybersicherheitsschutz bilden und Regelungen für die Zusammenarbeit mit diesen ÜNB im Bereich der Cybersicherheit enthalten.



Output

- Vereinbarung mit den benachbarten Übertragungsnetzbetreibern

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Dezember 2025

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: TSO

16.2 Absatz 2

Die ÜNB unterrichten die zuständige Behörde über die gemäß Absatz 1 geschlossenen Vereinbarungen.

Relevante NCCS-Artikel

- Artikel 14 (1)

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: TSO

Zu informieren: NCA

Chapter 17

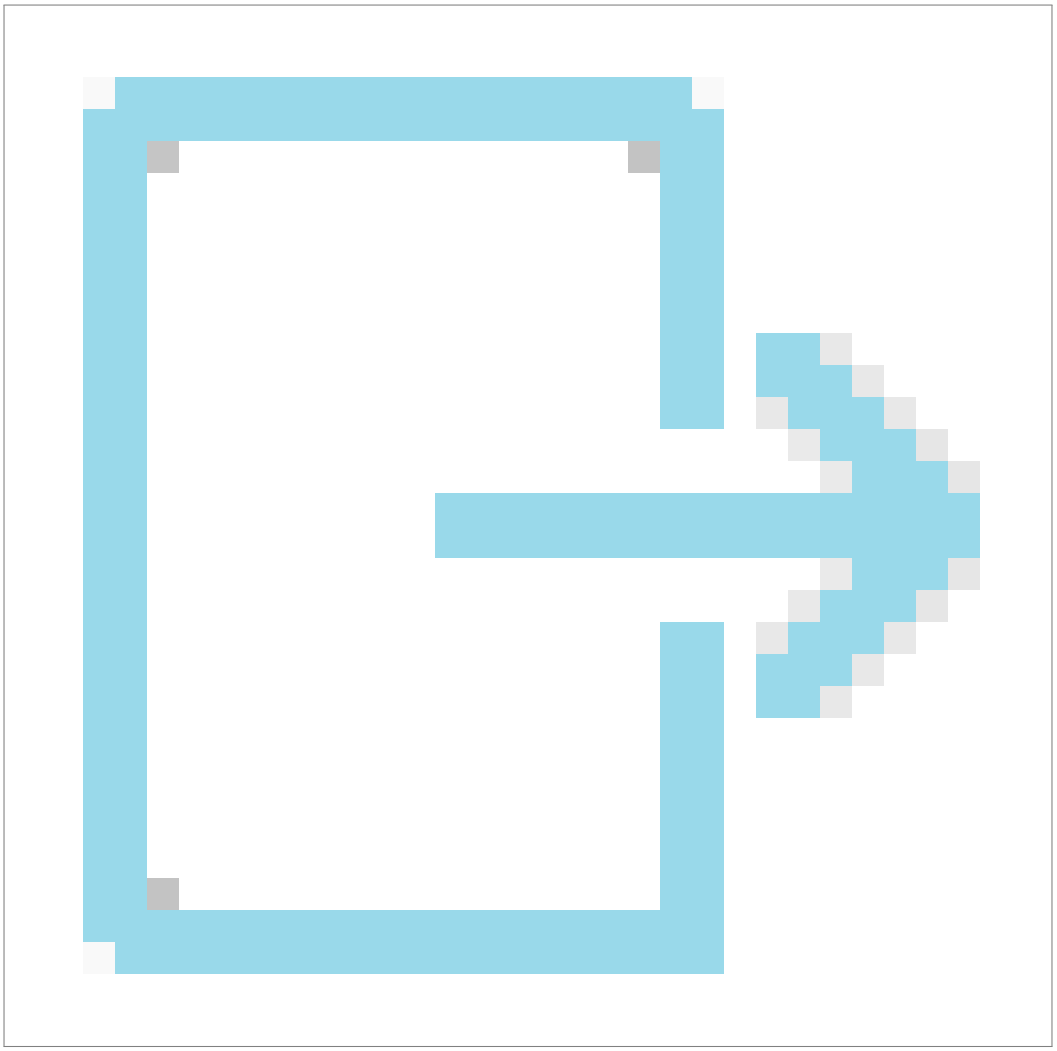
Artikel 15. : Gesetzlicher Vertreter

17.1 Absatz 1

Einrichtungen, die keine Niederlassung in der Union haben, aber Dienstleistungen für Einrichtungen in der Union erbringen und gemäß Artikel 24 Absatz 6 über ihren Status als Einrichtungen mit erheblichen oder kritischen Auswirkungen unterrichtet wurden, benennen innerhalb von drei Monaten nach der Unterrichtung schriftlich einen Vertreter in der Union und informieren die zuständige Behörde entsprechend.

Relevante NCCS-Artikel

- Artikel 24 (6)



Output

- Ernennung eines Rechtsvertreters

GOOD TO KNOW

Zeitpunkt

Bis zum 13. September 2028

Verantwortlich für die Aktivität: HIE, CIE, TSO

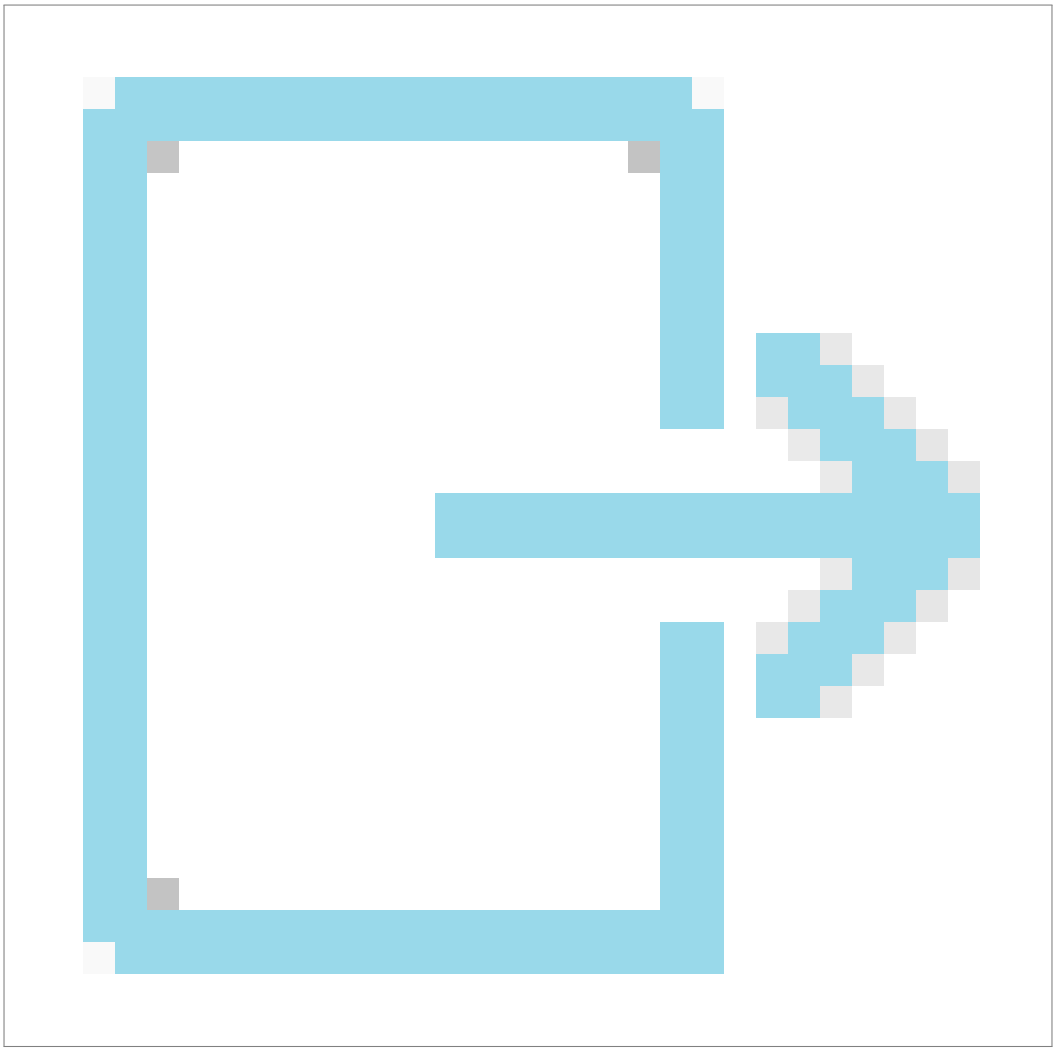
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Zu informieren: NCA

17.2 Absatz 2

Dieser Vertreter wird beauftragt, zusätzlich zu oder anstelle der Einrichtung mit erheblichen oder kritischen Auswirkungen als Ansprechpartner zu fungieren, an den sich jede zuständige Behörde und jedes CSIRT in der Union in Bezug auf die Verpflichtungen der Einrichtung aus dieser Verordnung wenden kann. Die Einrichtung mit erheblichen oder kritischen Auswirkungen stattet ihren gesetzlichen Vertreter mit den erforderlichen Befugnissen und ausreichenden Ressourcen aus, um eine effiziente und rechtzeitige Zusammenarbeit mit den jeweils zuständigen Behörden oder CSIRTs zu gewährleisten.



Output

- Ernennung eines Rechtsvertreters in der EU

A

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Zu informieren: NCA

17.3 Absatz 3

Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Einrichtung ihre Dienste anbietet. Die Einrichtung gilt als der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegend, in dem der Vertreter niedergelassen ist. Einrichtungen mit erheblichen oder kritischen Auswirkungen melden der zuständigen Behörde des Mitgliedstaats, in dem ihr gesetzlicher Vertreter ansässig oder niedergelassen ist, den Namen, die Postanschrift, die E-Mail-Adresse und die Telefonnummer des gesetzlichen Vertreters.

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Zu informieren: NCA

17.4 Absatz 4

Der benannte gesetzliche Vertreter kann für Verstöße gegen Pflichten aus dieser Verordnung haftbar gemacht werden; dies berührt nicht die Haftung und die rechtlichen Schritte,

die gegen die Einrichtung mit erheblichen oder kritischen Auswirkungen eingeleitet werden können.

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

17.5 Absatz 5

Wurde in der Union kein Vertreter im Sinne dieses Artikels benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienstleistungen erbringt, gegen die Einrichtung rechtliche Schritte wegen Verstößen gegen Pflichten aus dieser Verordnung einleiten.

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

17.6 Absatz 6

Die Benennung eines gesetzlichen Vertreters in der Union gemäß Absatz 1 gilt nicht als Niederlassung in der Union.

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Chapter 18

Artikel 16. : Zusammenarbeit zwischen ENTSO-E und der EU-VNBO

18.1 Absatz 1

ENTSO-E und die EU-VNBO arbeiten bei der Durchführung der Bewertungen des Cybersicherheitsrisikos gemäß Artikel 19 und Artikel 21 zusammen, insbesondere bei den folgenden Aufgaben:

a. Entwicklung der Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 18 Absatz 1;

b. Erstellung des umfassenden Berichts über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23;

c. Entwicklung des gemeinsamen Rahmens für die Cybersicherheit im Elektrizitätssektor gemäß Kapitel III;

d. Erstellung der Empfehlung für die Cybersicherheit bei der Auftragsvergabe gemäß Artikel 35;

e. Entwicklung der Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8;

f. Entwicklung des vorläufigen Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor (ECII) gemäß Artikel 48 Absatz 1 Buchstabe a;

g. Erstellung der konsolidierten vorläufigen Liste der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 48 Absatz 3;

h. Erstellung der vorläufigen Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen gemäß Artikel 48 Absatz 4;

i. Erstellung der vorläufigen Liste europäischer und internationaler Normen und Kontrollen gemäß Artikel 48 Absatz 6;

j. Durchführung der unionsweiten Bewertung des Cybersicherheitsrisikos gemäß Artikel 19;

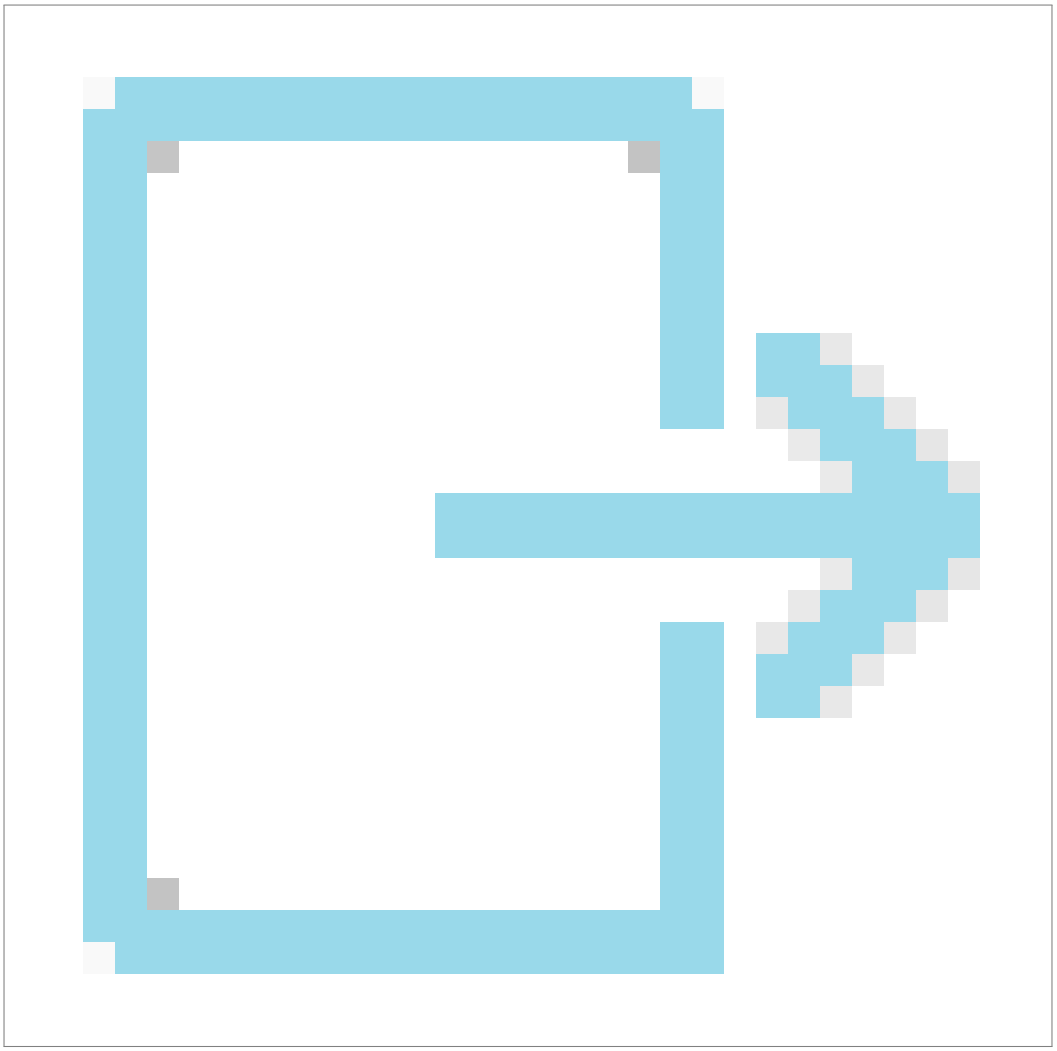
k. Durchführung der regionalen Bewertung des Cybersicherheitsrisikos gemäß Artikel 21;

l. Festlegung der regionalen Pläne zur Minderung des Cybersicherheitsrisikos gemäß Artikel 22;

m. Entwicklung von Leitlinien für europäische Schemata für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen gemäß Artikel 36;

Relevante NCCS-Artikel

- Artikel 19
- Artikel 21
- Artikel 18 (1)
- Artikel 23
- Artikel 35
- Artikel 37 (8)
- Artikel 48 (1)
- Artikel 48 (3)
- Artikel 48 (4)
- Artikel 48 (6)
- Artikel 22
- Artikel 36



Output

- Methoden zur Bewertung von Cybersicherheitsrisiken
- Umfassender Bericht zur Bewertung von Cybersicherheitsrisiken für den Elektrizitätssektor
- Gemeinsames Cybersicherheits-Rahmenwerk für den Elektrizitätssektor
- Empfehlung zur Beschaffung von Cybersicherheitslösungen
- Methodik zur Klassifizierung von Cyberangriffen
- Vorläufige ECII
- Vorläufige Liste identifizierter Organisationen
- Vorläufige Liste EU-weiter Prozesse mit erheblicher und kritischer Auswirkung

- Vorläufige Liste europäischer und internationaler Normen
- Bericht zur Bewertung der Cybersicherheitsrisiken auf EU-Ebene
- Bericht zur Bewertung der Cybersicherheitsrisiken auf regionaler Ebene
- Regionale Pläne zur Minderung von Cybersicherheitsrisiken
- Leitlinien zu Cybersicherheits-Zertifizierungssystemen
- Leitlinien zur Umsetzung

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

18.2 Absatz 1

n) Entwicklung von Leitlinien für die Durchführung dieser Verordnung, in Absprache mit der ACER und der ENISA.

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu konsultieren: ACER, ENISA

18.3 Absatz 2

Die Zusammenarbeit zwischen ENTSO-E und der EU-VNBO kann über eine Arbeitsgruppe für Cybersicherheitsrisiken erfolgen.

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

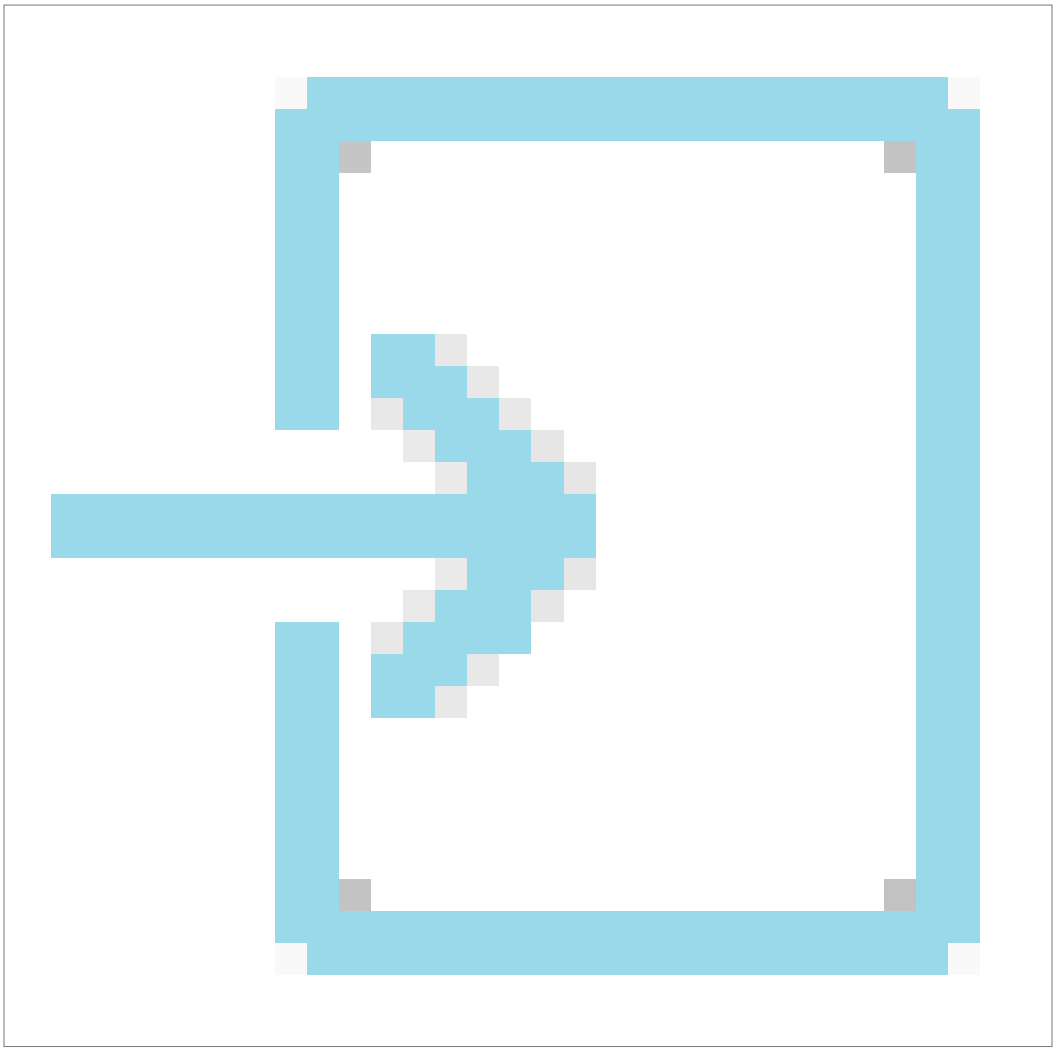
Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

18.4 Absatz 3

ENTSO-E und die EU-VNBO unterrichten die ACER, die ENISA, die NIS-Kooperationsgruppe und die Koordinierungsgruppe „Strom“ regelmäßig über die Fortschritte bei der Umsetzung der unionsweiten und regionalen Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 und Artikel 21.

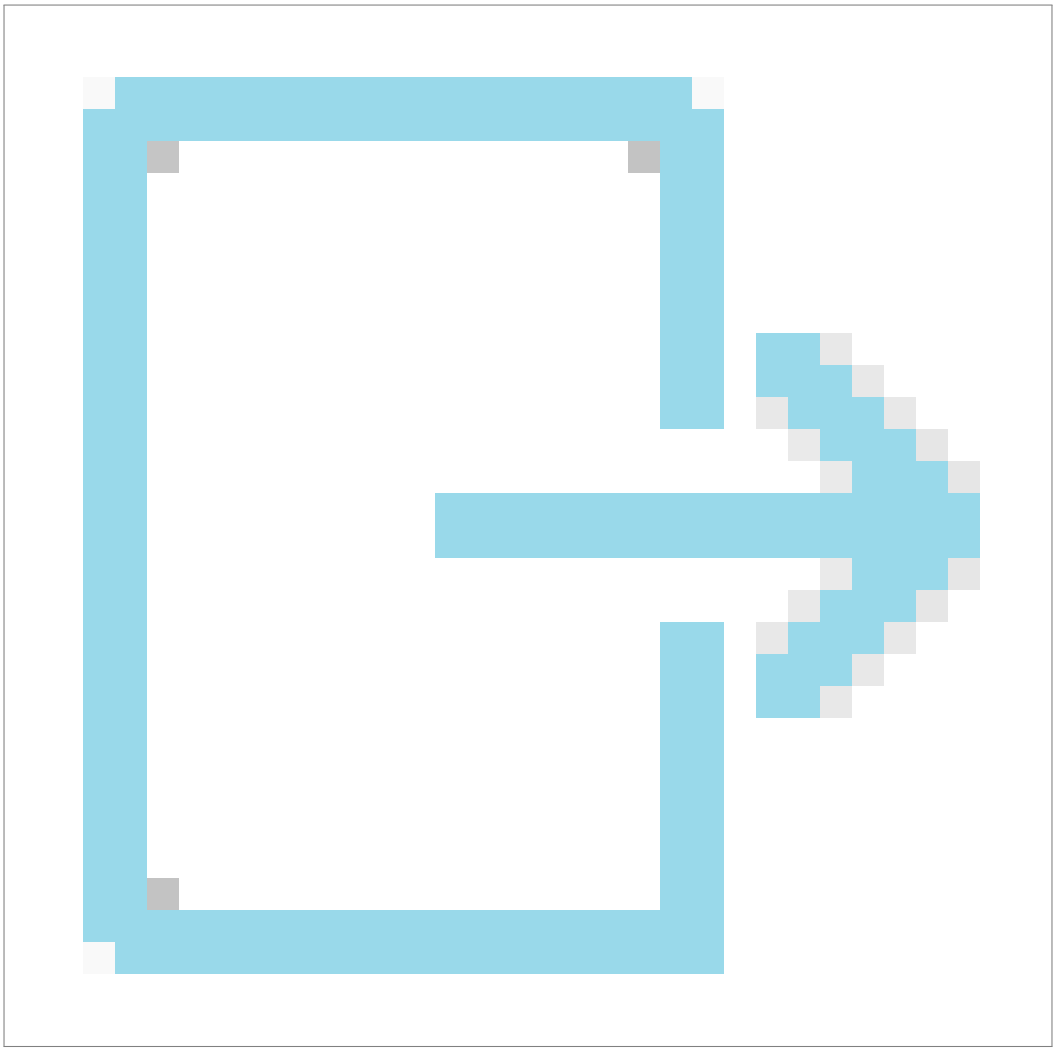
Relevante NCCS-Artikel

- Artikel 19
- Artikel 21



Input

- Unionweiter Risikobewertungsbericht
- Regionaler Risikobewertungsbericht



Output

- Unionweiter Risikobewertungsbericht
- Regionaler Risikobewertungsbericht

A

Verantwortlich für die Aktivität: ENTSO-E, EU DSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu informieren: ACER, ENISA, NIS CG, ECG

Chapter 19

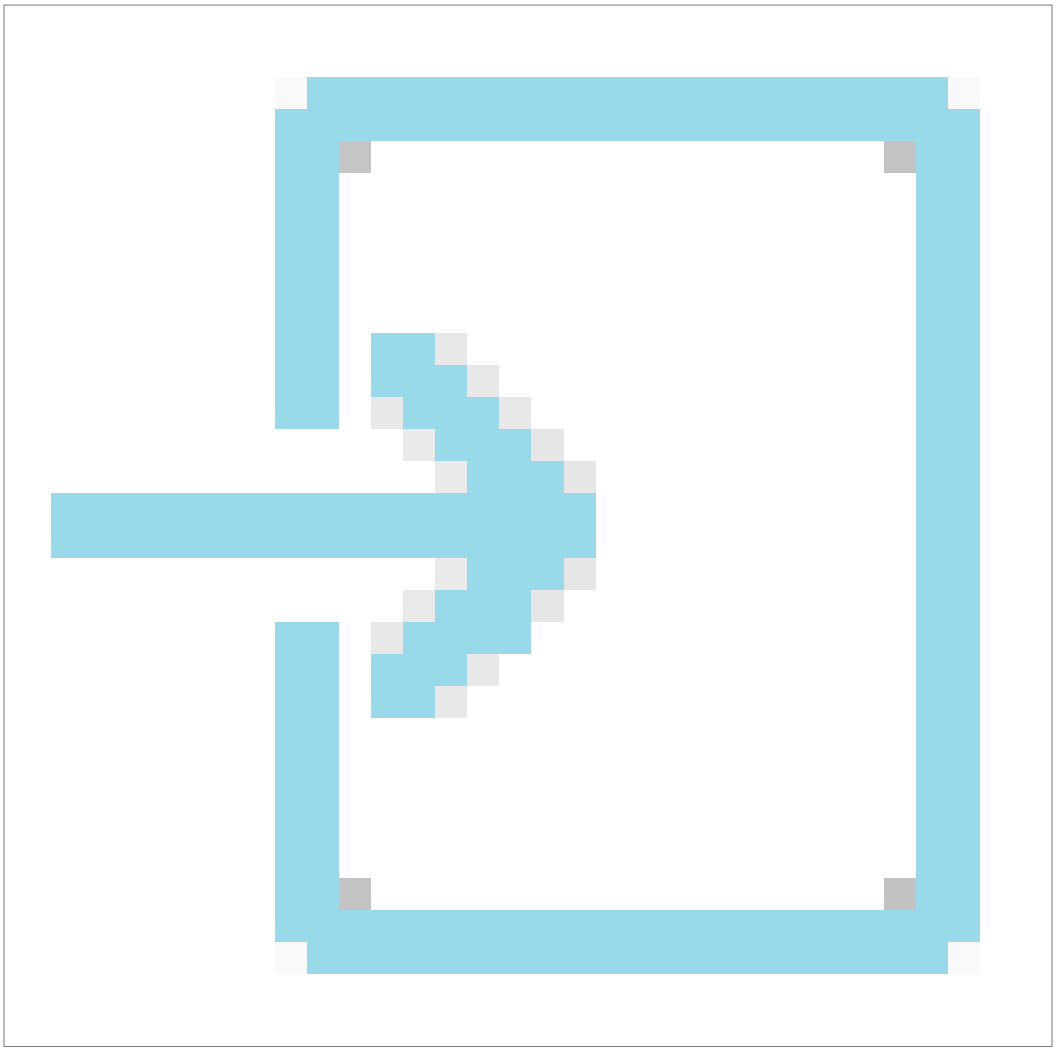
Artikel 17. : Zusammenarbeit zwischen der ACER und den zuständigen Behörden

19.1 Absatz 1

Die ACER überwacht in Zusammenarbeit mit jeder zuständigen Behörde (1) die Umsetzung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit gemäß Artikel 12 Absatz 2 Buchstabe a und der Berichterstattungspflichten gemäß den Artikeln 27 und 39 sowie

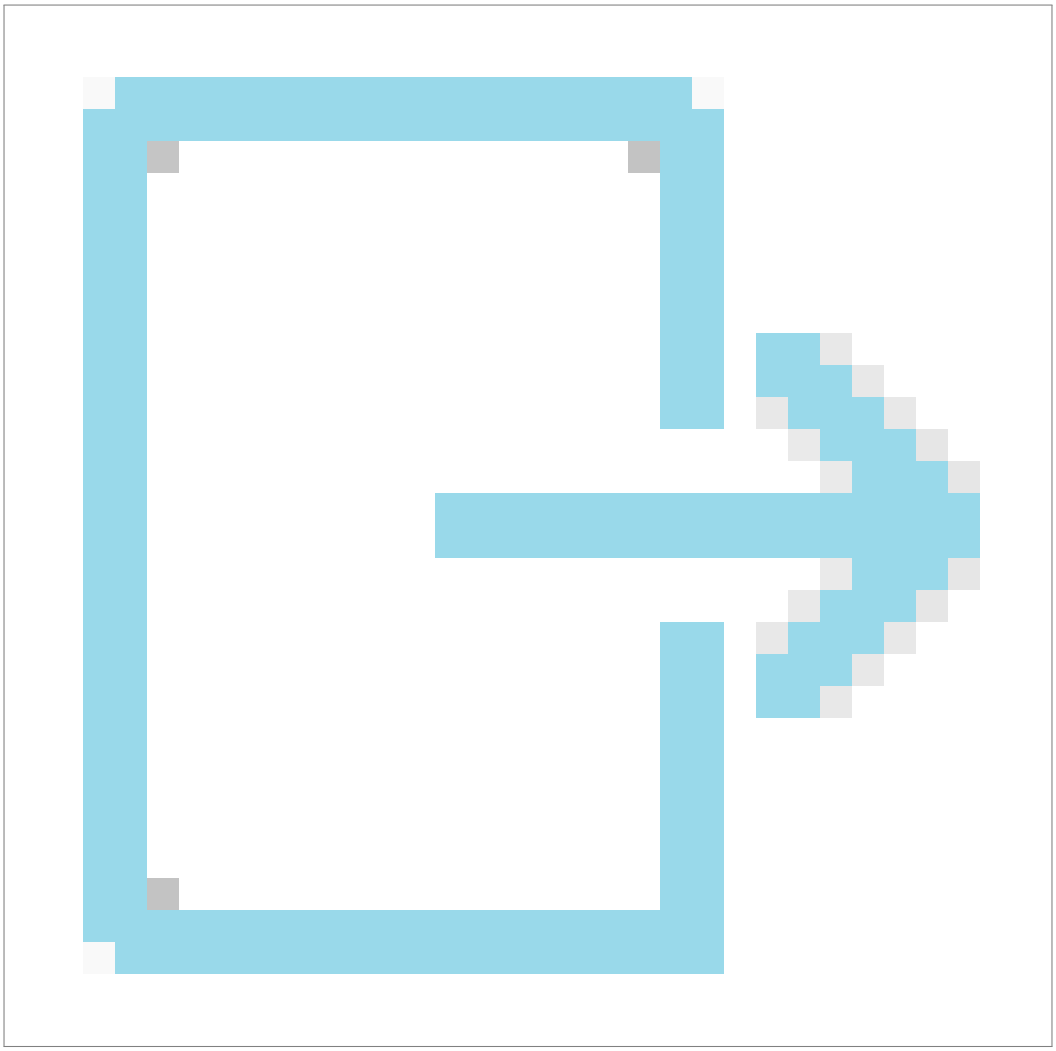
Relevante NCCS-Artikel

- Artikel 12 (2)
- Artikel 27
- Artikel 39



Input

- ACER-Überwachungsbericht
- Risikobewertungsbericht der Mitgliedstaaten
- Informationsaustausch über Cyberangriffe



Output

- ACER-Überwachungsbericht

A

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

R

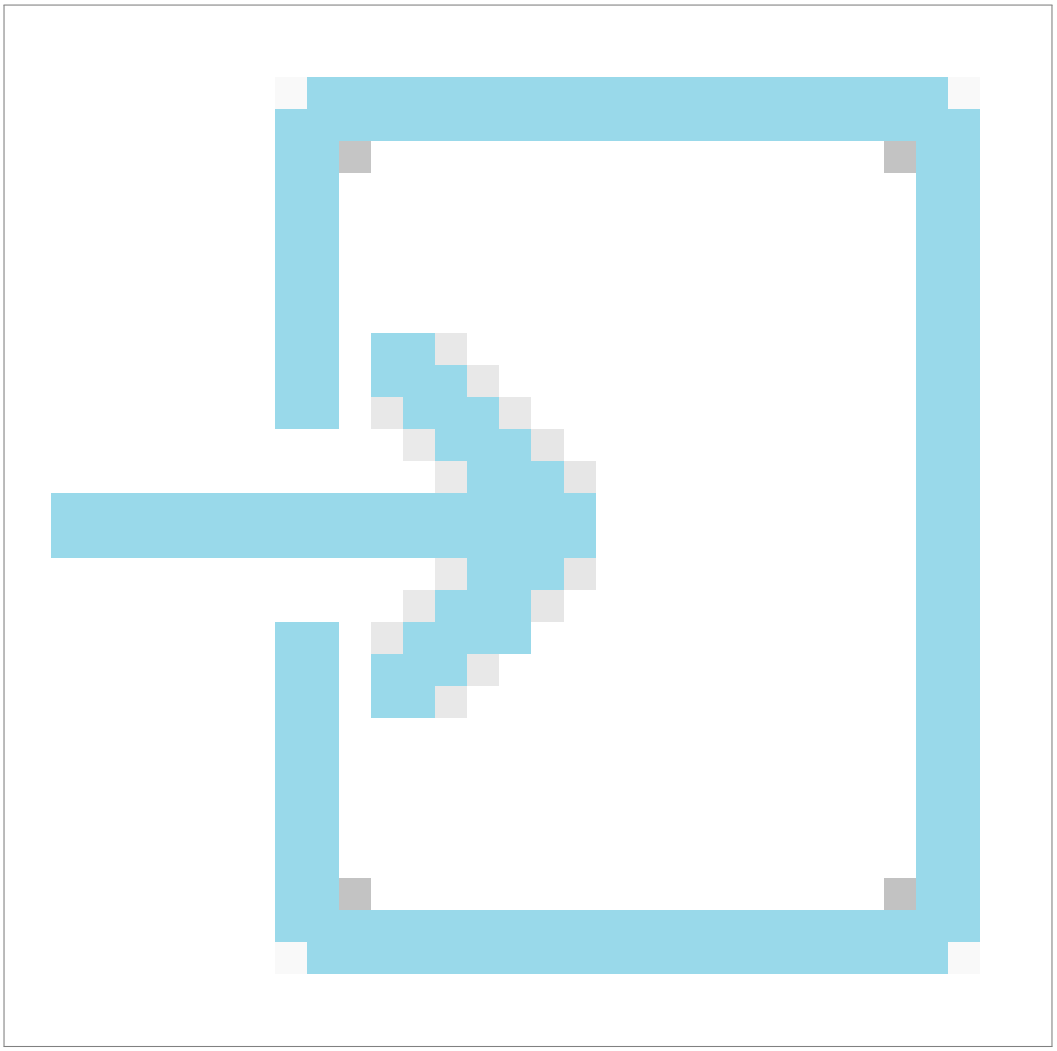
Beteiligt an der Aufgabenausführung: ACER

19.2 Absatz 1

(2) das Verfahren zur Annahme der Modalitäten, Methoden oder Pläne gemäß Artikel 6 Absätze 2 und 3 und deren Umsetzung. Die Zusammenarbeit zwischen der ACER, der ENISA und jeder zuständigen Behörde kann über ein Gremium zur Überwachung von Cybersicherheitsrisiken erfolgen.

Relevante NCCS-Artikel

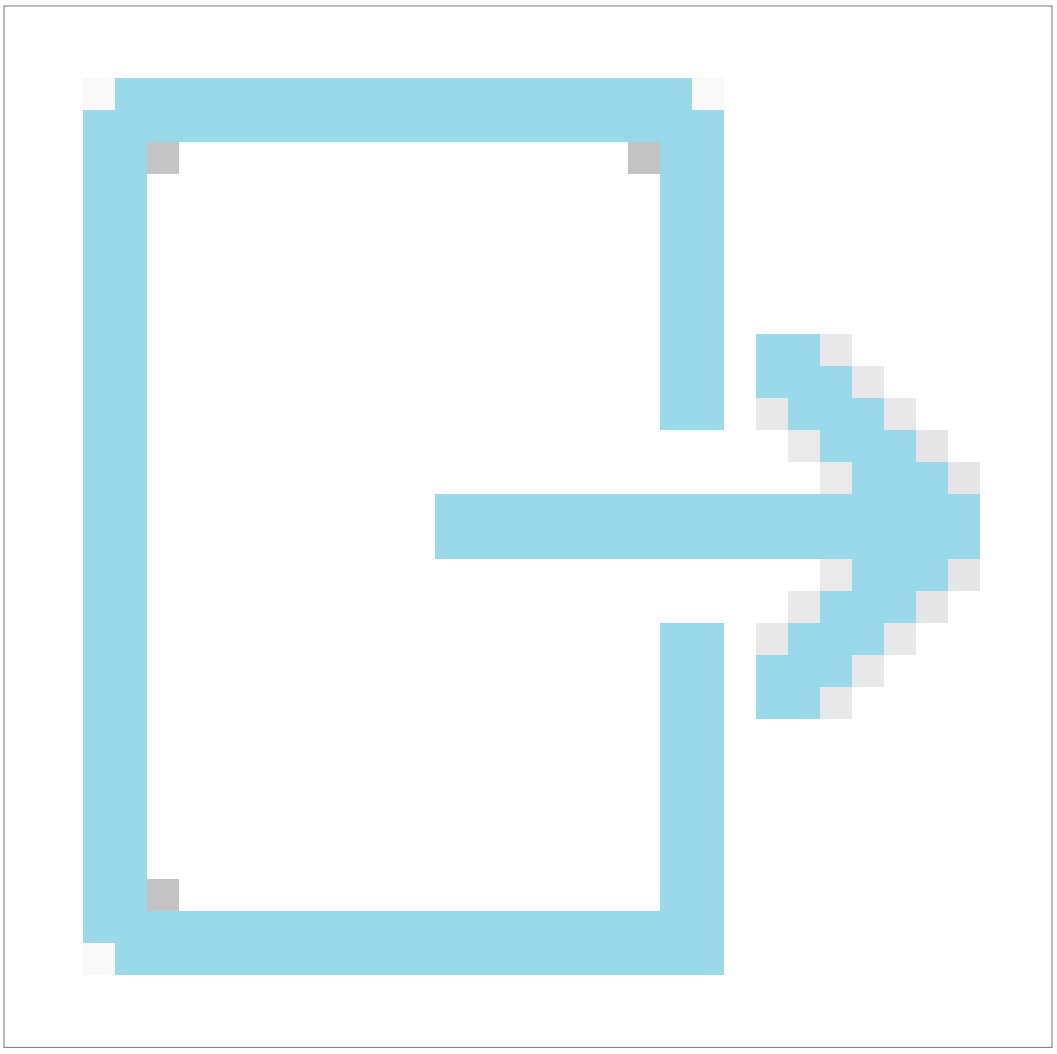
- Artikel 6 (2)
- Artikel 6 (3)



Input

- Methoden zur Bewertung von Cybersicherheitsrisiken (Entwurf)
- Umfassender Bericht zur Bewertung von Cybersicherheitsrisiken für den Stromsektor (Entwurf)
- Gemeinsamer Cybersicherheitsrahmen für den Stromsektor (Entwurf)
- Empfehlung zur Beschaffung von Cybersicherheit (Entwurf)
- Methodik zur Klassifizierung von Cyberangriffen (Entwurf)
- Vorläufige ECII (Entwurf)
- Vorläufige Liste identifizierter Unternehmen (Entwurf)
- Vorläufige Liste der Prozesse mit erheblicher und kritischer Auswirkung in der EU (Entwurf)

- Vorläufige Liste der europäischen und internationalen Normen (Entwurf)
- Bericht zur Bewertung der Cybersicherheitsrisiken auf EU-Ebene (Entwurf)
- Regionaler Bericht zur Bewertung der Cybersicherheitsrisiken (Entwurf)
- Regionale Pläne zur Minderung der Cybersicherheitsrisiken (Entwurf)
- Leitlinien zu Cybersicherheits-Zertifizierungssystemen (Entwurf)
- Durchführungsleitlinien (Entwurf)



Output

- Methoden zur Bewertung von Cybersicherheitsrisiken (genehmigt)
- Umfassender Bericht zur Bewertung von Cybersicherheitsrisiken für den Stromsektor (genehmigt)

- Gemeinsamer Cybersicherheitsrahmen für den Stromsektor (genehmigt)
- Empfehlung zur Beschaffung von Cybersicherheit (genehmigt)
- Methodik zur Klassifizierung von Cyberangriffen (genehmigt)
- Vorläufige ECII (genehmigt)
- Vorläufige Liste identifizierter Unternehmen (genehmigt)
- Vorläufige Liste EU-weiter Prozesse mit hoher und kritischer Auswirkung (genehmigt)
- Vorläufige Liste europäischer und internationaler Normen (genehmigt)
- Bericht zur Bewertung der Cybersicherheitsrisiken auf EU-Ebene (genehmigt)
- Regionaler Bericht zur Bewertung der Cybersicherheitsrisiken (genehmigt)
- Regionale Pläne zur Minderung der Cybersicherheitsrisiken (genehmigt)
- Leitlinien zu Cybersicherheitszertifizierungssystemen (genehmigt)
- Durchführungsleitlinien (genehmigt)

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

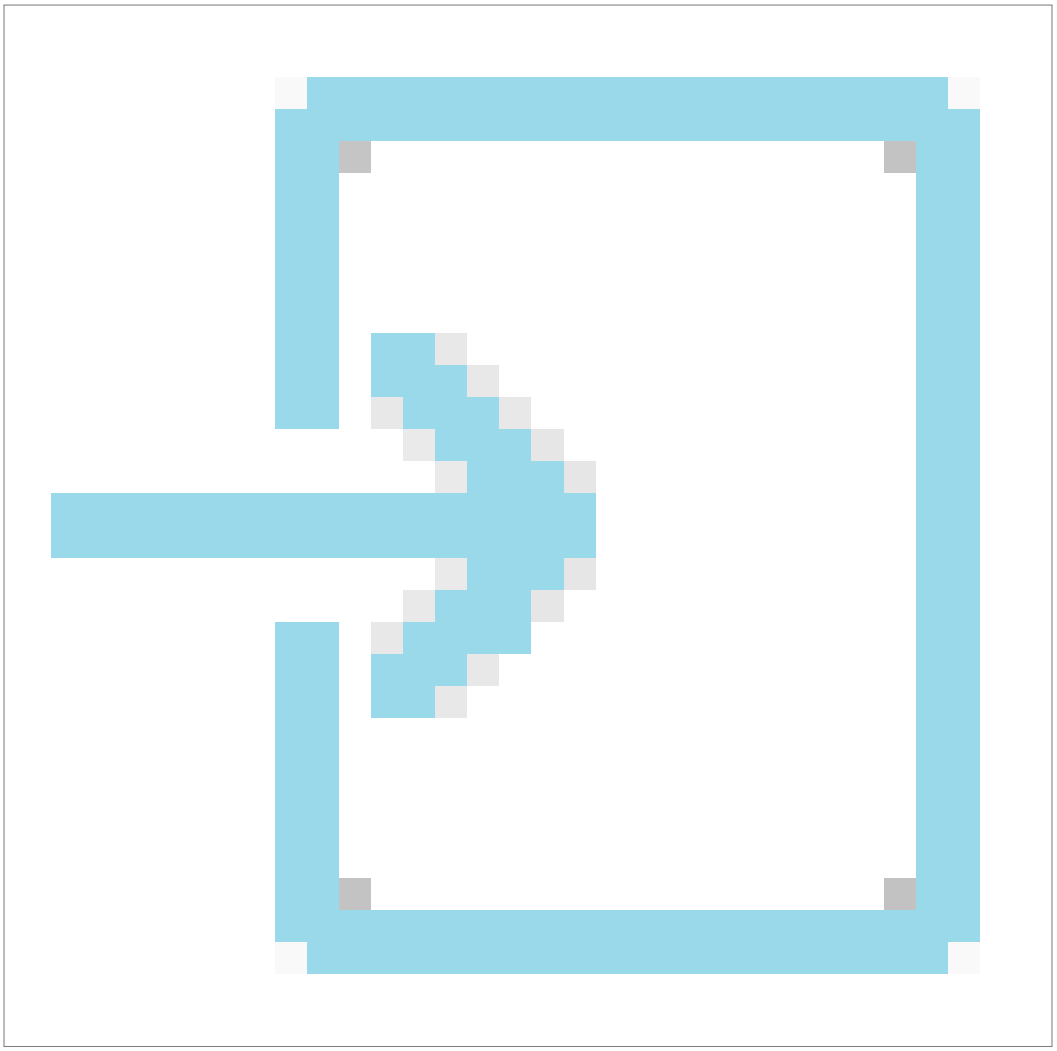
Beteiligt an der Aufgabenausführung: ACER, ENISA, NCA

Chapter 20

Artikel 18. : Methoden zur Bewertung des Cybersicherheitsrisikos

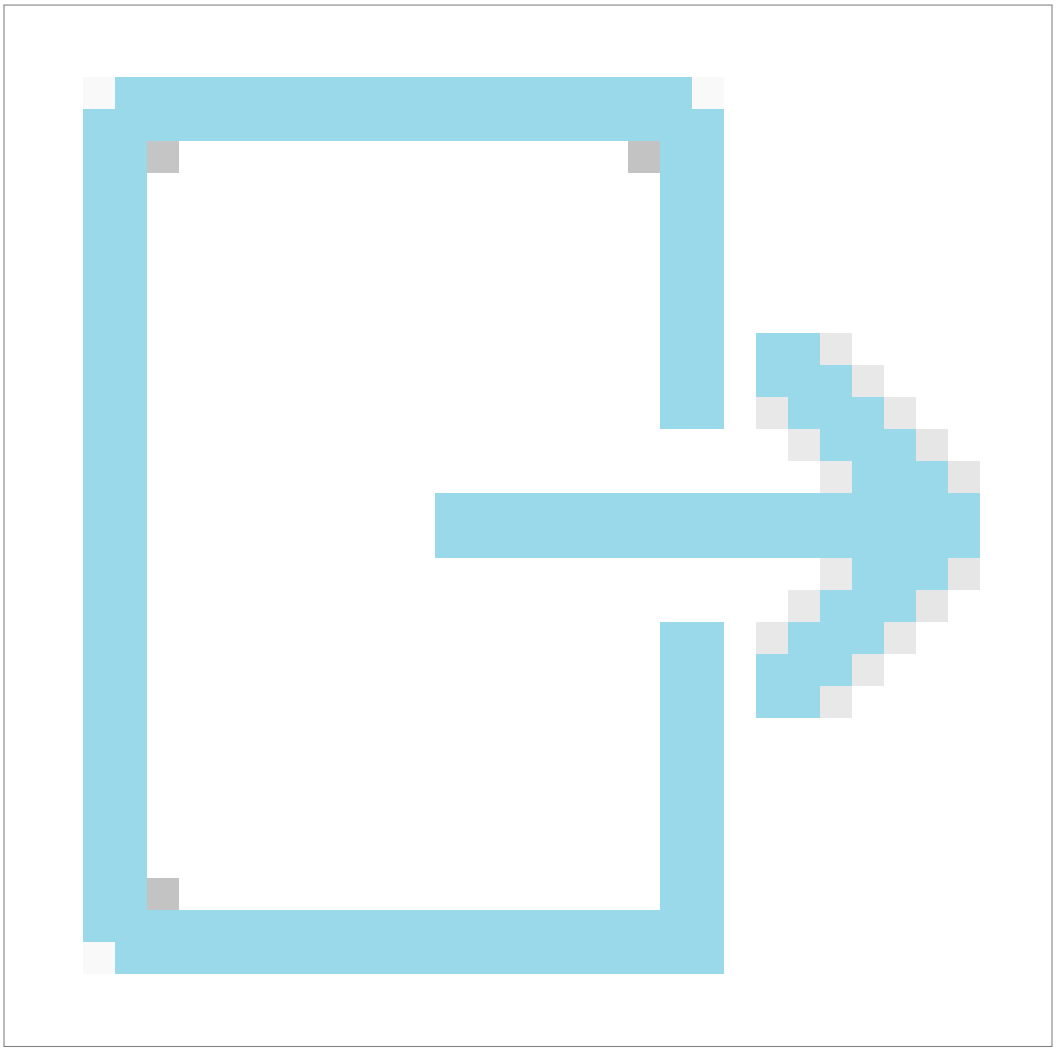
20.1 Absatz 1

Bis zum 13 März 2025 legen die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und nach Konsultation der NIS-Kooperationsgruppe einen Vorschlag für die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten vor.



Input

- Vorläufige ECII



Output

- Methoden zur Risikobewertung
- Matrix zur Risikowirkung

GOOD TO KNOW

Zeitpunkt

Bis zum 13. März 2025

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: NIS CG

20.2 Absatz 2

Die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten müssen Folgendes umfassen:

a. eine Liste der zu berücksichtigenden Cyberbedrohungen, einschließlich mindestens der folgenden Bedrohungen der Lieferkette:
   i. schwere und unerwartete Kompromittierung der Lieferkette;
   ii. Nichtverfügbarkeit von IKT-Produkten, -Diensten oder -Prozessen aus der Lieferkette;
   iii. von Akteuren in der Lieferkette ausgelöste Cyberangriffe;
   iv. Weitergabe sensibler Informationen durch die Lieferkette, einschließlich der Nachverfolgung der Lieferkette;
   v. Einführung von Schwachstellen oder Hintertüren in IKT-Produkten, -Diensten oder -Prozessen durch Akteure in der Lieferkette;

b. die Kriterien für die Einstufung der Auswirkungen von Cybersicherheitsrisiken als erheblich oder kritisch, wobei festgelegte Schwellenwerte für deren Folgen und Wahrscheinlichkeit zu nutzen sind;

c. einen Ansatz zur Analyse der Cybersicherheitsrisiken, die sich aus Altsystemen, den Kaskadeneffekten von Cyberangriffen und dem Echtzeitcharakter der Netzbetriebssysteme ergeben;

d. einen Ansatz zur Analyse der Cybersicherheitsrisiken, die sich aus der Abhängigkeit von einem einzigen Anbieter von IKT-Produkten, -Diensten oder -Prozessen ergeben.

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: NIS CG

20.3 Absatz 3

Die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten müssen dieselbe Risiko-Auswirkungs-Matrix umfassen. Mit der Risiko-Auswirkungs-Matrix

a. werden die Folgen von Cyberangriffen anhand folgender Kriterien gemessen:
    i. Lastverlust;
    ii. Verringerung der Stromerzeugung;
    iii. Kapazitätsverlust in der primären Frequenzreserve;
    iv. Verlust von Kapazitäten für die Wiederherstellung des Betriebs eines Stromnetzes ohne Rückgriff auf das externe Übertragungsnetz nach einer vollständigen oder teilweisen Abschaltung („Schwarzstart“);
    v. voraussichtliche Dauer eines Stromausfalls mit Auswirkungen auf die Kunden in Verbindung mit dem Ausmaß des Ausfalls (nach Zahl der Kunden) und
    vi. alle sonstigen quantitativen oder qualitativen Kriterien, die als sinnvolle Indikatoren für die Auswirkungen eines Cyberangriffs auf grenzüberschreitende Stromflüsse dienen könnten;

b. wird die Wahrscheinlichkeit eines Vorfalls als Häufigkeit der Cyberangriffe pro Jahr gemessen.

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: NIS CG

20.4 Absatz 4

In den Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene wird beschrieben, wie die ECIIS chwellenwerte für erhebliche und kritische Auswirkungen bestimmt werden. Der ECII muss es den Einrichtungen ermöglichen, im Rahmen der von ihnen gemäß Artikel 26 Absatz 4 Buchstabe c Ziffer i durchgeführten Folgenabschätzungen die Auswirkungen der Risiken auf ihre Geschäftsprozesse mithilfe der in Absatz 2 Buchstabe b genannten Kriterien abzuschätzen.

Relevante NCCS-Artikel

- Artikel 26 (4)
- Artikel 18 (2)

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

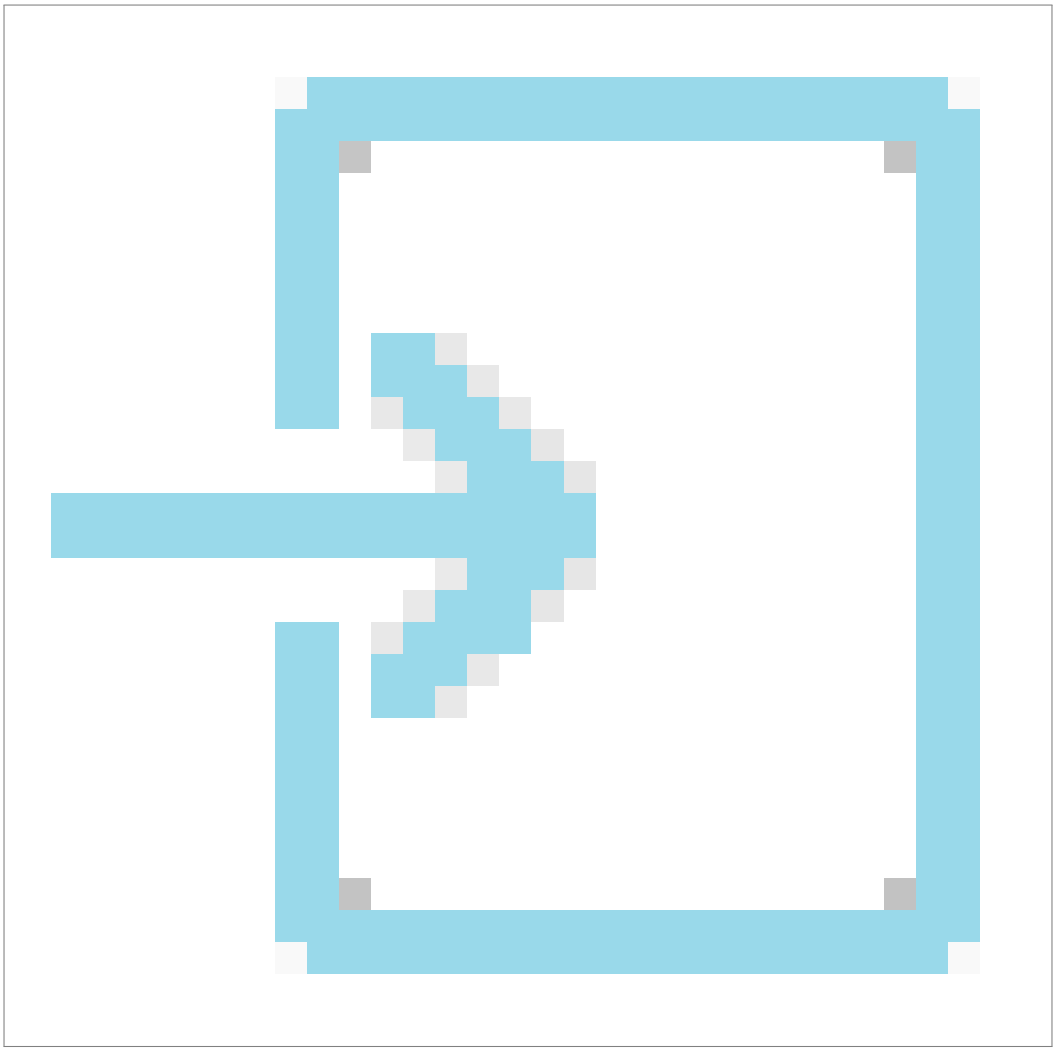
Zu konsultieren: NIS CG

20.5 Absatz 5

ENTSO-E unterrichtet die Koordinierungsgruppe „Strom“ in Abstimmung mit der EU-VNBO über die Vorschläge für die gemäß Absatz 1 zu entwickelnden Methoden zur Bewertung des Cybersicherheitsrisikos.

Relevante NCCS-Artikel

- Artikel 18 (1)



Input

- Methoden zur Risikobewertung

A

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu informieren: ECG

Chapter 21

Artikel 19. : Unionsweite Bewertung des Cybersicherheitsrisikos

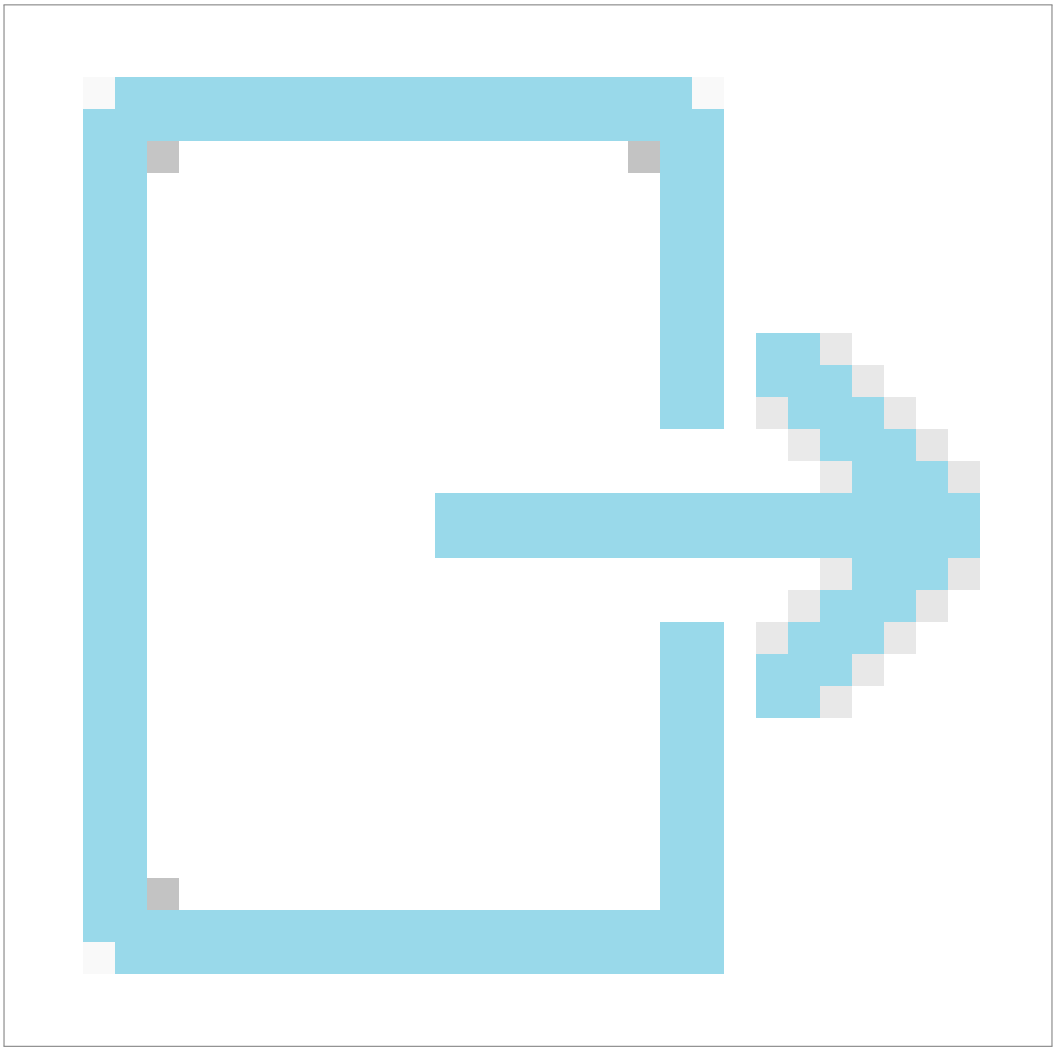
21.1 Absatz 1

Innerhalb von neun Monaten nach der Genehmigung der Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 8 und danach alle drei Jahre führt ENTSO-E in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe unbeschadet des Artikels 22 der Richtlinie (EU) 2022/2555 [a] eine unionsweite Bewertung des Cybersicherheitsrisikos durch und erstellt einen Entwurf eines Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos. Dabei wenden sie die gemäß Artikel 18 entwickelten und gemäß Artikel 8 genehmigten Methoden an, um die möglichen Folgen von Cyberangriffen, die sich auf die Betriebssicherheit des Elektrizitätssystems auswirken und grenzüberschreitende Stromflüsse stören, zu ermitteln, zu analysieren und zu bewerten. Bei der unionsweiten Bewertung des Cybersicherheitsrisikos werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_22

Relevante NCCS-Artikel

- Artikel 8
- Artikel 18



Output

- Unionsweiter Bericht zur Bewertung von Cybersicherheitsrisiken

GOOD TO KNOW

Zeitpunkt

> Innerhalb von 9 Monaten nach Genehmigung der Methoden zur Bewertung von Cybersicherheitsrisiken

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu konsultieren: NIS CG

21.2 Absatz 2

Der Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos muss Folgendes enthalten:

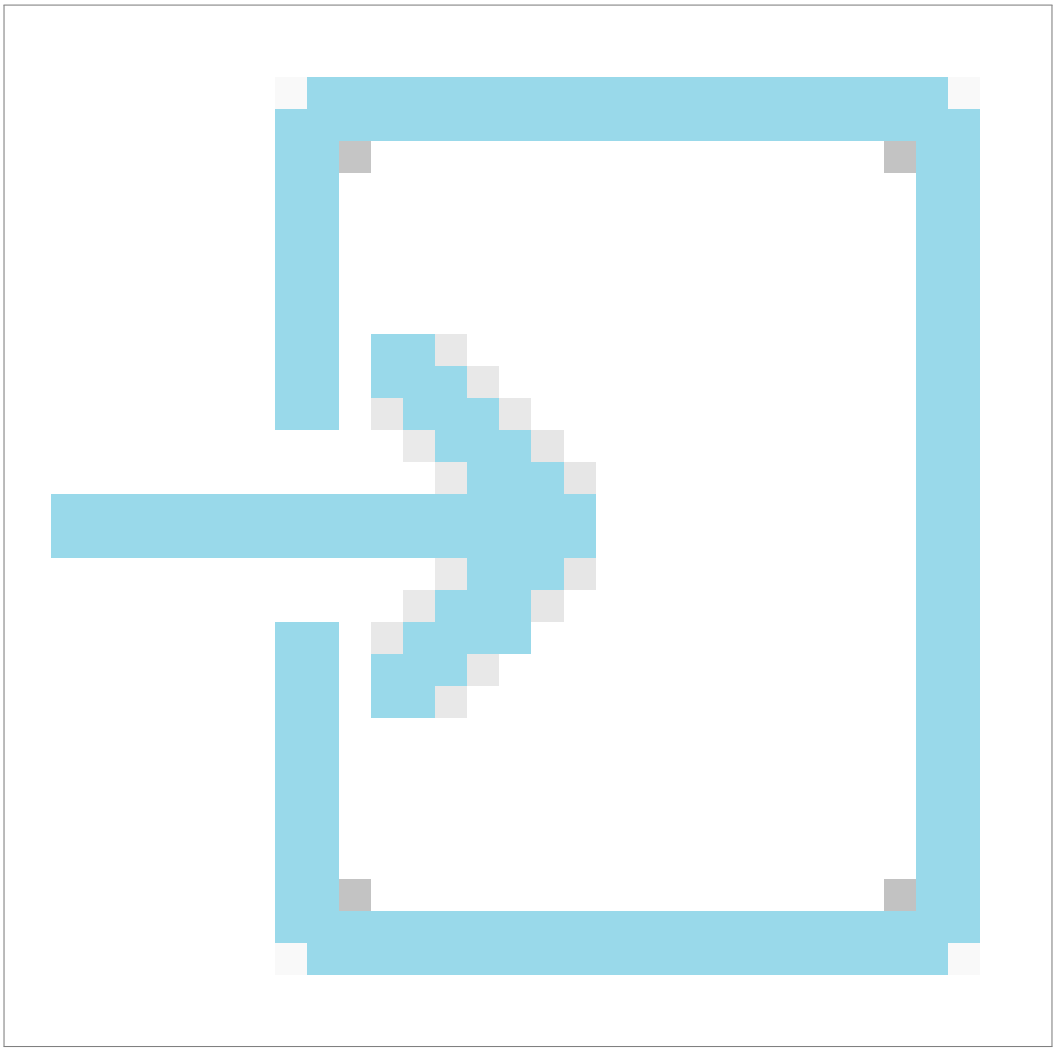
a. die unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen;

b. eine Risiko-Auswirkungs-Matrix, die Einrichtungen und die zuständigen Behörden nutzen müssen, um die Cybersicherheitsrisiken zu bewerten, die in der Bewertung des Cybersicherheitsrisikos auf der Ebene der Mitgliedstaaten gemäß Artikel 20 und in der Bewertung des Cybersicherheitsrisikos auf der Ebene von, Einrichtungen gemäß Artikel 26 Absatz 2 Buchstabe b ermittelt wurden.

>

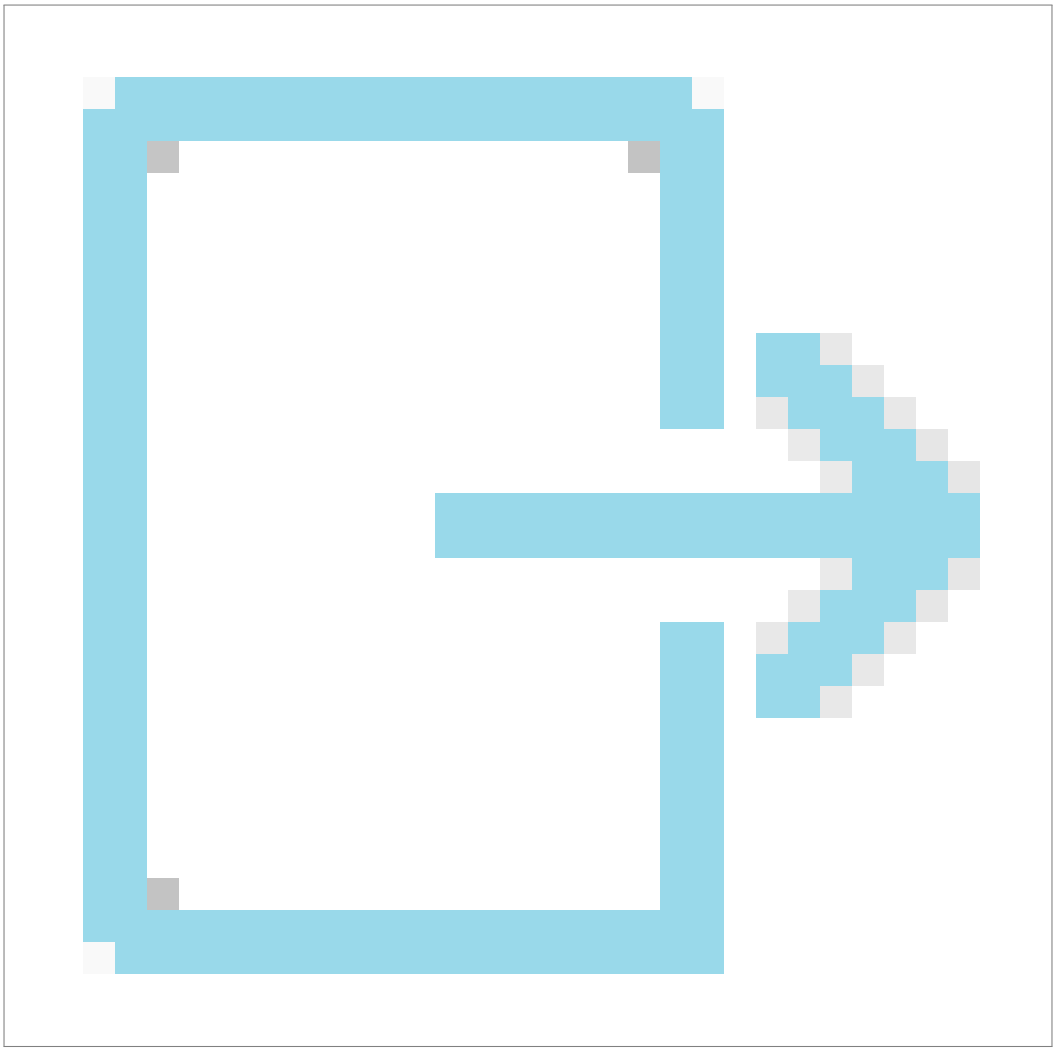
Relevante NCCS-Artikel

- Artikel 20
- Artikel 26 (2)



Input

- Vorläufige Prozessliste für die Union



Output

- Risikowirkungsmatrix
- Unionsweite Prozessliste

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu konsultieren: NIS CG

21.3 Absatz 3

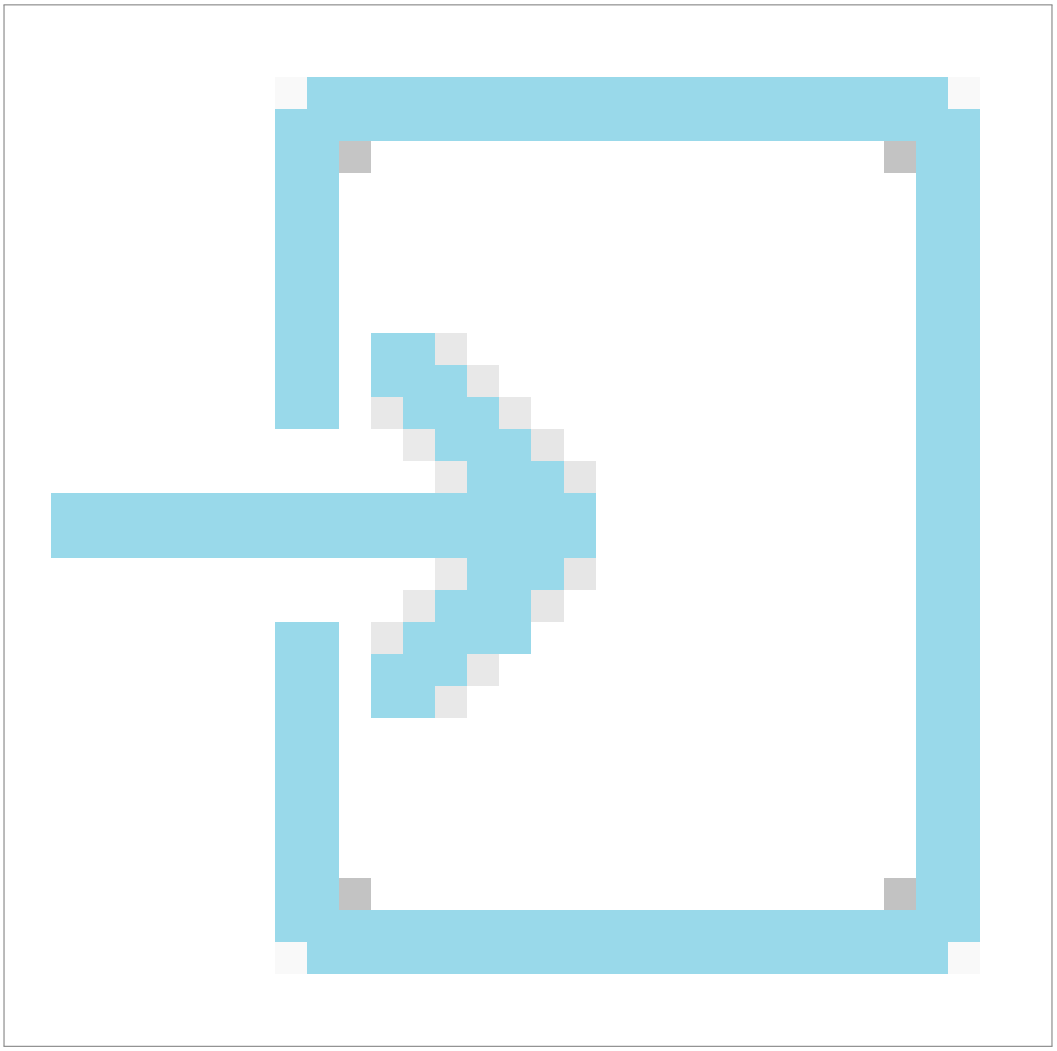
In Bezug auf die unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen muss der Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos Folgendes enthalten:

a. eine Bewertung der möglichen Folgen eines Cyberangriffs anhand der Parameter, die in der gemäß Artikel 18 Absätze 2, 3 und 4 entwickelten und gemäß Artikel 8 genehmigten Methode zur Bewertung des Cybersicherheitsrisikos festgelegt sind;

b. den ECII und die Schwellenwerte für erhebliche und kritische Auswirkungen, die die zuständigen Behörden gemäß Artikel 24 Absätze 1 und 2 nutzen müssen, um Einrichtungen mit erheblichen oder kritischen Auswirkungen zu ermitteln, die an unionsweiten Prozessen mit erheblichen bzw. kritischen Auswirkungen beteiligt sind.

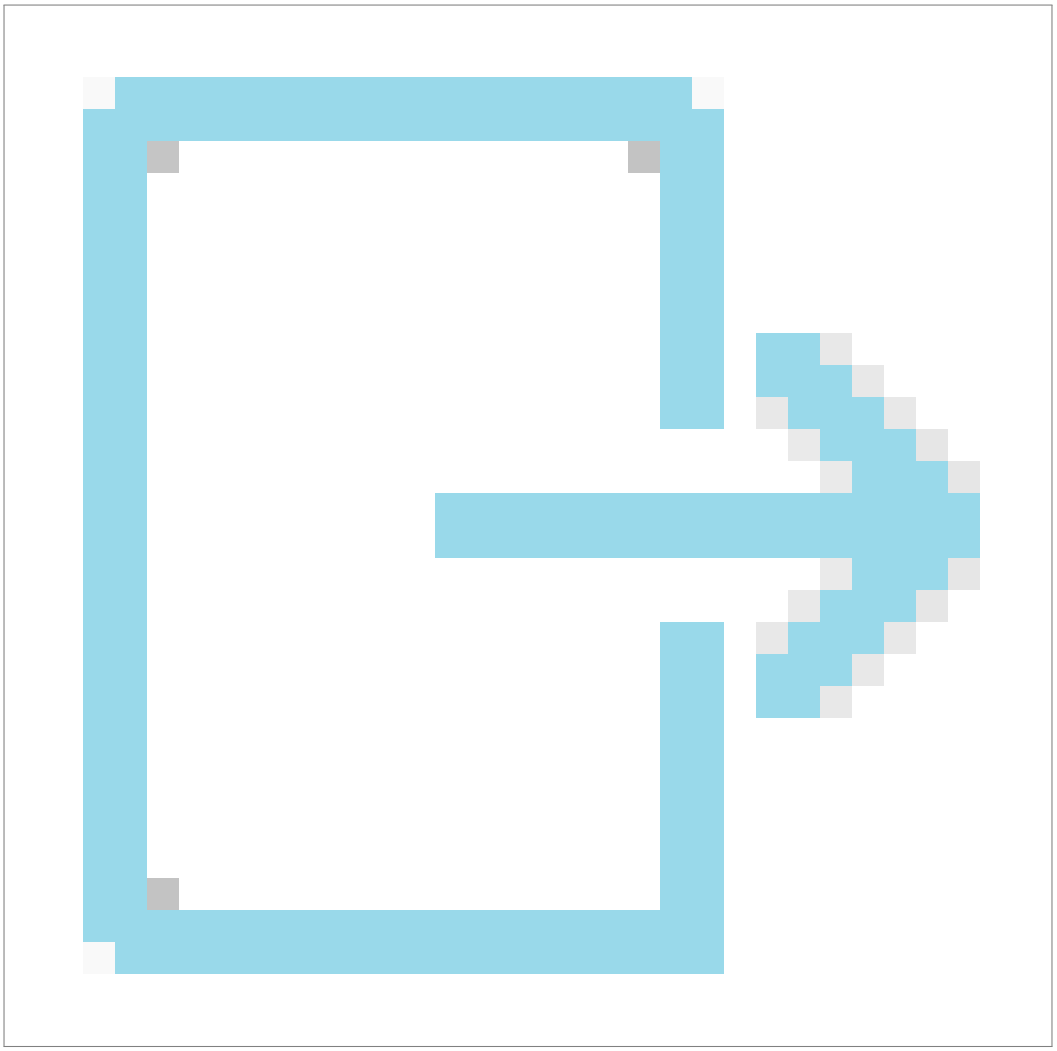
Relevante NCCS-Artikel

- Artikel 18 (2)
- Artikel 18 (3)
- Artikel 18 (4)
- Artikel 24 (1)
- Artikel 24 (2)



Input

- Unionsweite Prozessliste
- Methoden zur Risikobewertung



Output

- ECII

A

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

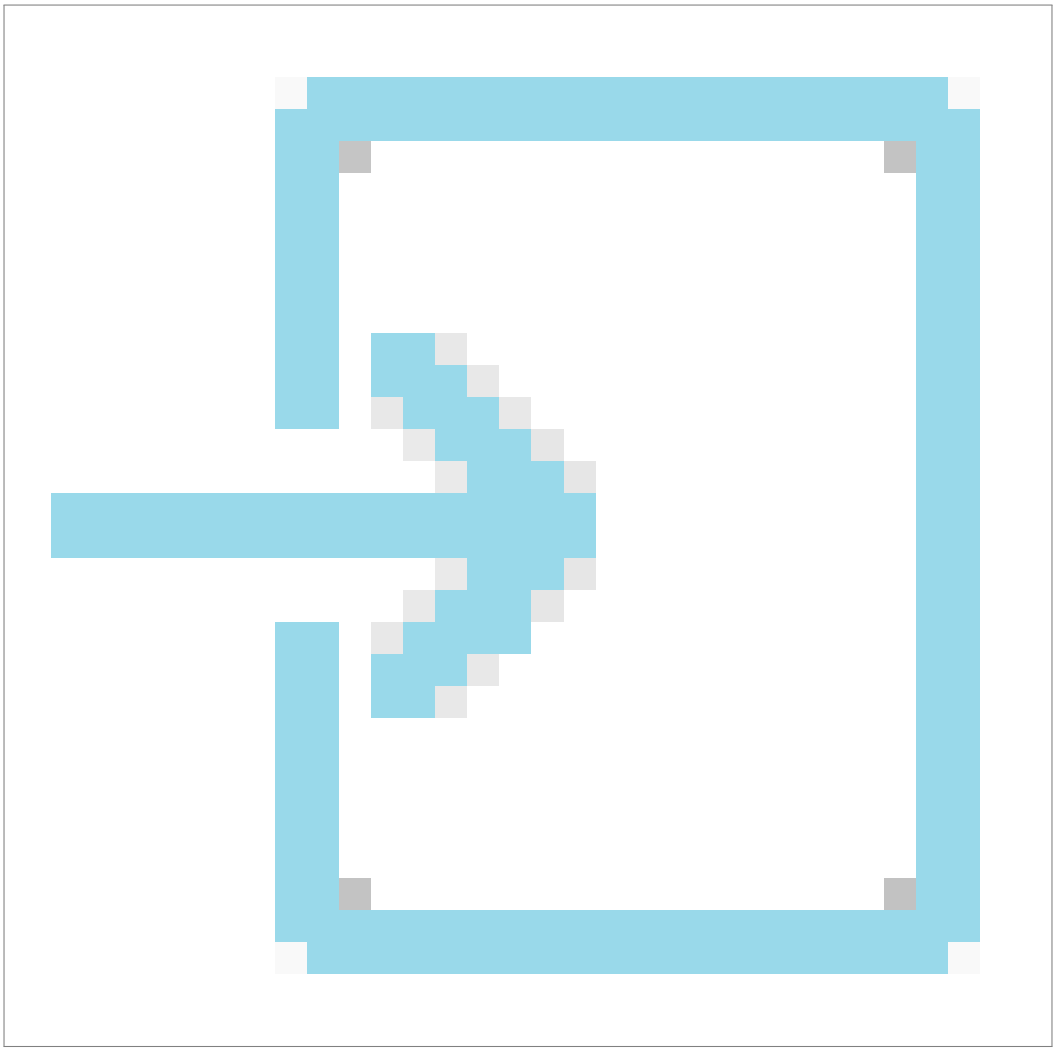
R

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu konsultieren: NIS CG

21.4 Absatz 4

ENTSO-E legt der ACER in Zusammenarbeit mit der EU-VNBO den Entwurf des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos mit den Ergebnissen der unionsweiten Bewertung des Cybersicherheitsrisikos zur Stellungnahme vor.



Input

- Unionsweiter Risikobewertungsbericht (Entwurf)

A

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

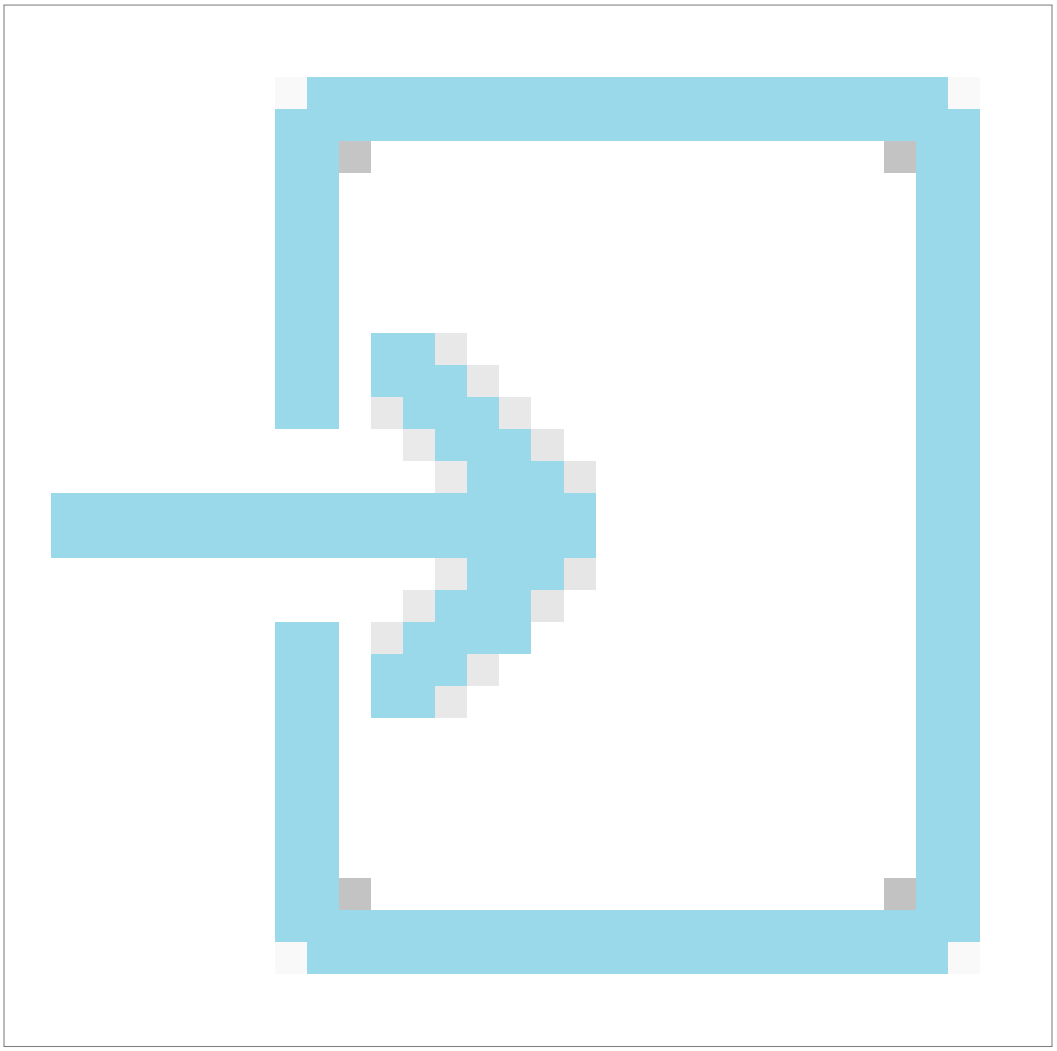
R

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu informieren: ACER

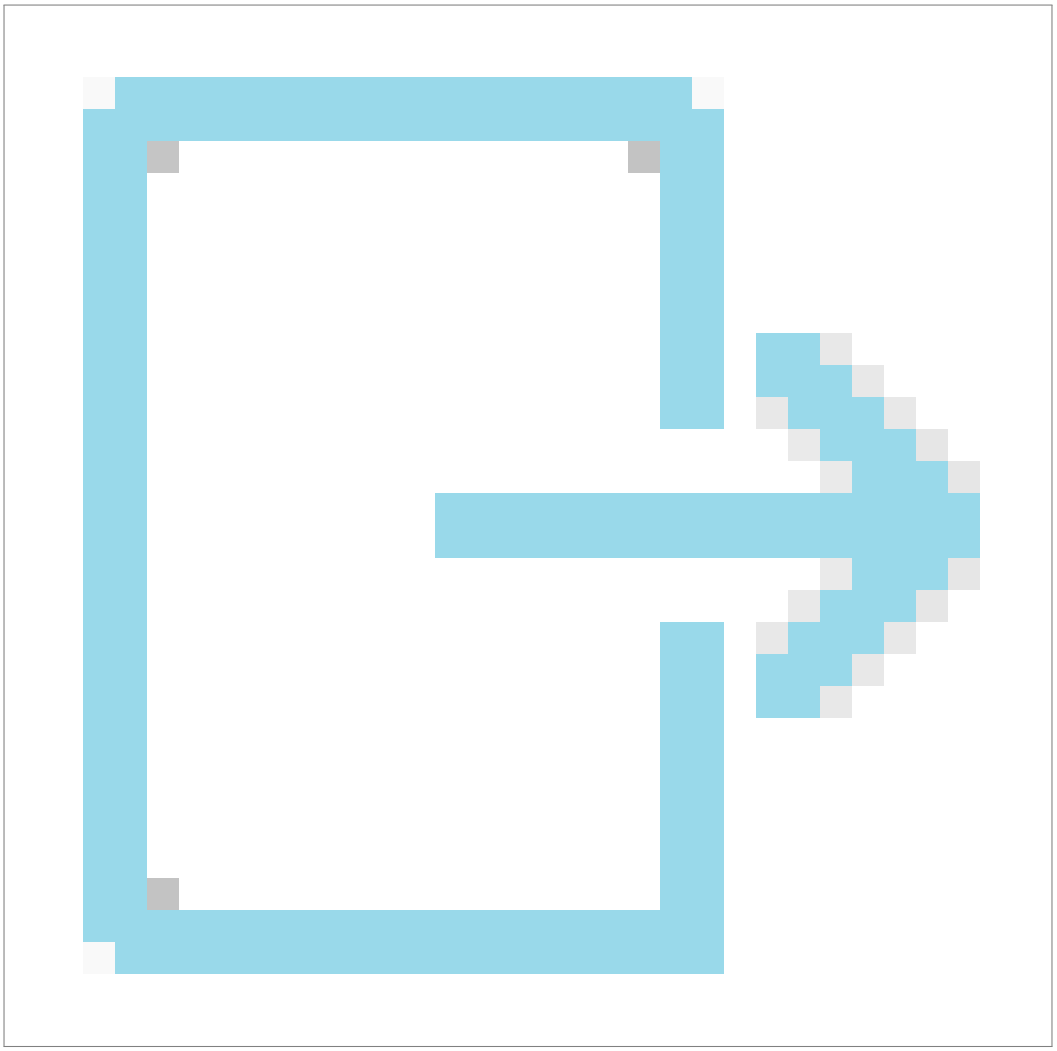
21.5 Absatz 4

Die ACER gibt innerhalb von drei Monaten nach Eingang eine Stellungnahme zu dem Entwurf des Berichts ab. ENTSO-E und die EU-VNBO tragen der Stellungnahme der ACER bei der Fertigstellung dieses Berichts so weit wie möglich Rechnung.



Input

- Unionsweiter Risikobewertungsbericht (Entwurf)



Output

- Stellungnahme von Acer

GOOD TO KNOW

Zeitpunkt

Innerhalb von drei Monaten nach Erhalt des Berichtsentwurfs

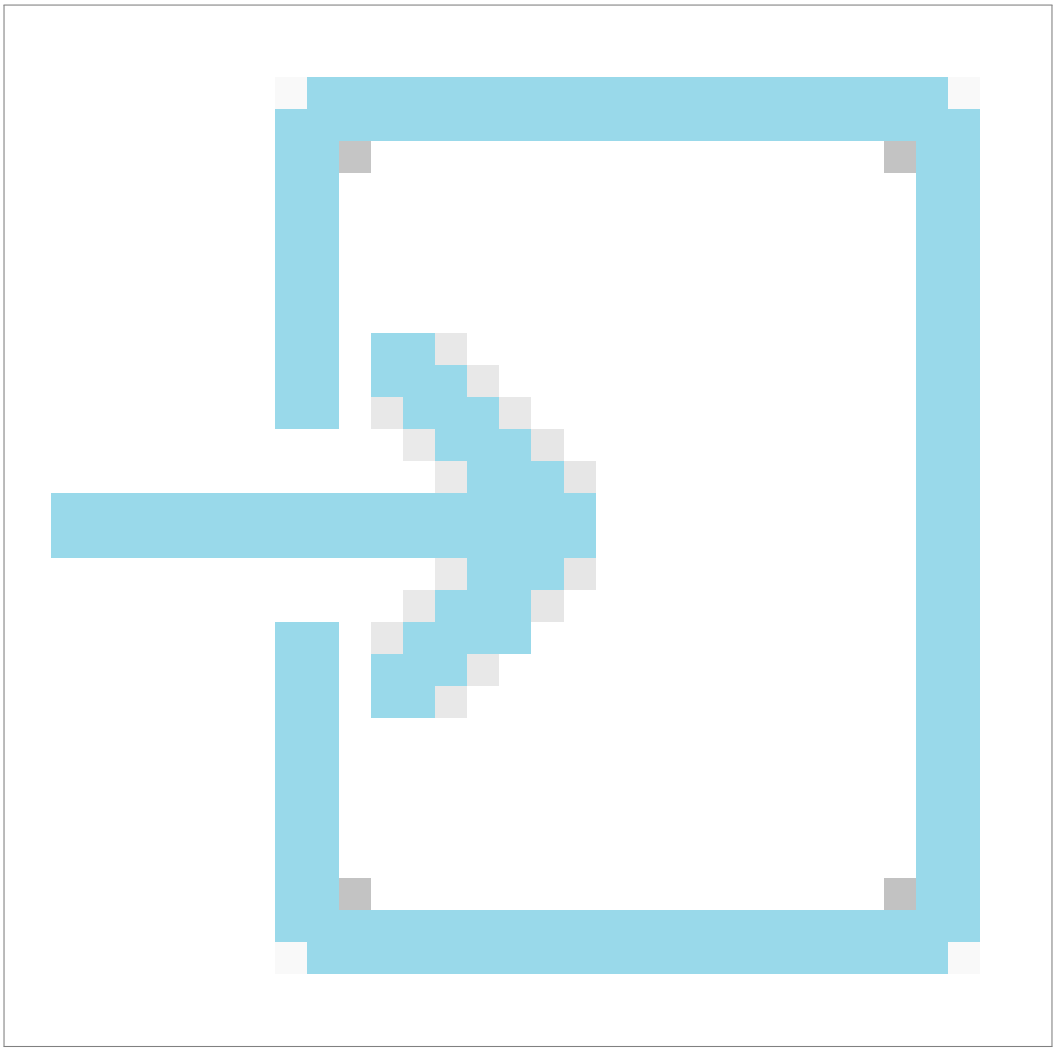
Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, ACER, EU DSO

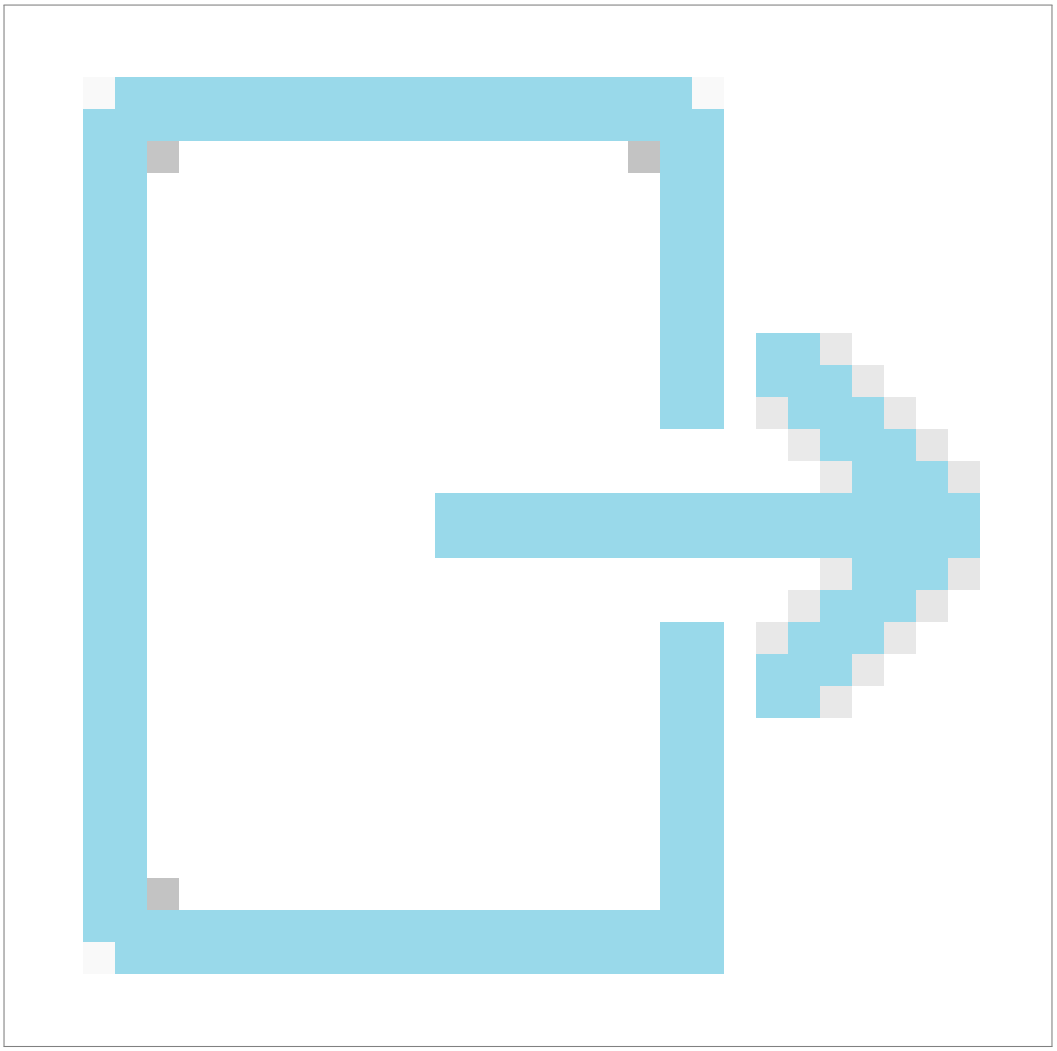
21.6 Absatz 5

Innerhalb von drei Monaten nach Eingang der Stellungnahme der ACER übermittelt ENTSO-E in Zusammenarbeit mit der EU-VNBO der ACER, der Kommission, der ENISA und den zuständigen Behörden den endgültigen Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos.



Input

- Stellungnahme von ACER



Output

- Unionsweiter Risikobewertungsbericht (Entwurf)

GOOD TO KNOW

Zeitpunkt

Innerhalb von drei Monaten nach Erhalt der Stellungnahme der ACER

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu informieren: EC, ACER, ENISA, NCA

Chapter 22

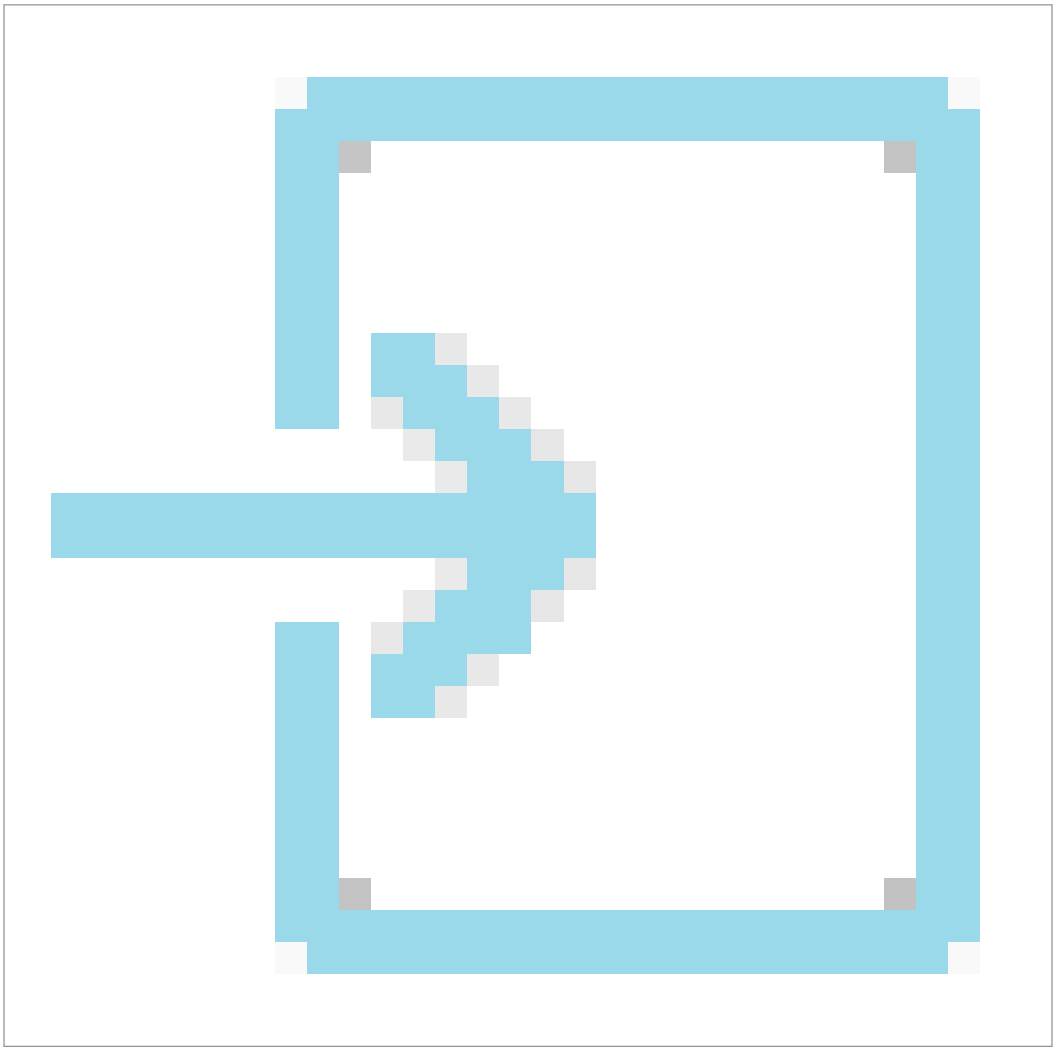
Artikel 20. : Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten

22.1 Absatz 1

Jede zuständige Behörde führt in Bezug auf alle Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat eine Bewertung des Cybersicherheitsrisikos des Mitgliedstaats durch und nutzt dabei die gemäß Artikel 18 entwickelten und gemäß Artikel 8 genehmigten Methoden. Bei der Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten werden die Risiken von Cyberangriffen ermittelt und analysiert, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören. Bei der Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

Relevante NCCS-Artikel

- Artikel 18
- Artikel 8



Input

- Methoden zur Risikobewertung

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

22.2 Absatz 2

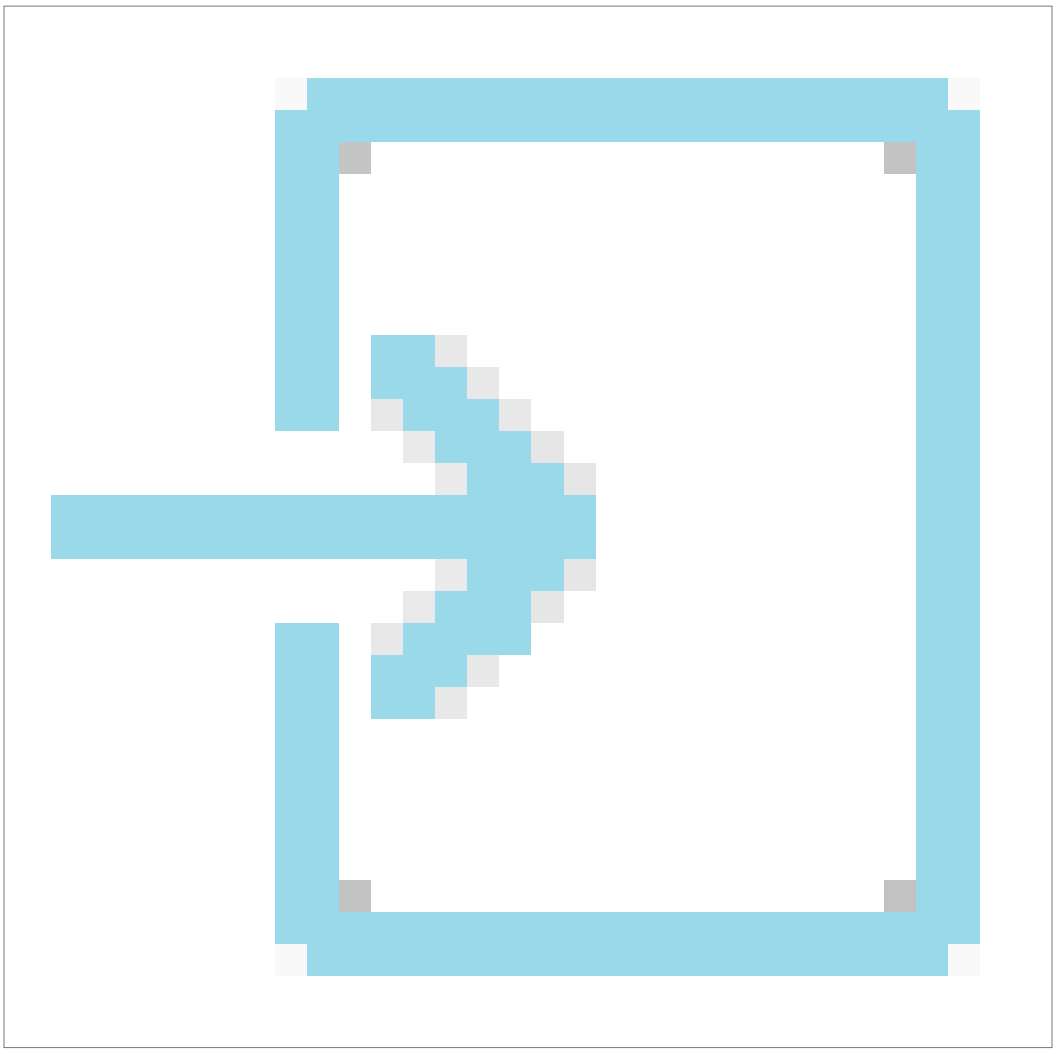
Innerhalb von 21 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre übermittelt jede zuständige Behörde mit Unterstützung des CSIRT und nach Konsultation der für Elektrizität zuständigen CS-NCA dem ENTSO-E und der EU-VNBO einen Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats, der in Bezug auf jeden Geschäftsprozess mit erheblichen oder kritischen Auswirkungen folgende Informationen enthält:

a. den Stand der Umsetzung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskorntrollen gemäß Artikel 29;
b. eine Liste aller in den letzten drei Jahren gemäß Artikel 38 Absatz 3 gemeldeten Cyberangriffe;
c. eine Zusammenfassung aller in den letzten drei Jahren gemäß Artikel 38 Absatz 6 gemeldeten Informationen zu Cyberbedrohungen;
d. für jeden unionsweiten Prozess mit erheblichen oder kritischen Auswirkungen eine Schätzung der mit einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten verbundenen Risiken;
e. erforderlichenfalls eine Liste zusätzlicher Einrichtungen, die gemäß Artikel 24 Absätze 1, 2, 3 und 5 als Einrichtungen mit erheblichen oder kritischen Auswirkungen ermittelt wurden.

Relevante NCCS-Artikel

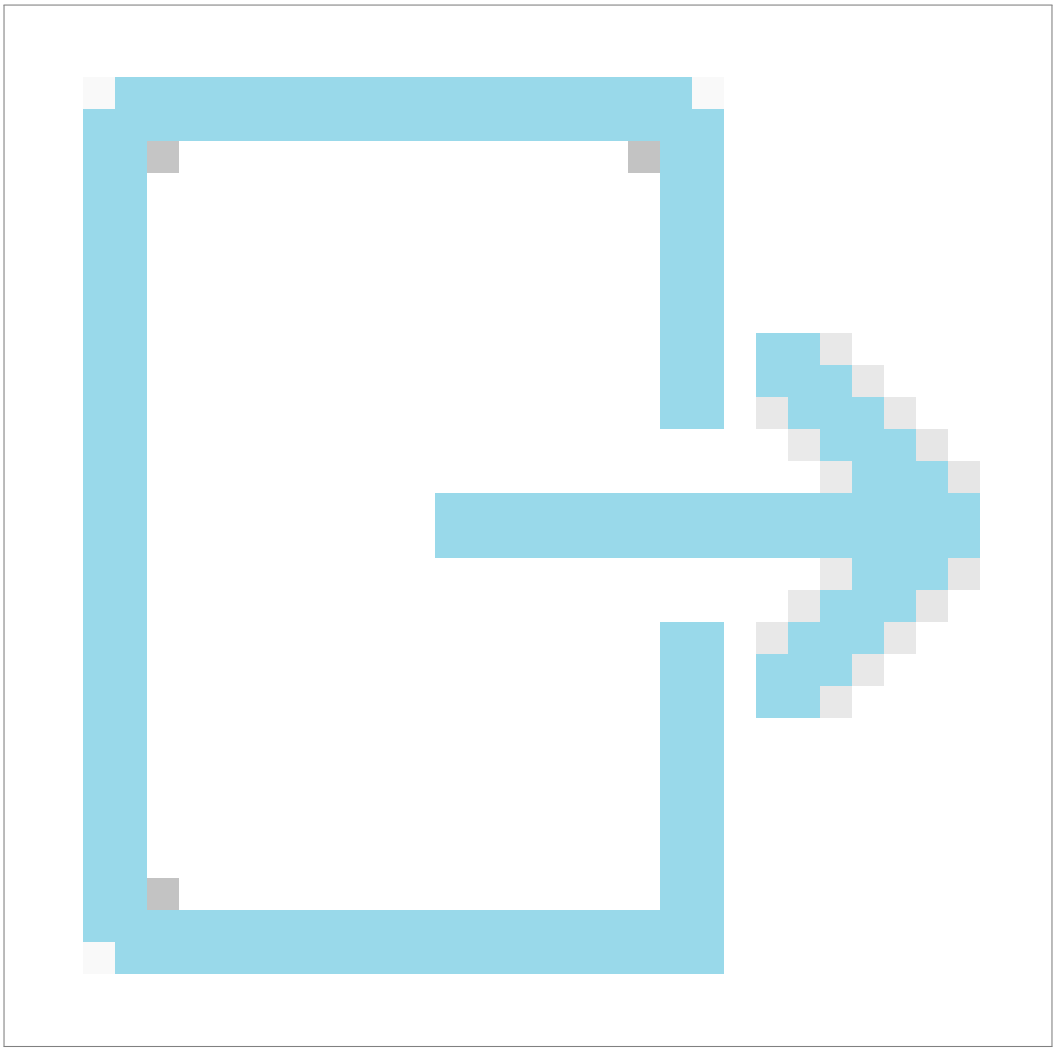
- Artikel 24 (6)
- Artikel 29
- Artikel 38

- Artikel 38 (3)
- Artikel 38 (6)
- Artikel 24 (1)
- Artikel 24 (2)
- Artikel 24 (3)
- Artikel 24 (5)



Input

- Risikobewertung auf Unternehmensebene



Output

- Risikobewertung auf Ebene der Mitgliedstaaten

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

Bis zum 13. März 2030

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu konsultieren: CS NCA

Zu informieren: ENTSO-E, EU DSO

22.3 Absatz 3

Der Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats muss dem gemäß Artikel 10 der Verordnung (EU) 2019/941 [a] erstellten Risikovorsorgeplan des Mitgliedstaats Rechnung tragen.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e928-1-1

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu konsultieren: CS NCA

Zu informieren: ENTSO-E, EU DSO

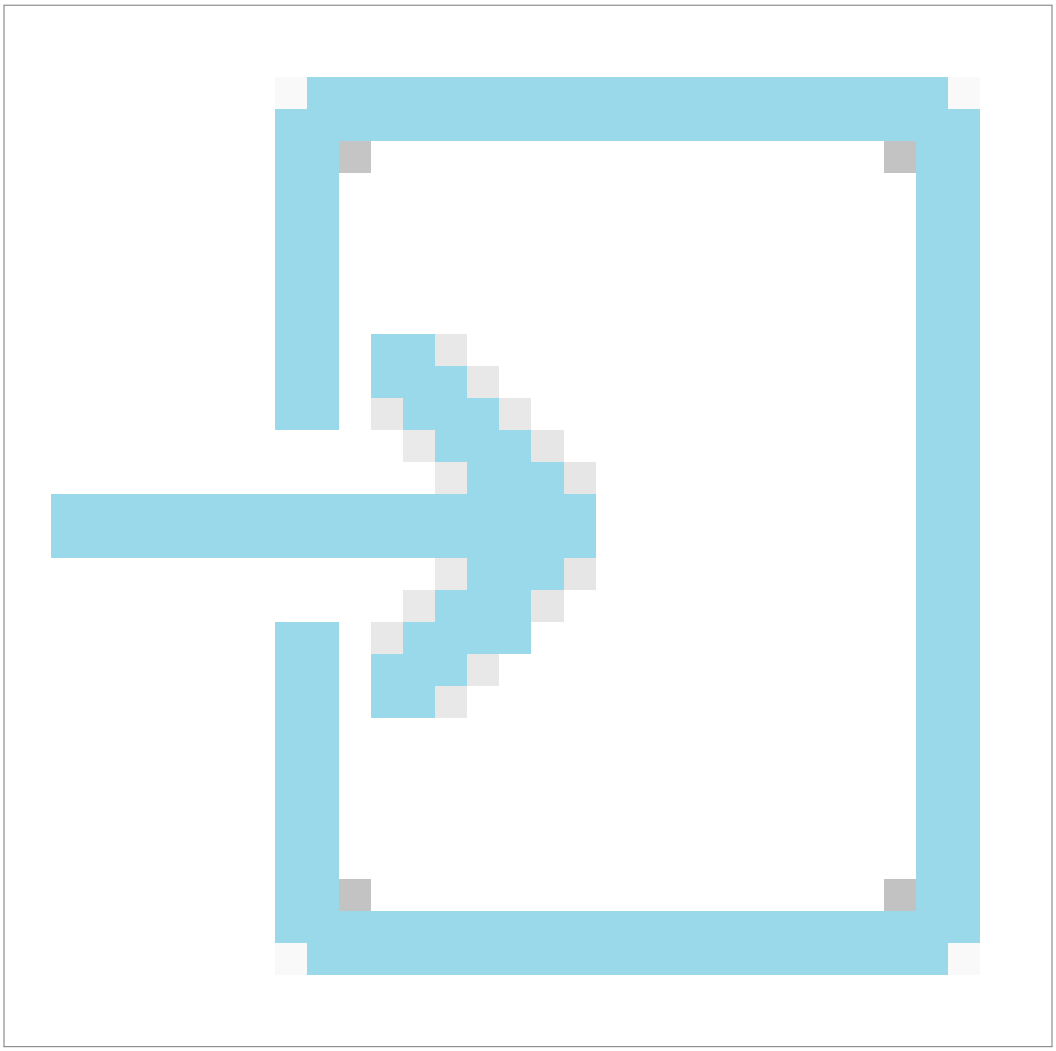
22.4 Absatz 4

Die Informationen in dem Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats gemäß Absatz 2 Buchstaben a bis d dürfen nicht mit bestimmten Einrichtungen oder Vermögenswerten verknüpft sein. In dem Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats sind auch die Risiken im Zusammenhang mit den von den zuständigen Behörden der Mitgliedstaaten gemäß Artikel 30 gewährten befristeten Ausnahmen zu bewerten.

Relevante NCCS-Artikel

- Artikel 20 (2)

- Artikel 30



Input

- Risikobewertung der vorübergehenden Ausnahmeregelungen

A

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu konsultieren: CS NCA

Zu informieren: ENTSO-E, EU DSO

22.5 Absatz 5

ENTSO-E und die EU-VNBO können im Zusammenhang mit den in Unterabsatz 2 Buchstaben a und c genannten Aufgaben die zuständigen Behörden um zusätzliche Informationen ersuchen.

Relevante NCCS-Artikel

- Artikel 20 (2)

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO, NCA

22.6 Absatz 6

Die zuständigen Behörden stellen sicher, dass die von ihnen bereitgestellten Informationen genau und zutreffend sind.

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Chapter 23

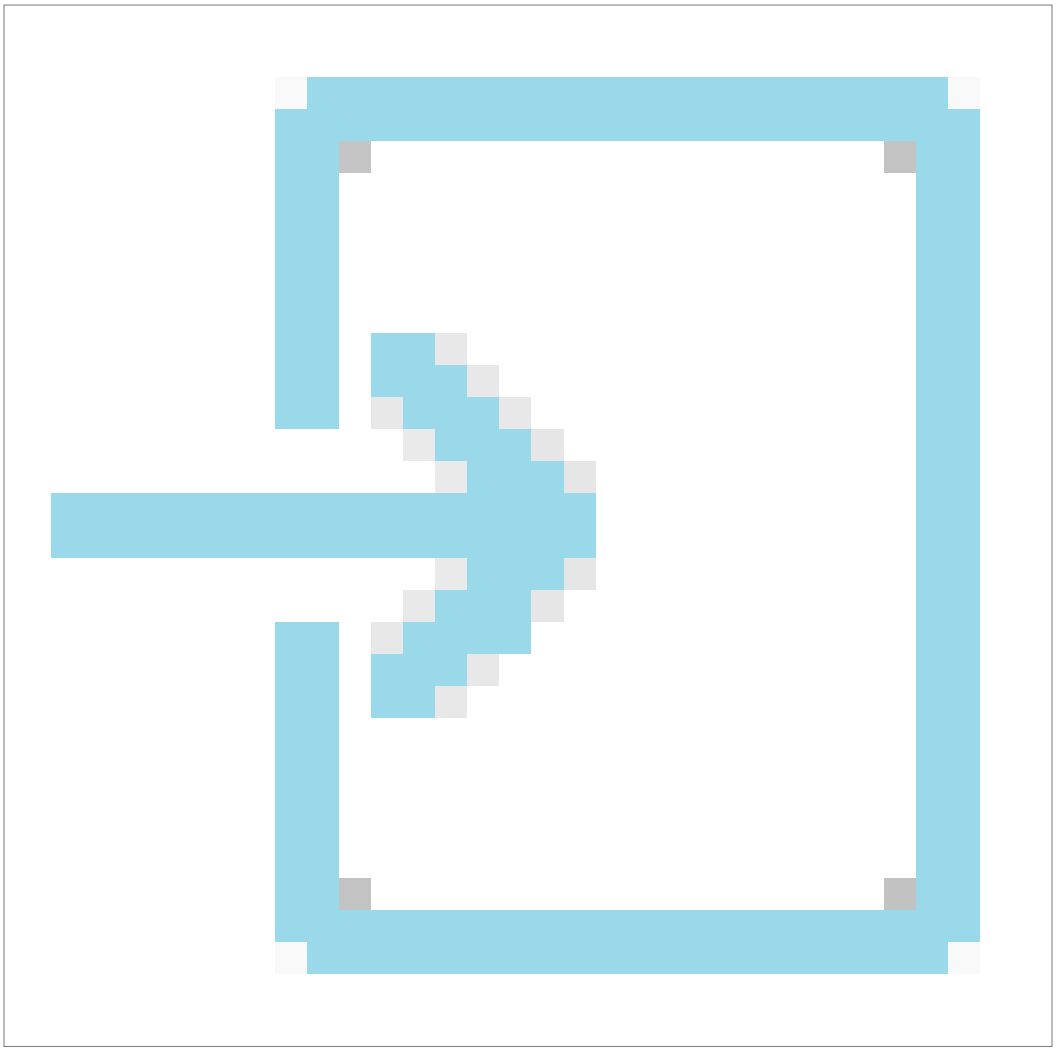
Artikel 21. : Regionale Bewertungen des Cybersicherheitsrisikos

23.1 Absatz 1

ENTSO-E führt in Zusammenarbeit mit der EU-VNBO und in Absprache mit dem zuständigen regionalen Koordinierungszentrum für jede Netzbetriebsregion eine regionale Bewertung des Cybersicherheitsrisikos durch und nutzt dabei die gemäß Artikel 19 entwickelten und gemäß Artikel 8 genehmigten Methoden, um die Risiken von Cyberangriffen, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören, zu ermitteln, zu analysieren und zu bewerten. Bei der regionalen Bewertung des Cybersicherheitsrisikos werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

Relevante NCCS-Artikel

- Artikel 18
- Artikel 8



Input

- Methoden zur Risikobewertung

A

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

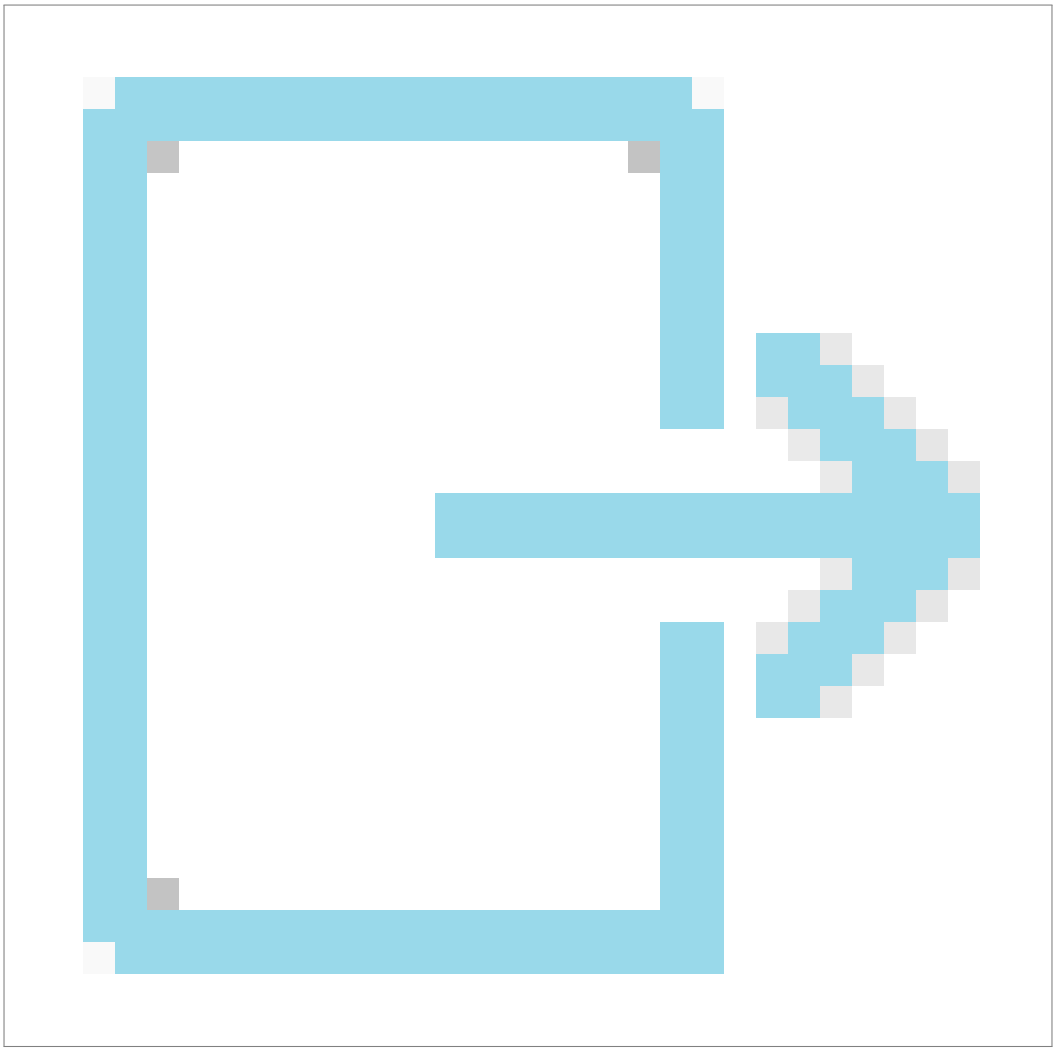
Zu konsultieren: RCC

23.2 Absatz 2

Innerhalb von 30 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe für jede Netzbetriebsregion einen Bericht über die regionale Bewertung des Cybersicherheit-srisikos.

Relevante NCCS-Artikel

- Artikel 24 (6)



Output

- Risikobewertung auf regionaler Ebene

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Dezember 2030

Verantwortlich für die Aktivität: ENTSO-E

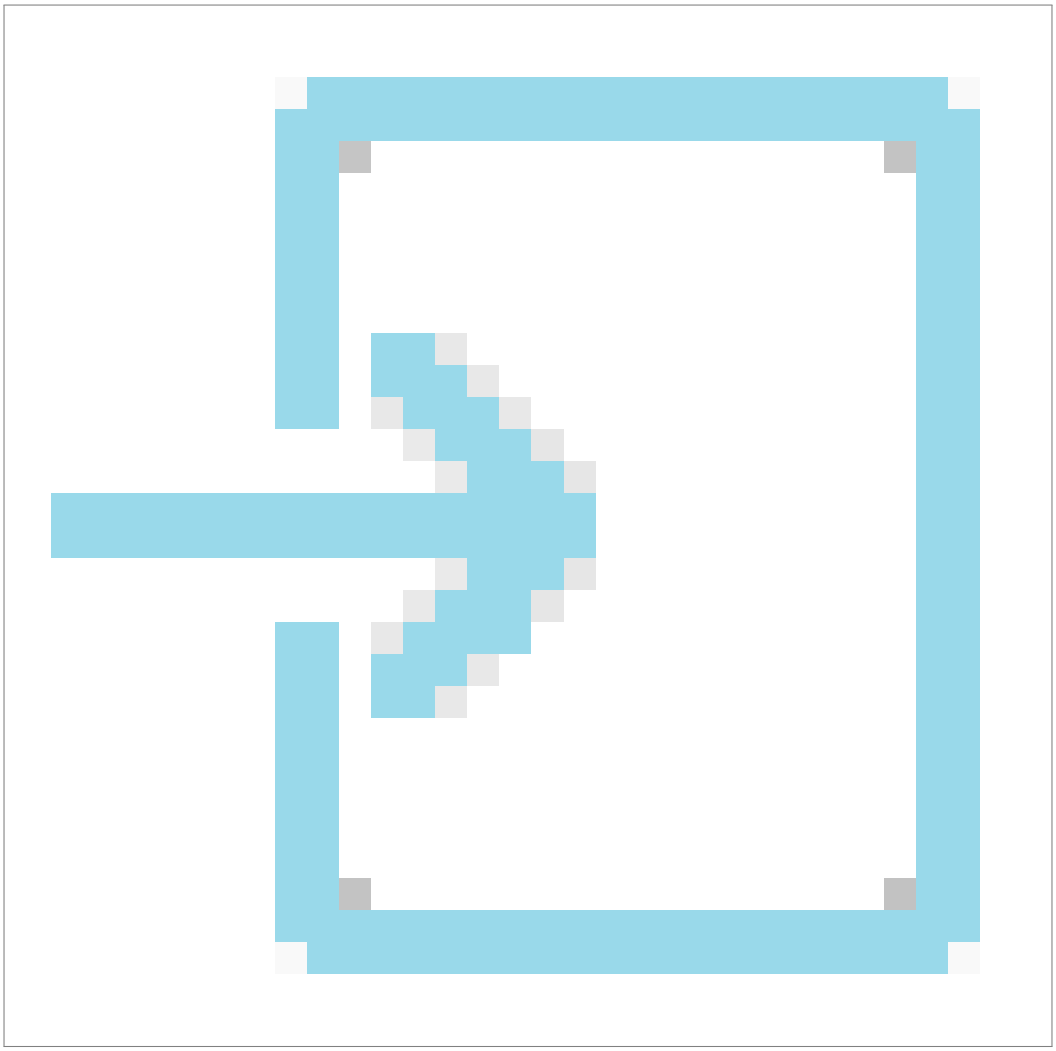
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu konsultieren: NIS CG

23.3 Absatz 3

Der Bericht über die regionale Bewertung des Cybersicherheitsrisikos muss den einschlägigen Informationen Rechnung tragen, die in den Berichten über die unionsweite Bewertung des Cybersicherheitsrisikos und in den Berichten der Mitgliedstaaten über die Bewertung des Cybersicherheitsrisikos enthalten sind.



Input

- Risikobewertung auf Unionsebene
- Risikobewertung auf Ebene der Mitgliedstaaten

A

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

23.4 Absatz 4

Bei der regionalen Bewertung des Cybersicherheitsrisikos werden die gemäß Artikel 6 der Verordnung (EU) 2019/941 [a] bestimmten regionalen Szenarien für Stromversorgungskrisen im Bereich der Cybersicherheit berücksichtigt.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e698-1-1

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Chapter 24

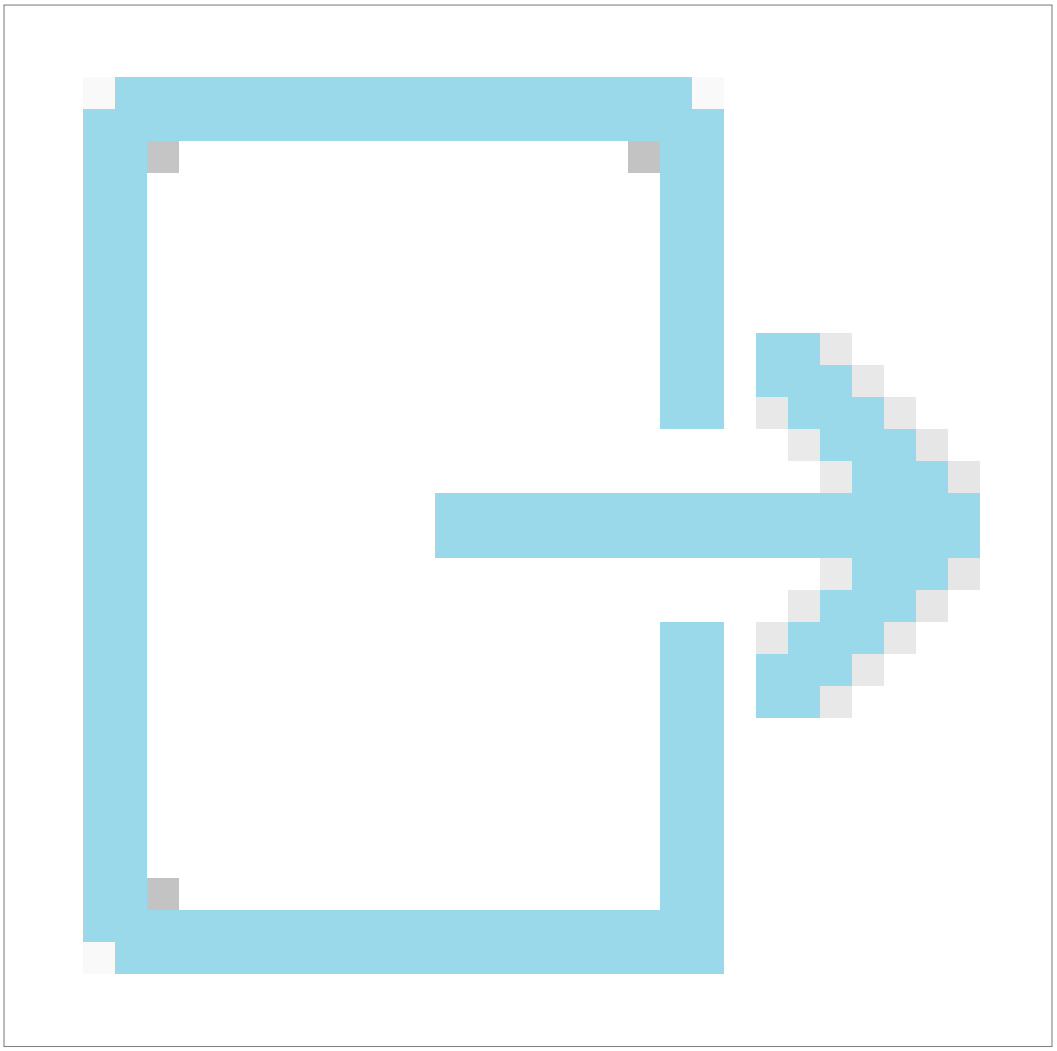
Artikel 22. : Regionale Pläne zur Minderung des Cybersicherheitsrisikos

24.1 Absatz 1

Innerhalb von 36 Monaten nach Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6, spätestens jedoch am 13 Juni 2031, und danach alle drei Jahre erstellen die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit den regionalen Koordinierungszentren und der NIS-Kooperationsgruppe für jede Netzbetriebsregion einen regionalen Plan zur Minderung des Cybersicherheitsrisikos.

Relevante NCCS-Artikel

- Artikel 24 (6)



Output

- Regionaler Risikominderungsplan (Entwurf)

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Juni 2031

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

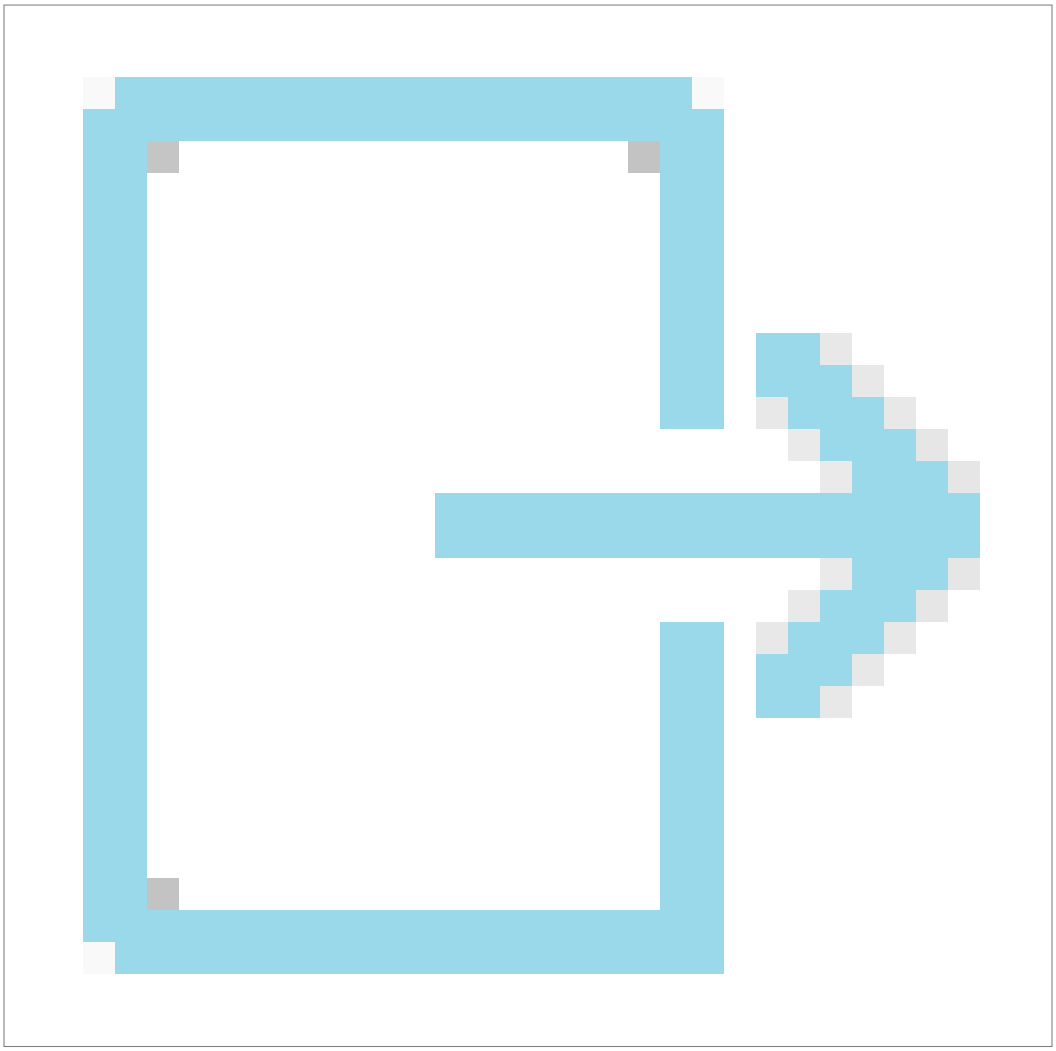
Zu konsultieren: RCC

24.2 Absatz 2

Die regionalen Pläne zur Minderung des Cybersicherheitsrisikos müssen Folgendes enthalten:

a. die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen, die die Einrichtungen mit erheblichen bzw. kritischen Auswirkungen in der Netzbetriebsregion anwenden müssen;

b. die verbleibenden Cybersicherheitsrisiken in den Netzbetriebsregionen nach Anwendung der unter Buchstabe a genannten Kontrollen.



Output

- Minimale und erweiterte Kontrollen
- Restrisiken

Verantwortlich für die Aktivität: TSO

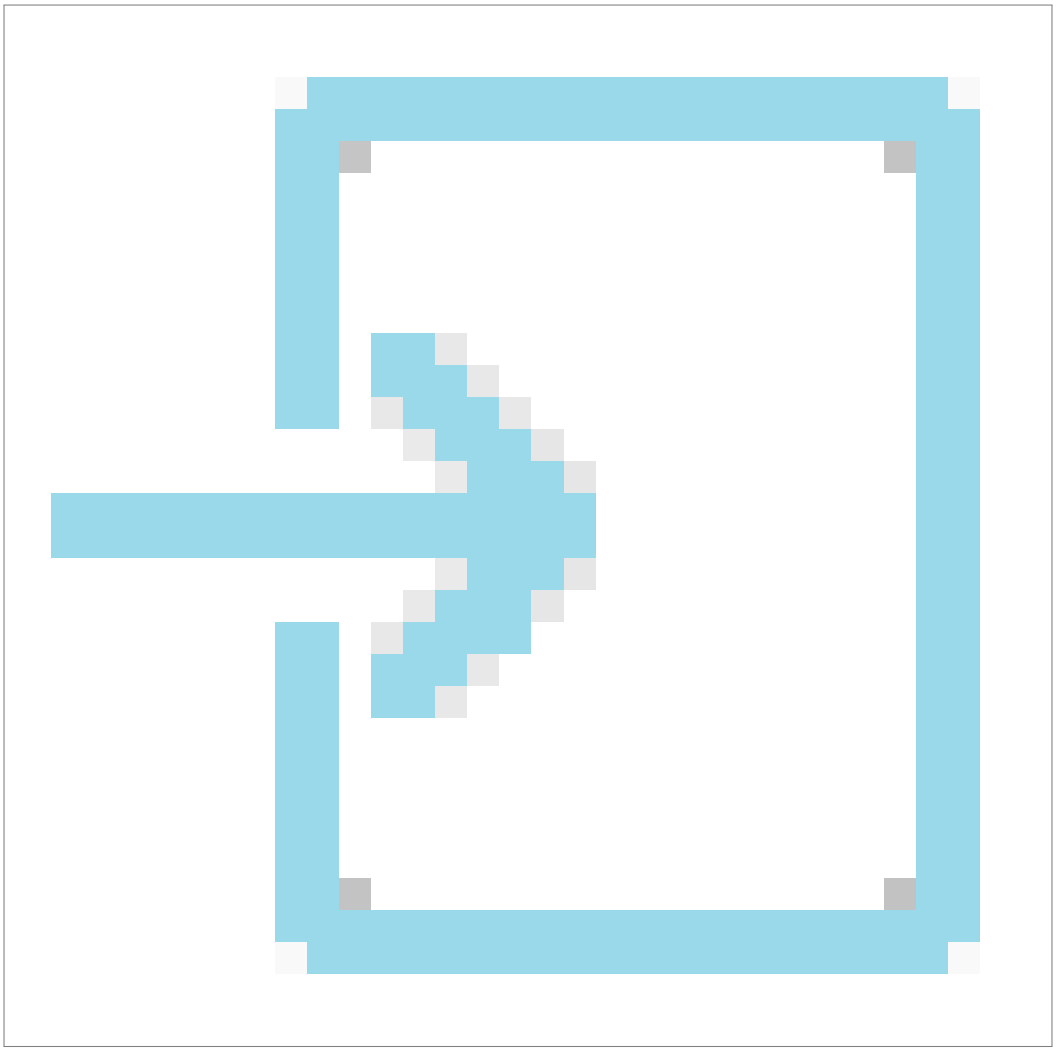
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: RCC

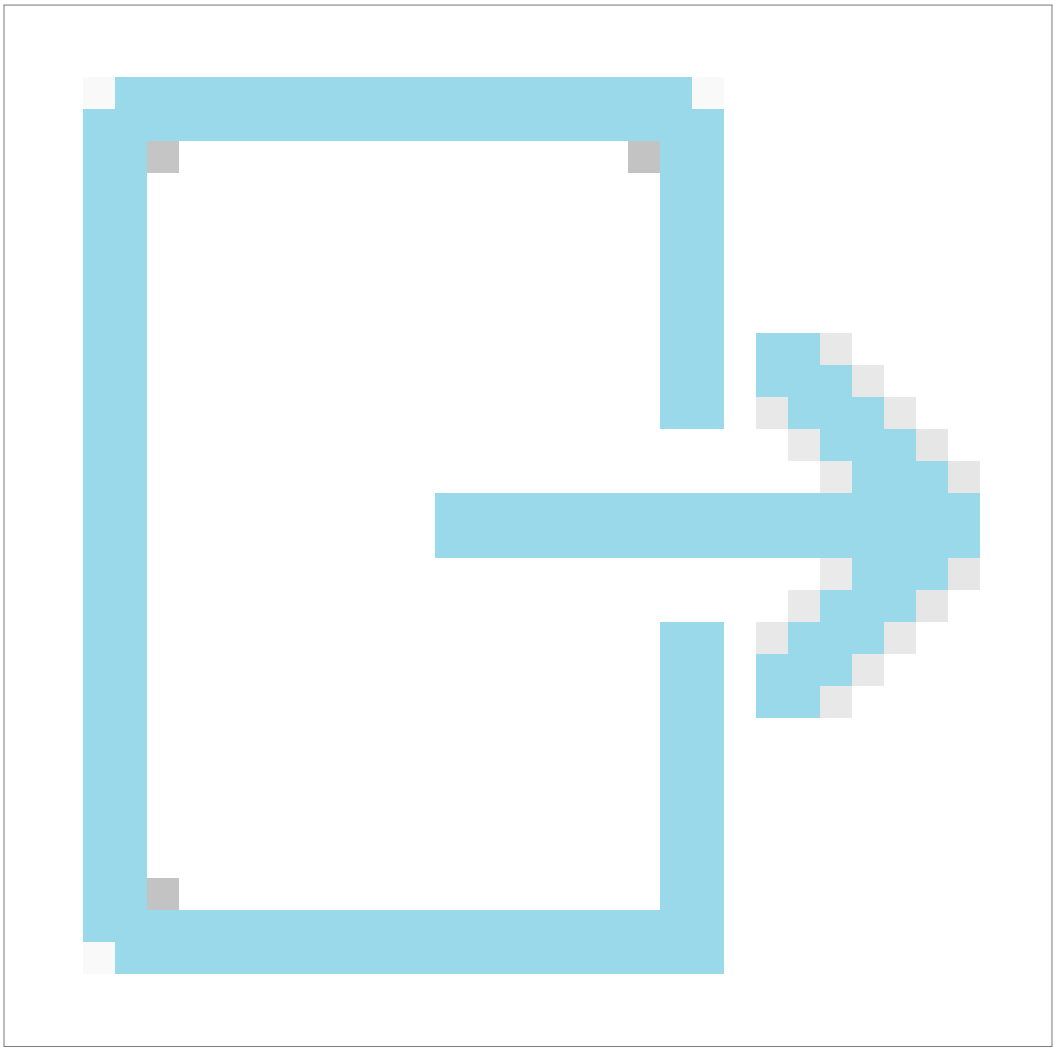
24.3 Absatz 3

ENTSO-E legt die regionalen Pläne zur Minderung des Cybersicherheitsrisikos den relevanten Übertragungsnetzbetreibern, den zuständigen Behörden und der Koordinierungsgruppe „Strom“ vor. Die Koordinierungsgruppe „Strom“ kann Änderungen empfehlen.



Input

- Regionaler Risikominderungsplan



Output

- Änderungsantrag

A

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

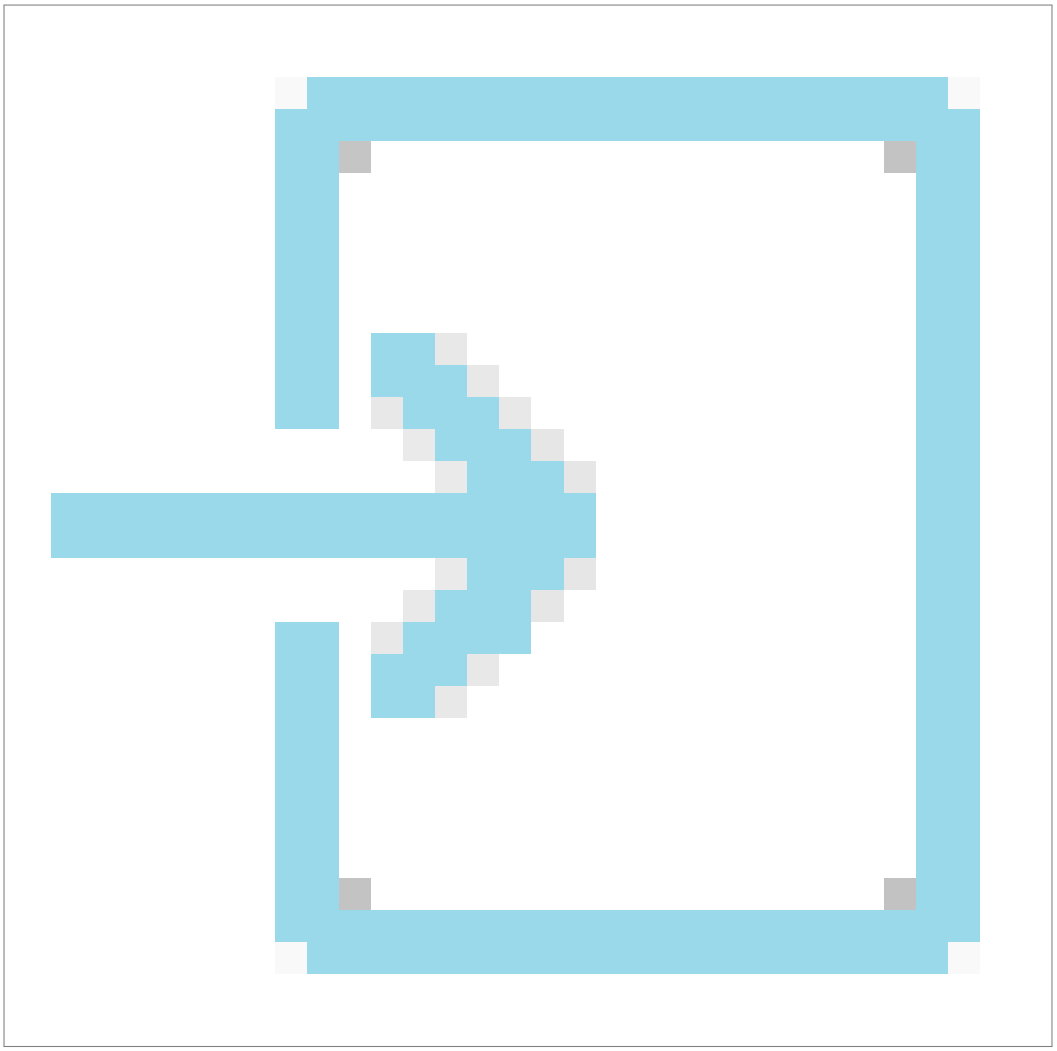
R

Beteiligt an der Aufgabenausführung: ENTSO-E, ECG

Zu informieren: TSO, NCA

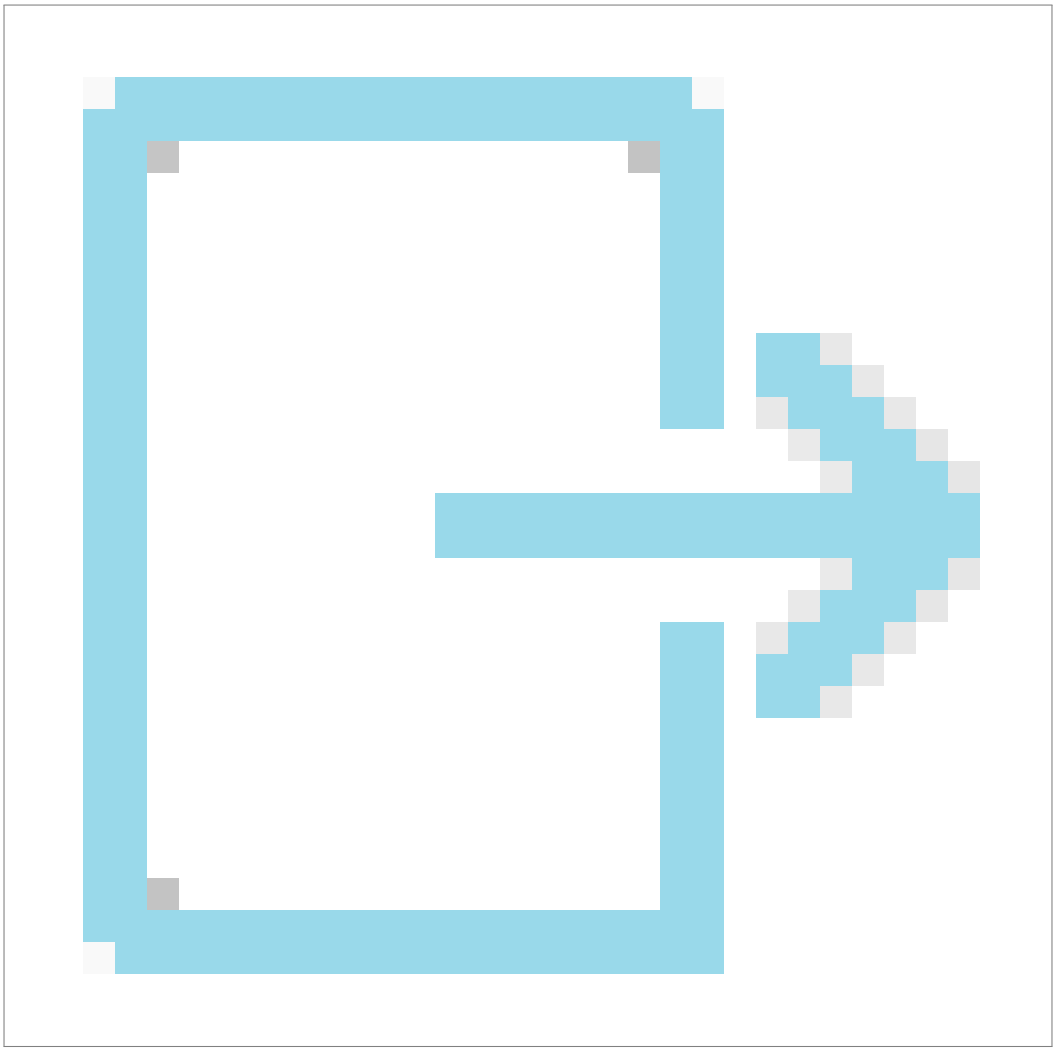
24.4 Absatz 4

Die ÜNB aktualisieren mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe die regionalen Risikominderungspläne alle drei Jahre, soweit aufgrund der Umstände keine häufigere Aktualisierung erforderlich ist.



Input

- Regionaler Risikominderungsplan



Output

- Regionaler Risikominderungsplan

GOOD TO KNOW

Rekurrenz

mindestens 3 Jahre

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: NIS CG, RCC

Chapter 25

Artikel 23. : Umfassender Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse

25.1 Absatz 1

Innerhalb von 40 Monaten nach Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre übermitteln die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe der Koordinierungsgruppe „Strom“ einen Bericht über die Ergebnisse der Bewertung der Cybersicherheitsrisiken in Bezug auf grenzüberschreitende Stromflüsse (im Folgenden „umfassender Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse“).

Relevante NCCS-Artikel

- Artikel 24 (6)

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Oktober 2031

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: NIS CG

Zu informieren: ECG

25.2 Absatz 2

Der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse stützt sich auf den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos, die Berichte der Mitgliedstaaten über die Bewertung des Cybersicherheitsrisikos und die Berichte über die regionale Bewertung des Cybersicherheitsrisikos und muss folgende Informationen enthalten:

a. die Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen, die im Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 2 Buchstabe a ermittelt wurden, einschließlich der Schätzung der Wahrscheinlichkeit und der Auswirkungen von Cybersicherheitsrisiken, die in den Berichten über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 und Artikel 19 Absatz 3 Buchstabe a bewertet wurden;

b. aktuelle Cyberbedrohungen, insbesondere neu aufkommende Bedrohungen und Risiken für das Elektrizitätssystem;

c. Cyberangriffe im vorangegangenen Zeitraum auf Unionsebene mit einem kritischen Überblick darüber, wie sich diese Cyberangriffe auf grenzüberschreitende Stromflüsse ausgewirkt haben könnten;

d. allgemeiner Stand der Umsetzung der Cybersicherheitsmaßnahmen;

e. Stand der Umsetzung der Informationsflüsse gemäß den Artikeln 37 und 38;

f. Liste der Informationen oder spezifische Kriterien für die Klassifizierung von Informationen gemäß Artikel 46;

g. ermittelte und besonders zu beachtende Risiken, die sich aus einem unsicheren Lieferkettenmanagement ergeben können;

h. Ergebnisse der regionalen und überregionalen Cybersicherheitsübungen gemäß Artikel 44 und dabei insgesamt gewonnene Erfahrungen;

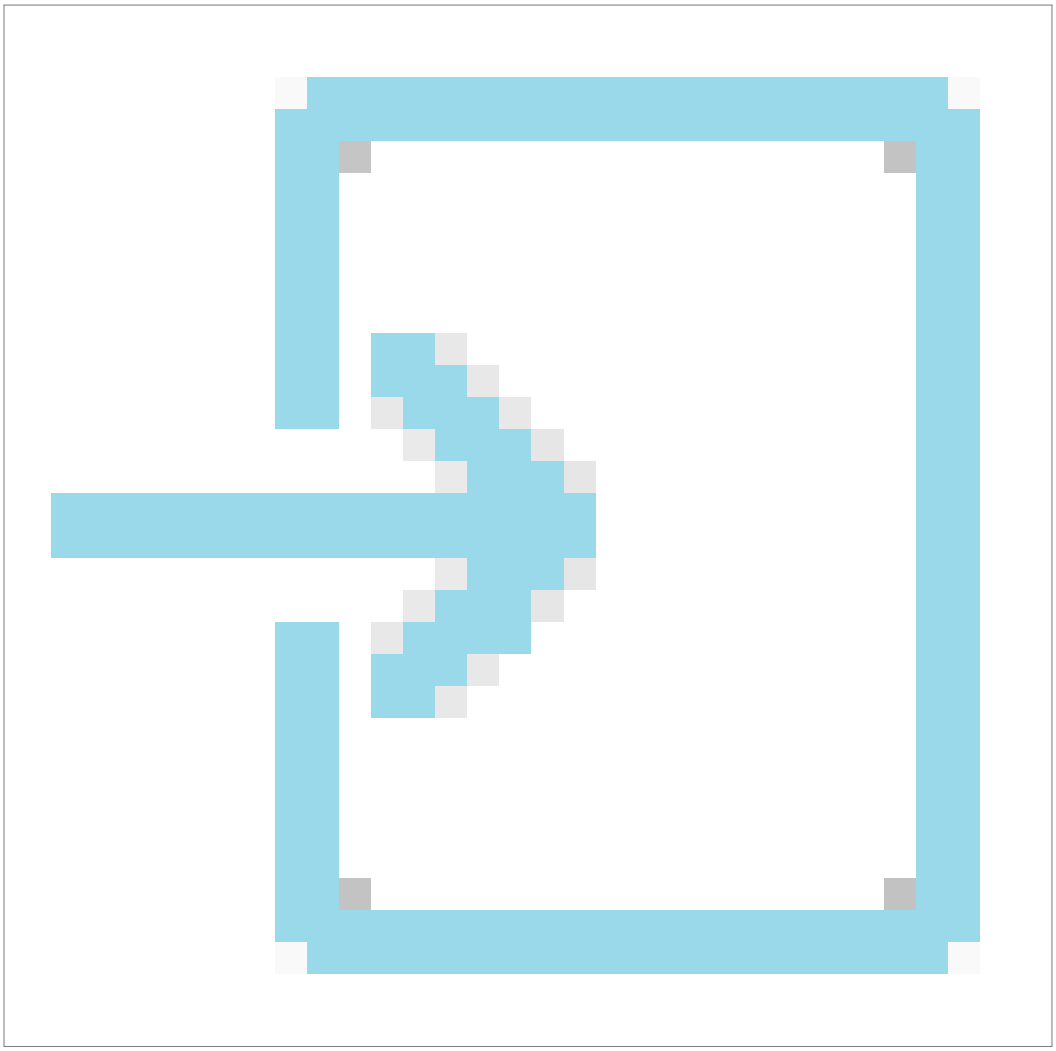
i. eine Analyse der Entwicklung des allgemeinen Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse seit den letzten regionalen Bewertungen des Cybersicherheitsrisikos;

j. alle sonstigen Informationen, die nützlich sein können, um mögliche Verbesserungen dieser Verordnung oder die Notwendigkeit einer Überarbeitung dieser Verordnung oder ihrer Instrumente zu ermitteln, sowie

k. aggregierte und anonymisierte Informationen über die gemäß Artikel 30 Absatz 3 gewährten Ausnahmen.

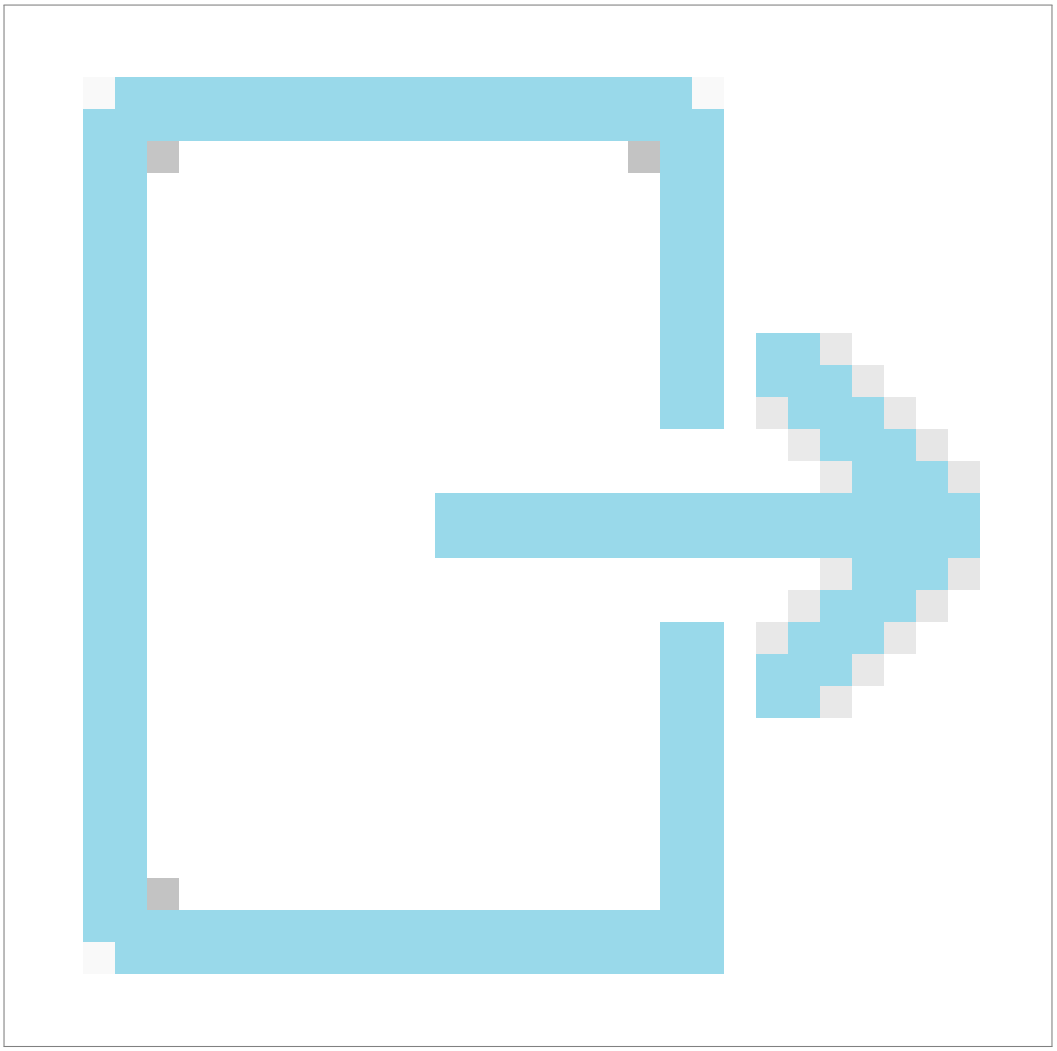
Relevante NCCS-Artikel

- Artikel 19 (2)
- Artikel 19 (3)
- Artikel 21 (2)
- Artikel 37
- Artikel 38
- Artikel 44
- Artikel 30 (3)



Input

- Risikobewertungsbericht auf Unionsebene
- Risikobewertung auf Ebene der Mitgliedstaaten
- Regionale Risikobewertung



Output

- Umfassender Bericht zur Bewertung grenzüberschreitender Cybersicherheitsrisiken im Stromsektor

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: NIS CG

25.3 Absatz 3

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen können zur Ausarbeitung des umfassenden Berichts über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse beitragen, wobei sie die Vertraulichkeit der Informationen gemäß Artikel 47 wahren müssen. Die ÜNB konsultieren diese Einrichtungen mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO frühzeitig.

Relevante NCCS-Artikel

- Artikel 47
- Artikel 2 (1)

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

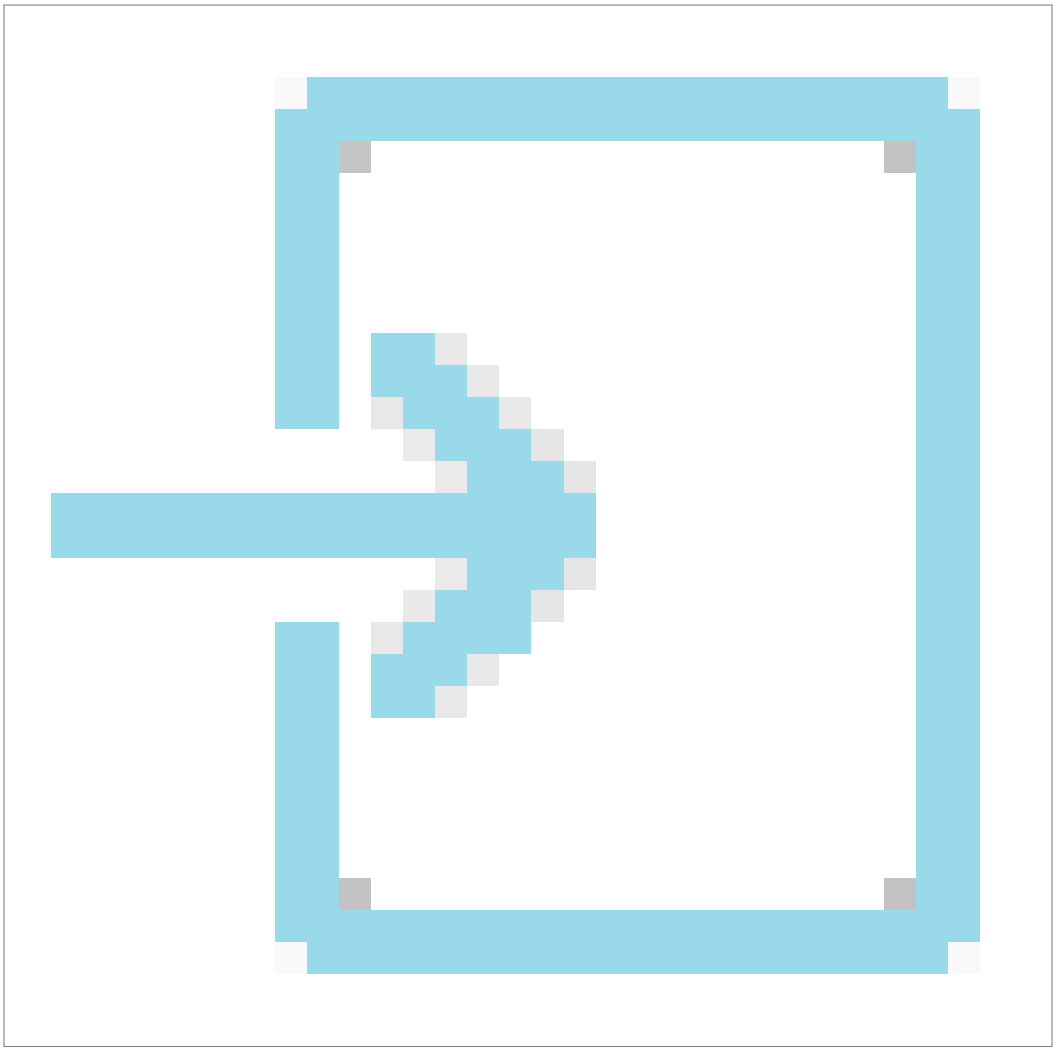
Beteiligt an der Aufgabenausführung: HIE, CIE, ENTSO-E, TSO, EU DSO

25.4 Absatz 4

Der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse unterliegt den Bestimmungen des Artikels 46 über den Schutz ausgetauschter Informationen. Unbeschadet des Artikels 10 Absatz 4 und des Artikels 47 Absatz 4 veröffentlichen ENTSO-E und die EU-VNBO eine öffentliche Fassung dieses Berichts, die keine Informationen enthält, die den in Artikel 2 Absatz 1 aufgeführten Einrichtungen schaden können.

Relevante NCCS-Artikel

- Artikel 46
- Artikel 20 (4)
- Artikel 47 (4)
- Artikel 2 (1)



Input

- Umfassender Bericht zur Bewertung grenzüberschreitender Cybersicherheitsrisiken im Stromsektor

Verantwortlich für die Aktivität: TSO

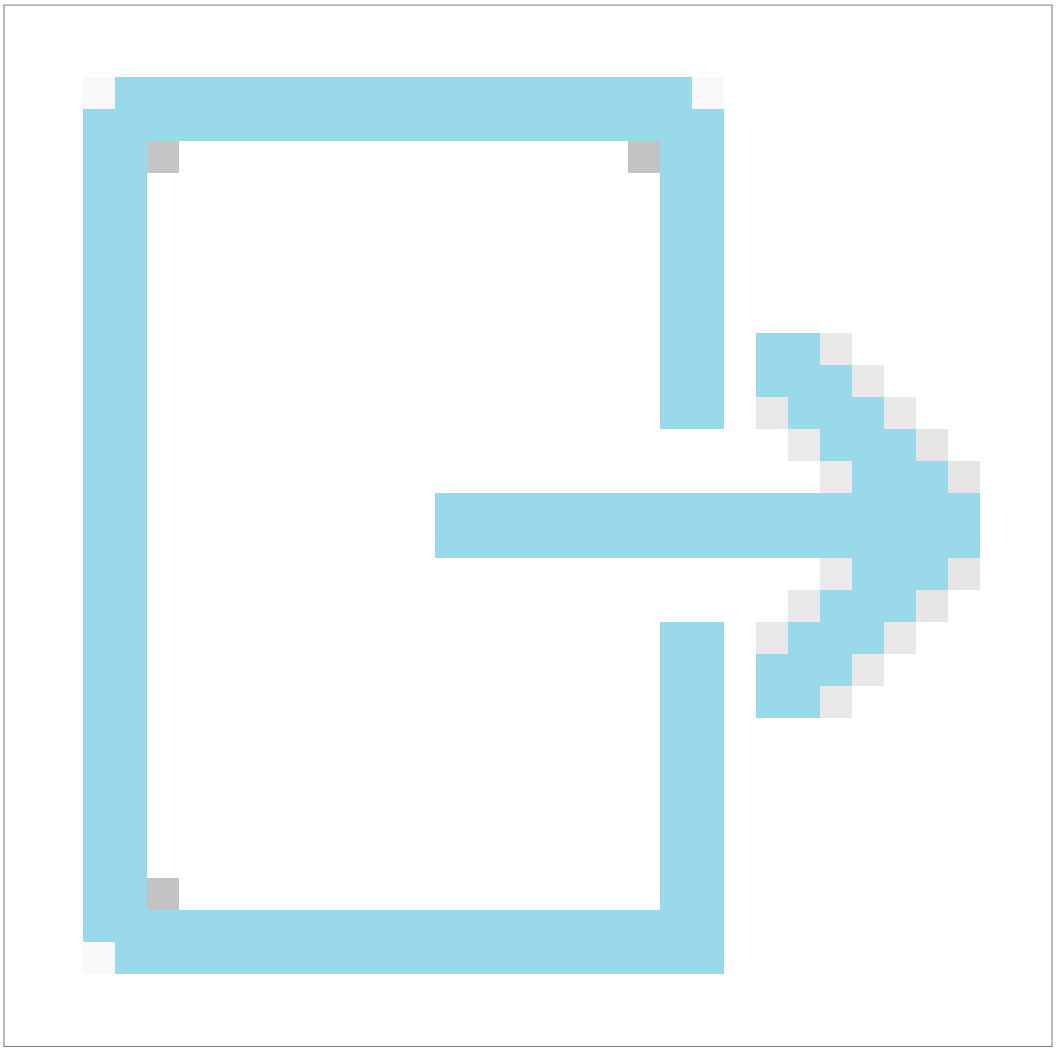
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: NIS CG

25.5 Absatz 4

Die öffentliche Fassung dieses Berichts wird nur mit Zustimmung der NIS-Kooperationsgruppe und der Koordinierungsgruppe „Strom“ veröffentlicht. ENTSO-E ist in Abstimmung mit der EU-VNBO für die Zusammenstellung und Veröffentlichung der öffentlichen Fassung des Berichts verantwortlich.



Output

- Umfassender Bericht zur Bewertung grenzüberschreitender Cybersicherheitsrisiken im Stromsektor (veröffentlicht)

A

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO, NIS CG, ECG

Chapter 26

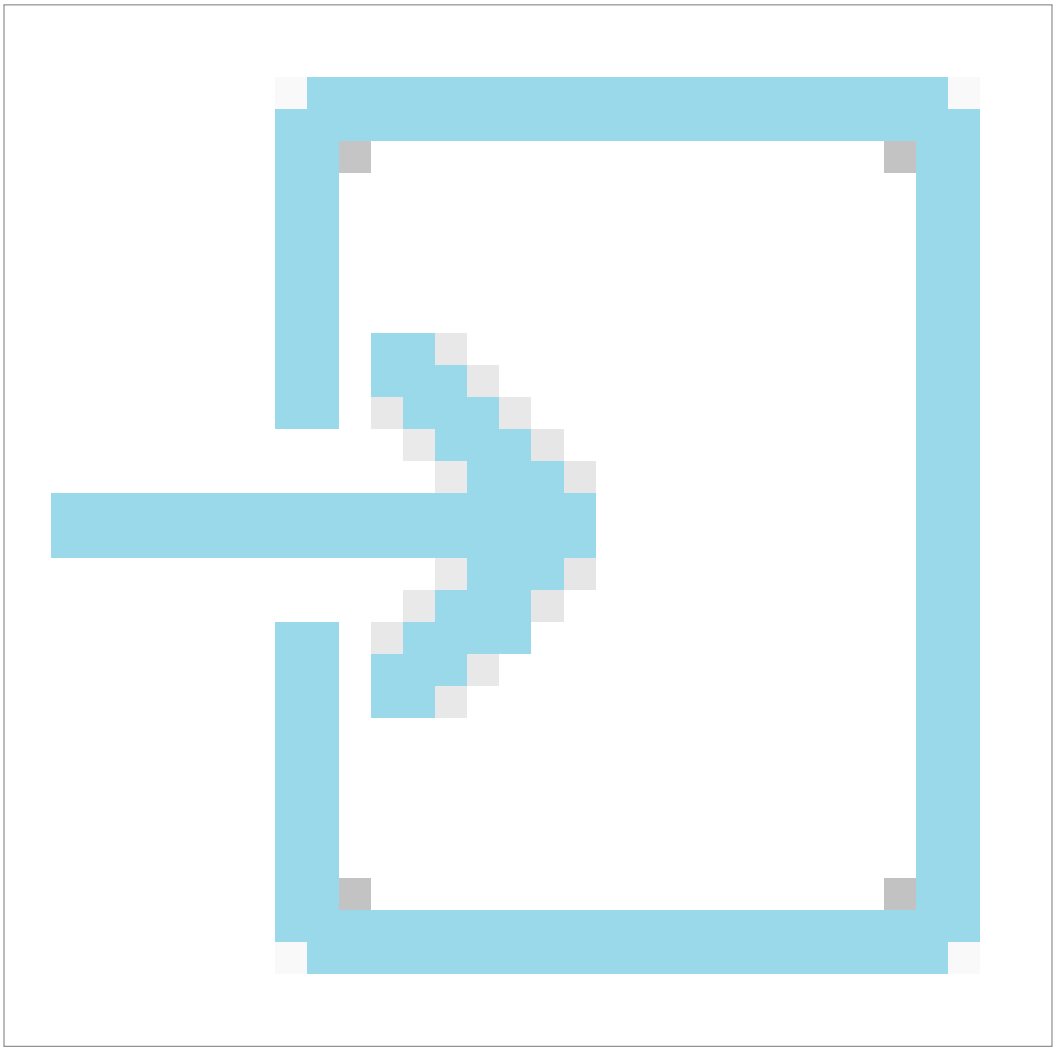
Artikel 24. : Ermittlung von Einrichtungen mit erheblichen oder kritischen Auswirkungen

26.1 Absatz 1

Jede zuständige Behörde ermittelt anhand des ECII und der Schwellenwerte für erhebliche und kritische Auswirkungen, die im Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 3 Buchstabe b enthalten sind, die Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat, die an unionsweiten Prozessen mit erheblichen bzw. kritischen Auswirkungen beteiligt sind. Die zuständigen Behörden können von einer Einrichtung in ihrem Mitgliedstaat Informationen anfordern, um die ECII-Werte für diese Einrichtung zu bestimmen. Liegt der ermittelte ECII einer Einrichtung über dem Schwellenwert für erhebliche oder kritische Auswirkungen, wird die ermittelte Einrichtung in dem in Artikel 20 Absatz 2 genannten Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats aufgeführt.

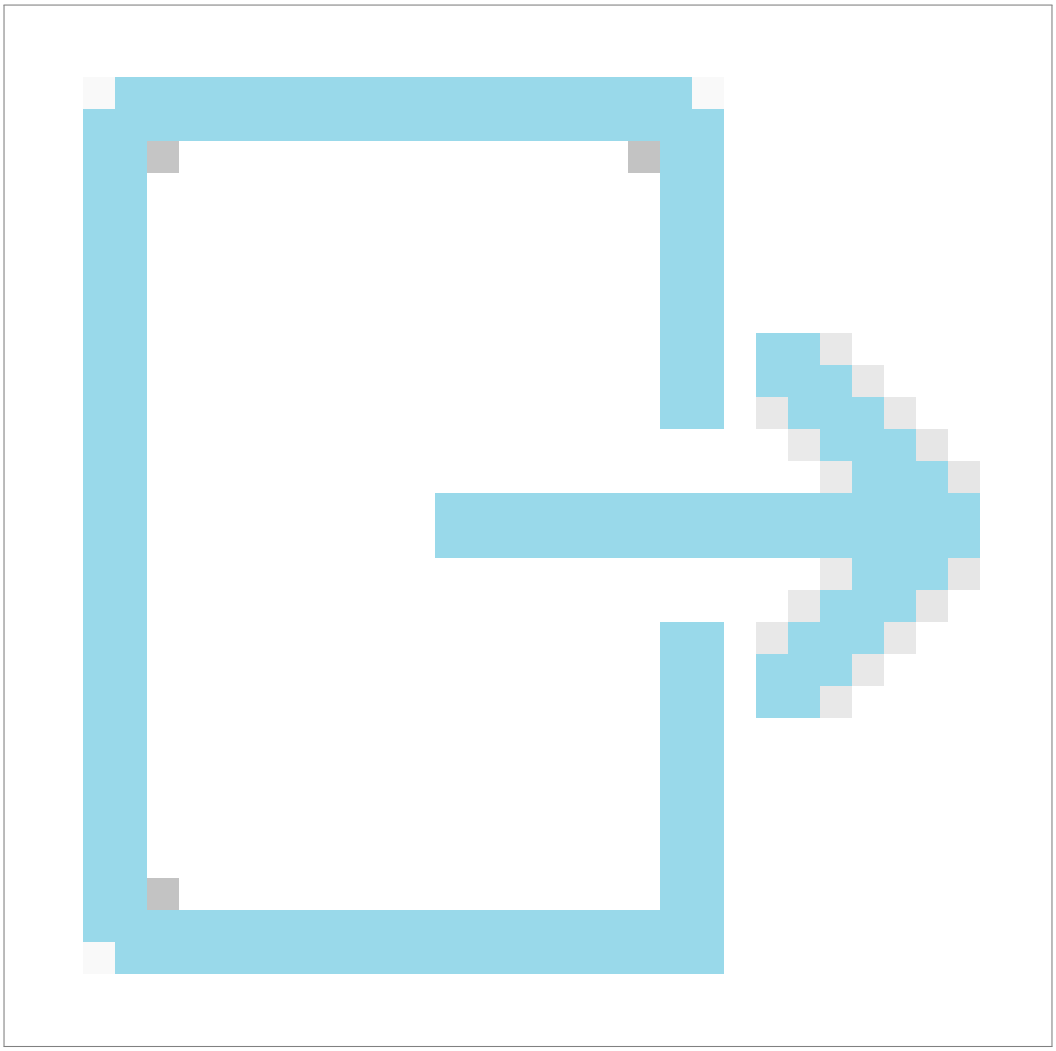
Relevante NCCS-Artikel

- Artikel 19 (3)
- Artikel 20 (2)



Input

- Unionsweiter Risikobewertungsbericht
- ECII
- Unionsweite Prozesse mit erheblicher und kritischer Auswirkung



Output

- Identifizierte Organisationen

A

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA

26.2 Absatz 2

Jede zuständige Behörde ermittelt anhand des ECII und der Schwellenwerte für erhebliche und kritische Auswirkungen aus dem Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 3 Buchstabe b die nicht in der Union niedergelassenen Einrichtungen mit erheblichen oder kritischen Auswirkungen, soweitsie in der Union tätig sind. Die zuständige Behörde kann von einer nicht in der Union niedergelassenen Einrichtung Informationen anfordern, um die ECII-Werte für die Einrichtung zu bestimmen.

Relevante NCCS-Artikel

- Artikel 19 (3)

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

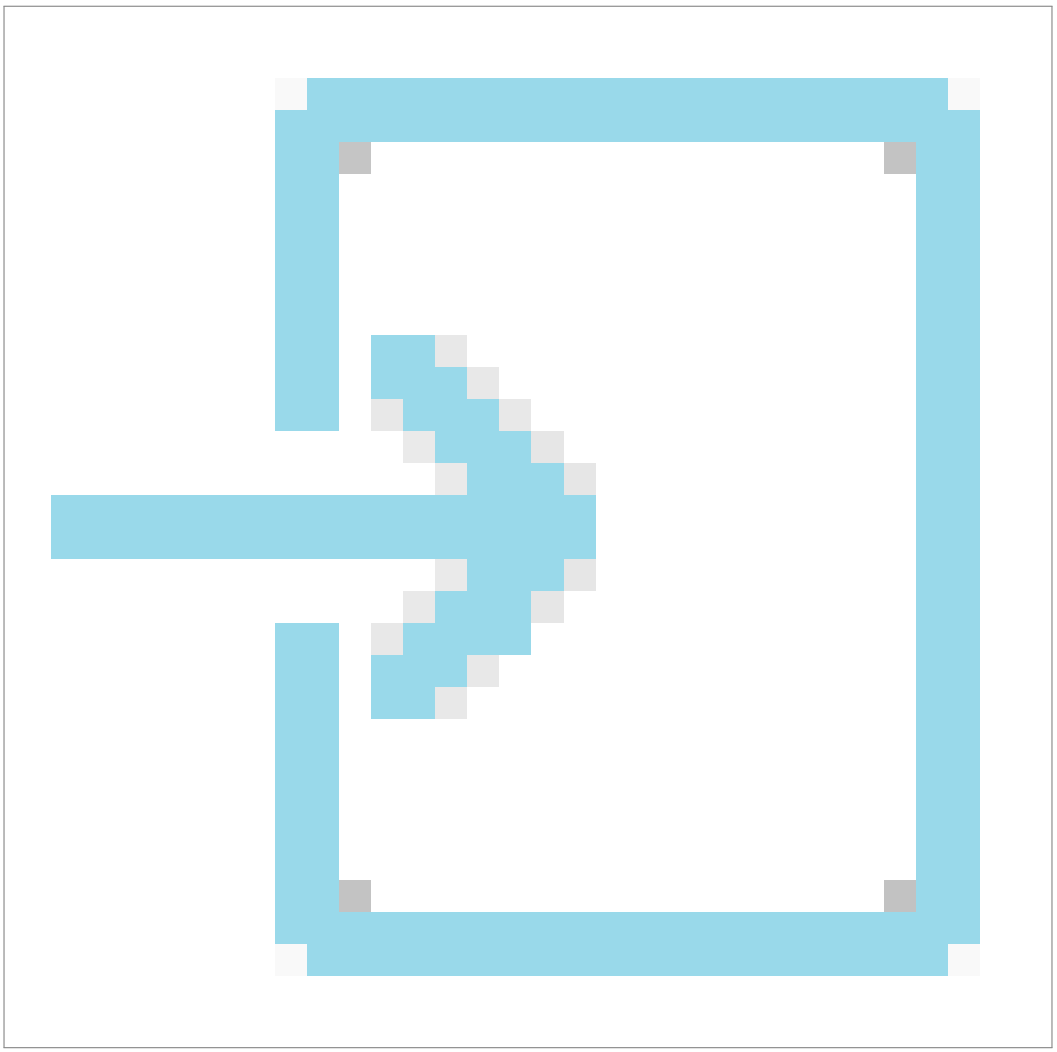
Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA

26.3 Absatz 3

Jede zuständige Behörde kann weitere Einrichtungen in ihrem Mitgliedstaat als Einrichtungen mit erheblichen oder kritischen Auswirkungen einstufen, wenn die folgenden Kriterien erfüllt sind:

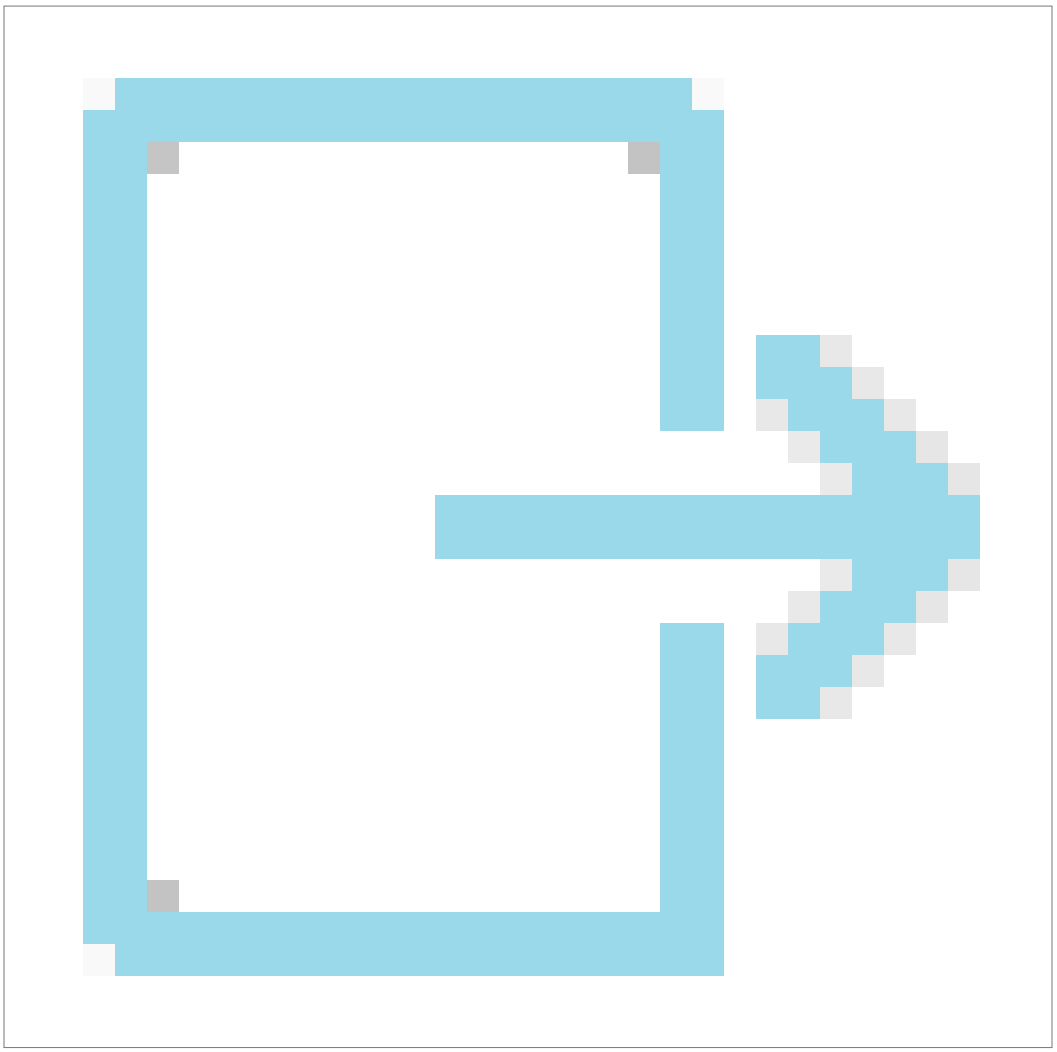
a. Die Einrichtung ist Teil einer Gruppe von Einrichtungen, für die ein erhebliches Risiko besteht, dass sie zeitgleich Ziel eines Cyberangriffs sein könnten;

b. der über die Gruppe von Einrichtungen aggregierte ECII liegt über dem Schwellenwert für erhebliche oder kritische Auswirkungen.



Input

- Gruppierungskriterien



Output

- Identifizierte Unternehmen

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

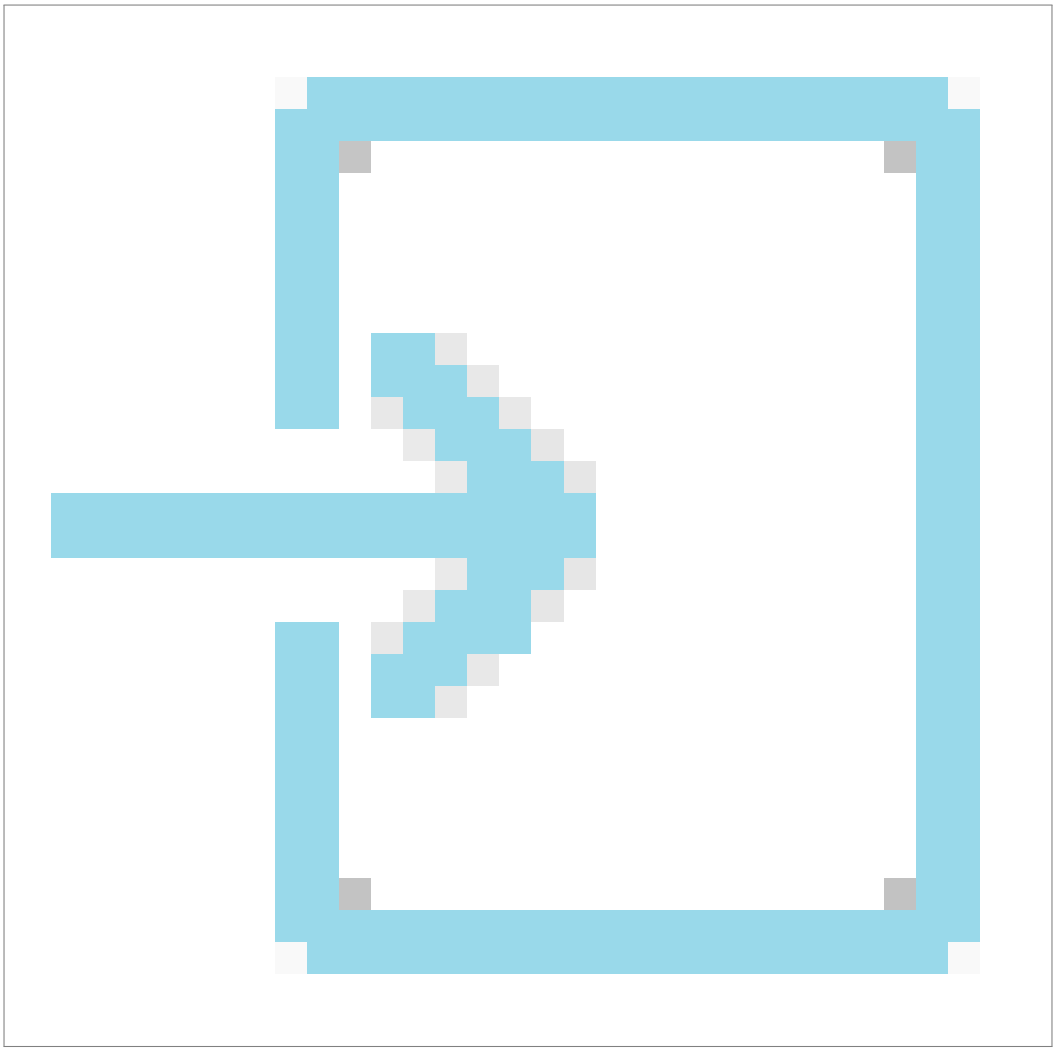
Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA

26.4 Absatz 4

Ermittelt eine zuständige Behörde gemäß Absatz 3 zusätzliche Einrichtungen, so gelten alle Prozesse dieser Einrichtungen, deren über die Gruppe aggregierter ECII über dem Schwellenwert für erhebliche Auswirkungen liegt, als Prozesse mit erheblichen Auswirkungen, und alle Prozesse, deren über die Gruppe aggregierter ECII über den Schwellenwerten für kritische Auswirkungen liegt, gelten als Prozesse mit kritischen Auswirkungen.

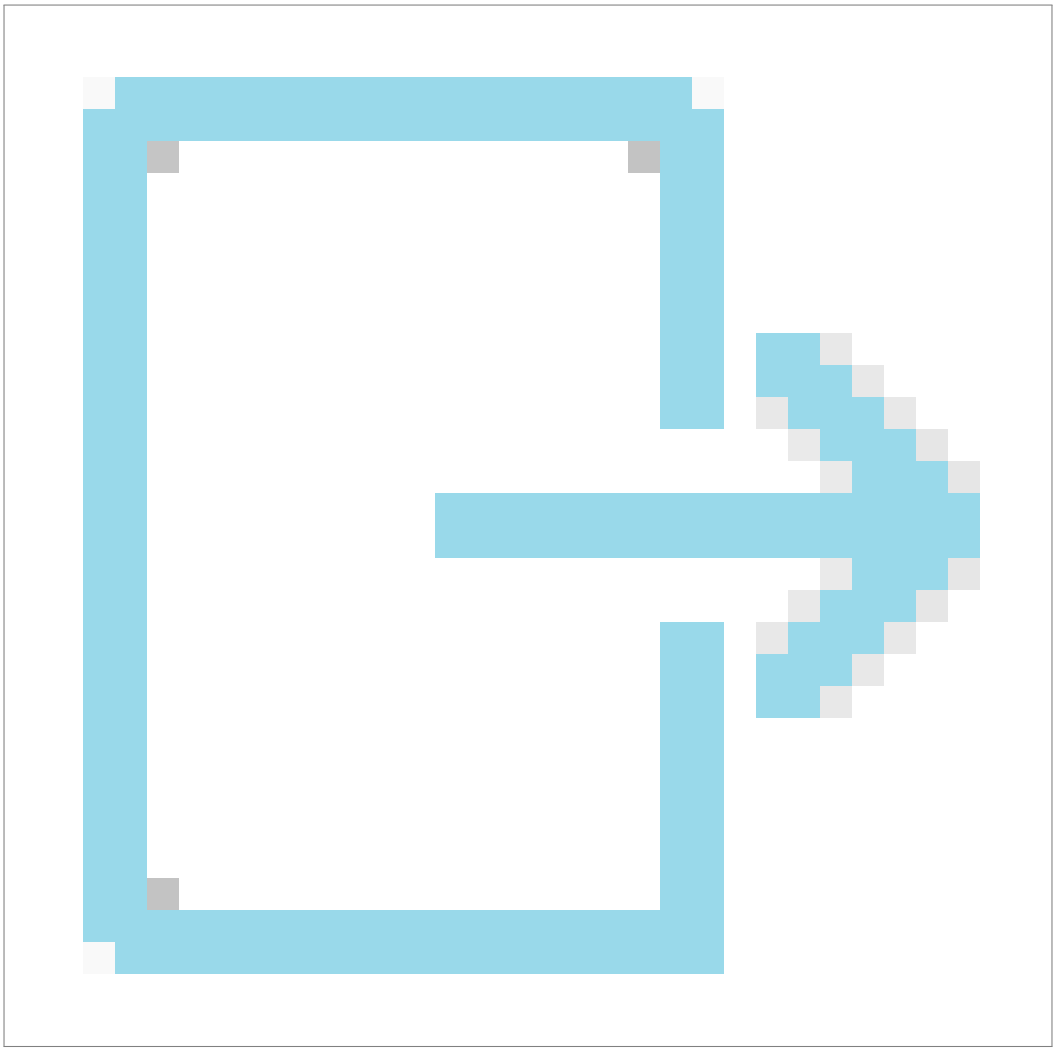
Relevante NCCS-Artikel

- Artikel 24 (3)



Input

- Unionsweiter Risikobewertungsbericht
- ECII
- Unionsweite Prozesse mit erheblicher und kritischer Auswirkung



Output

- Prozesse auf Unternehmensebene mit erheblicher und kritischer Auswirkung

A

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

R

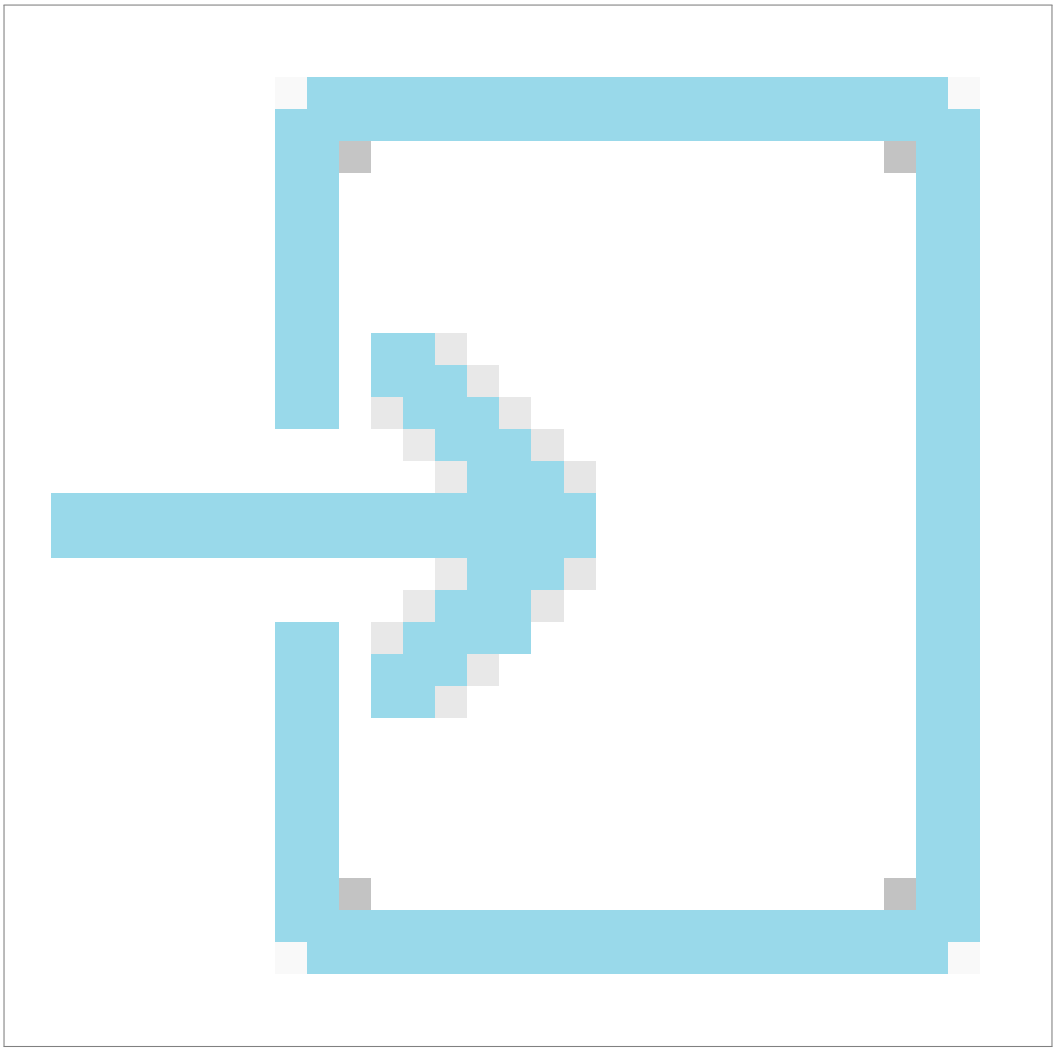
Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA

26.5 Absatz 5

Ermittelt eine zuständige Behörde Einrichtungen gemäß Absatz 3 Buchstabe a in mehr als einem Mitgliedstaat, so unterrichtet sie die anderen zuständigen Behörden, ENTSO-E und die EU-VNBO.

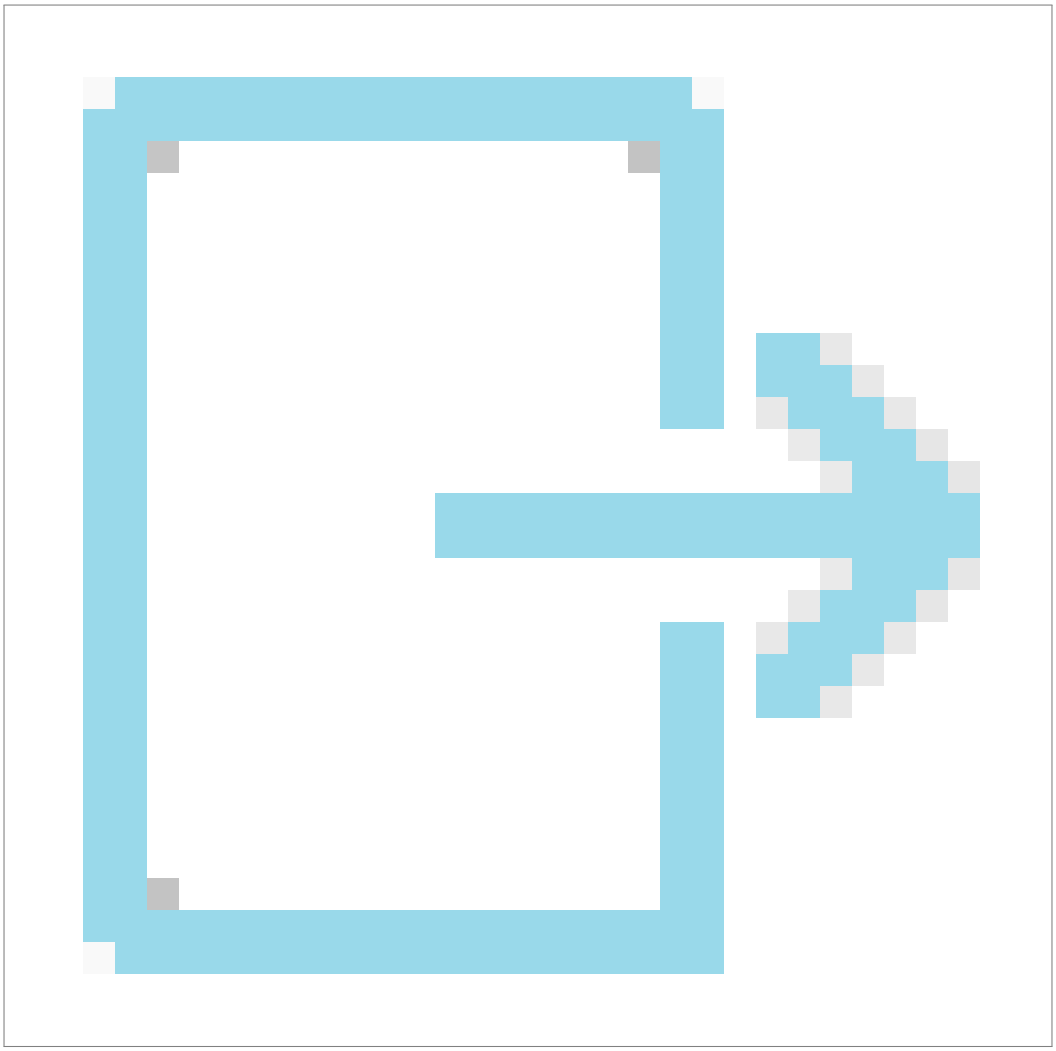
Relevante NCCS-Artikel

- Artikel 24 (3)



Input

- Identifizierte Unternehmen



Output

- Informationsaustausch

A

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

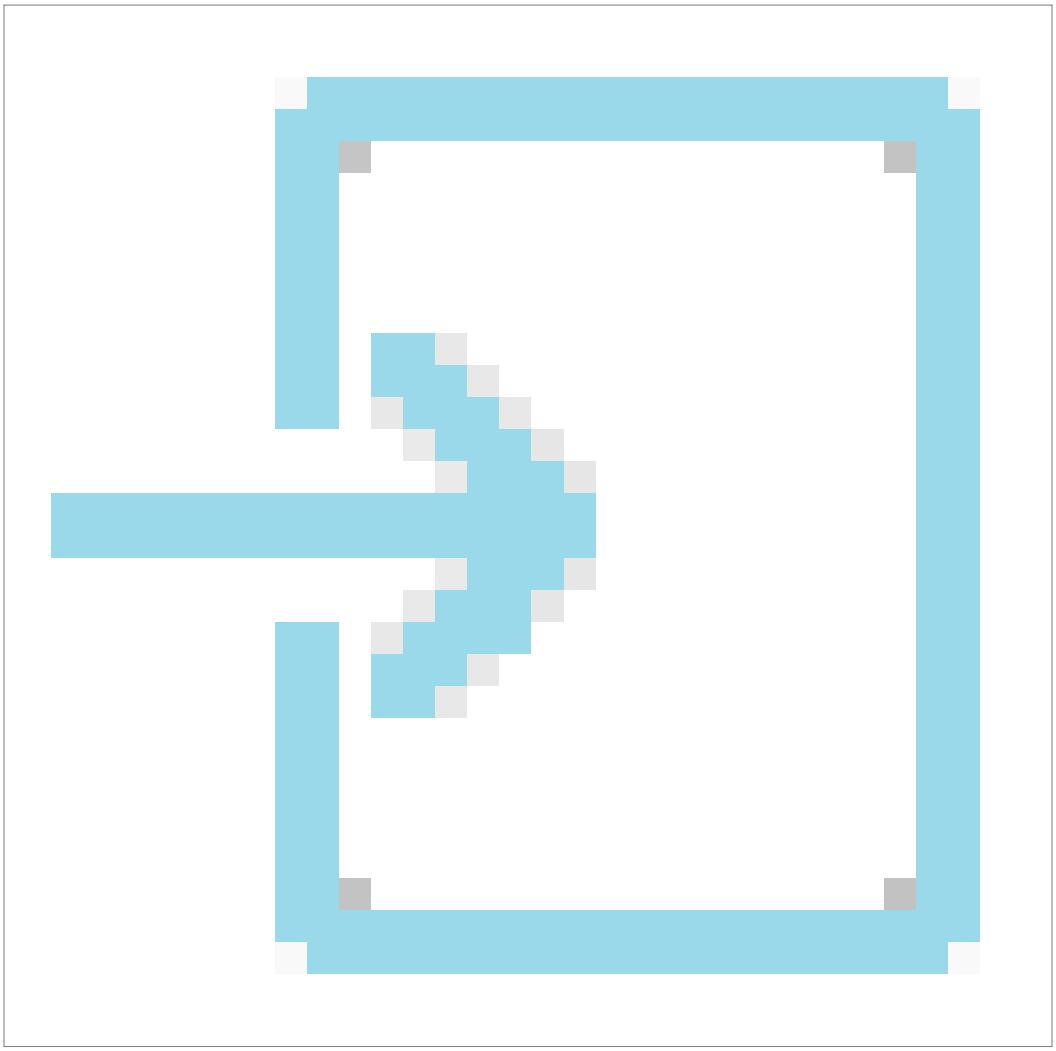
R

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA

Zu informieren: ENTSO-E, EU DSO

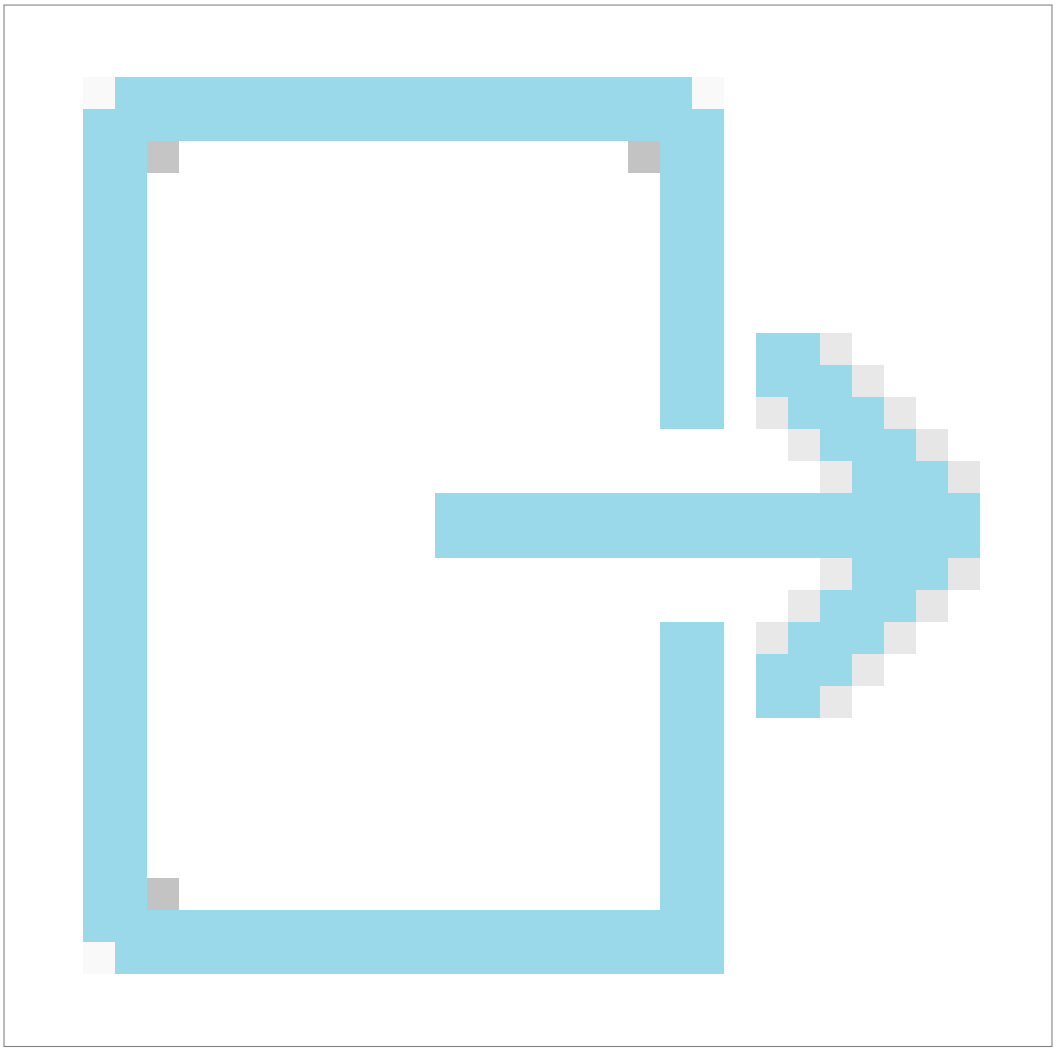
26.6 Absatz 5

ENTSO-E übermittelt den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO auf der Grundlage der von allen zuständigen Behörden übermittelten Informationen eine Analyse der Aggregierung von Einrichtungen in mehr als einem Mitgliedstaat, die zu einer von verschiedenen Punkten ausgehenden Störung der grenzüberschreitenden Stromflüsse führen und einen Cyberangriff nach sich ziehen können.



Input

- Informationsaustausch



Output

- Unionsweiter Bericht zur Bewertung von Cybersicherheitsrisiken

A

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu informieren: NCA

26.7 Absatz 5

Wird eine Gruppe von Einrichtungen in mehreren Mitgliedstaaten als Aggregierung ermittelt, deren ECII über dem Schwellenwert für erhebliche oder kritische Auswirkungen liegt, so stufen alle betroffenen zuständigen Behörden die Einrichtungen in dieser Gruppe für ihren jeweiligen Mitgliedstaat auf der Grundlage des aggregierten ECII für die Gruppe der Einrichtungen als Einrichtungen mit erheblichen bzw. kritischen Auswirkungen ein, und die ermittelten Einrichtungen werden in den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos aufgenommen.

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

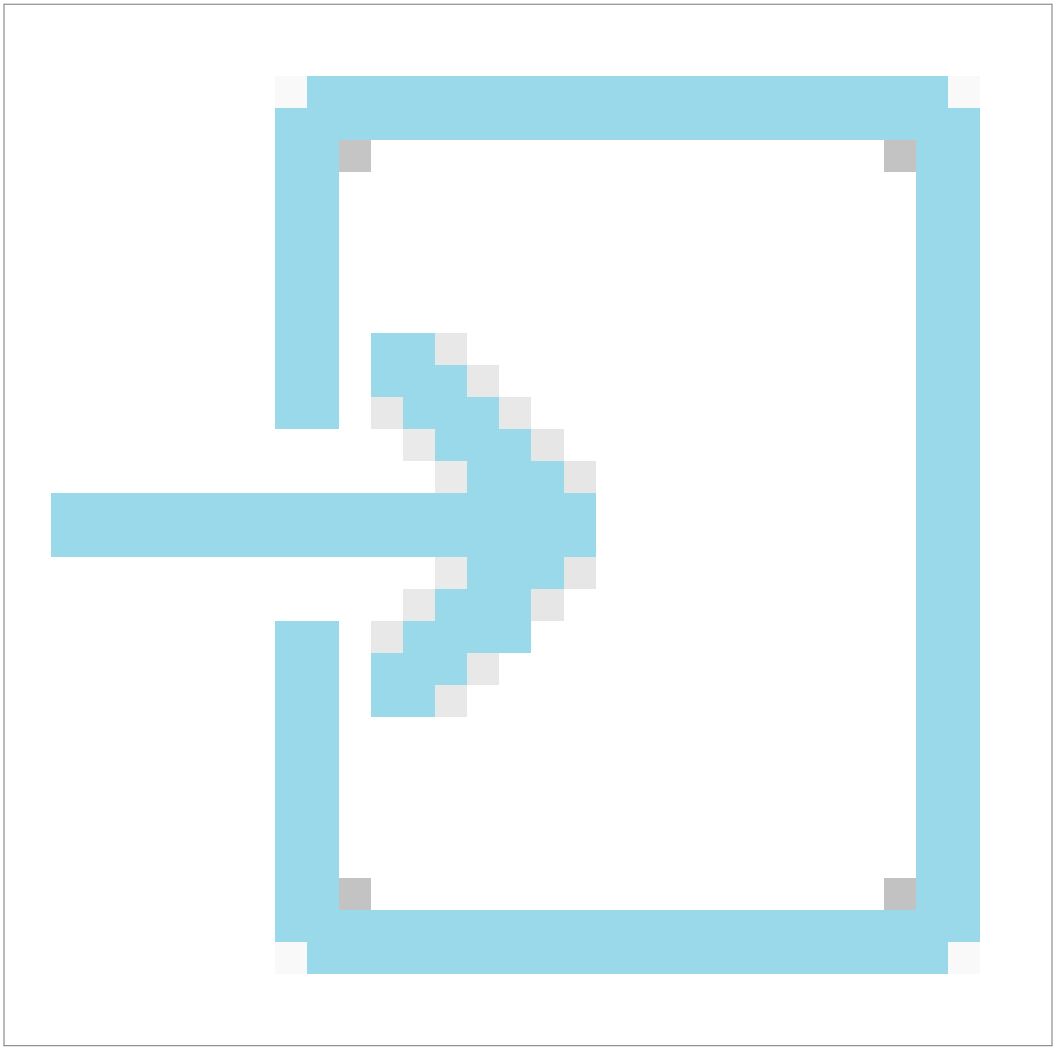
Beteiligt an der Aufgabenausführung: NCA

26.8 Absatz 6

Jede zuständige Behörde unterrichtet innerhalb von neun Monaten, nachdem ENTSO-E und die EU-VNBO den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 5 übermittelt haben, spätestens jedoch bis zum 13 Juni 2028, die in der Liste aufgeführten Einrichtungen, dass sie in ihrem Mitgliedstaat als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

Relevante NCCS-Artikel

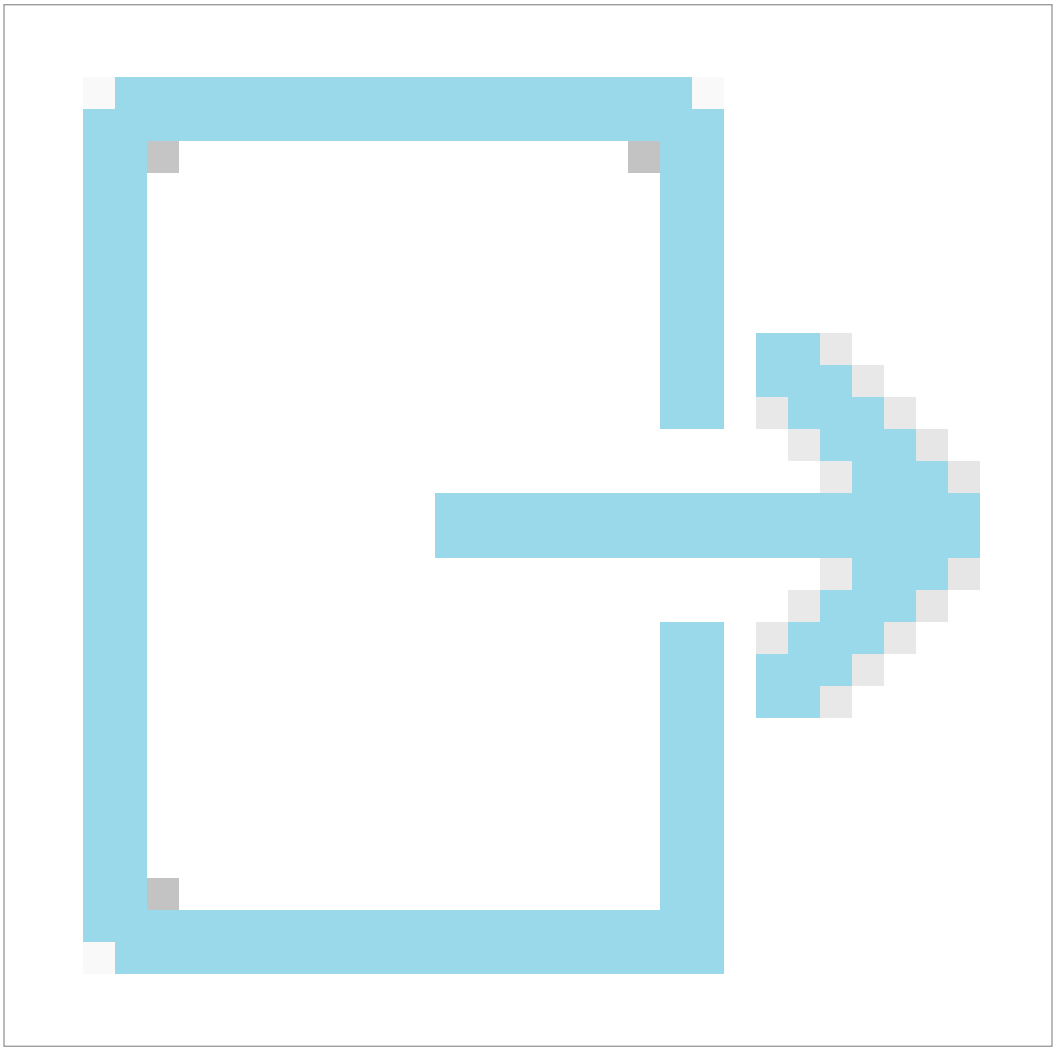
- Artikel 19 (5)



Input

- Unionsweiter Risikobewertungsbericht

- ECII
- Unionsweite Prozesse mit erheblicher und kritischer Auswirkung



Output

- Identifizierte Unternehmen

GOOD TO KNOW

Zeitpunkt

> Bis zum 13. Juni 2028

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu informieren: HIE, CIE

26.9 Absatz 7

> Wird einer zuständigen Behörde ein Diensteanbieter als Anbieter kritischer IKT-Dienste gemäß Artikel 27 Buchstabe c gemeldet,

Relevante NCCS-Artikel

- Artikel 27

Verantwortlich für die Aktivität: HIE, CIE, TSO

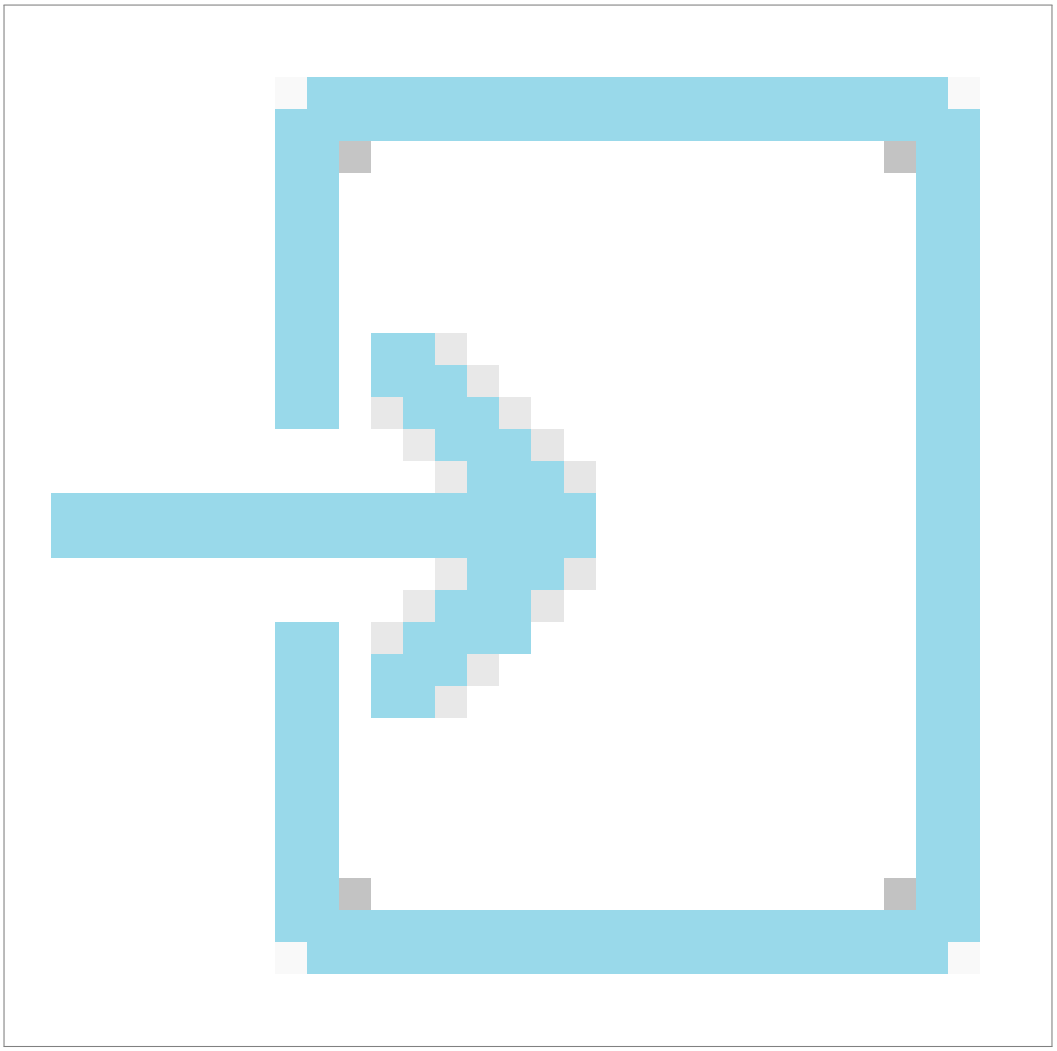
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Zu informieren: NCA, Critical ICT

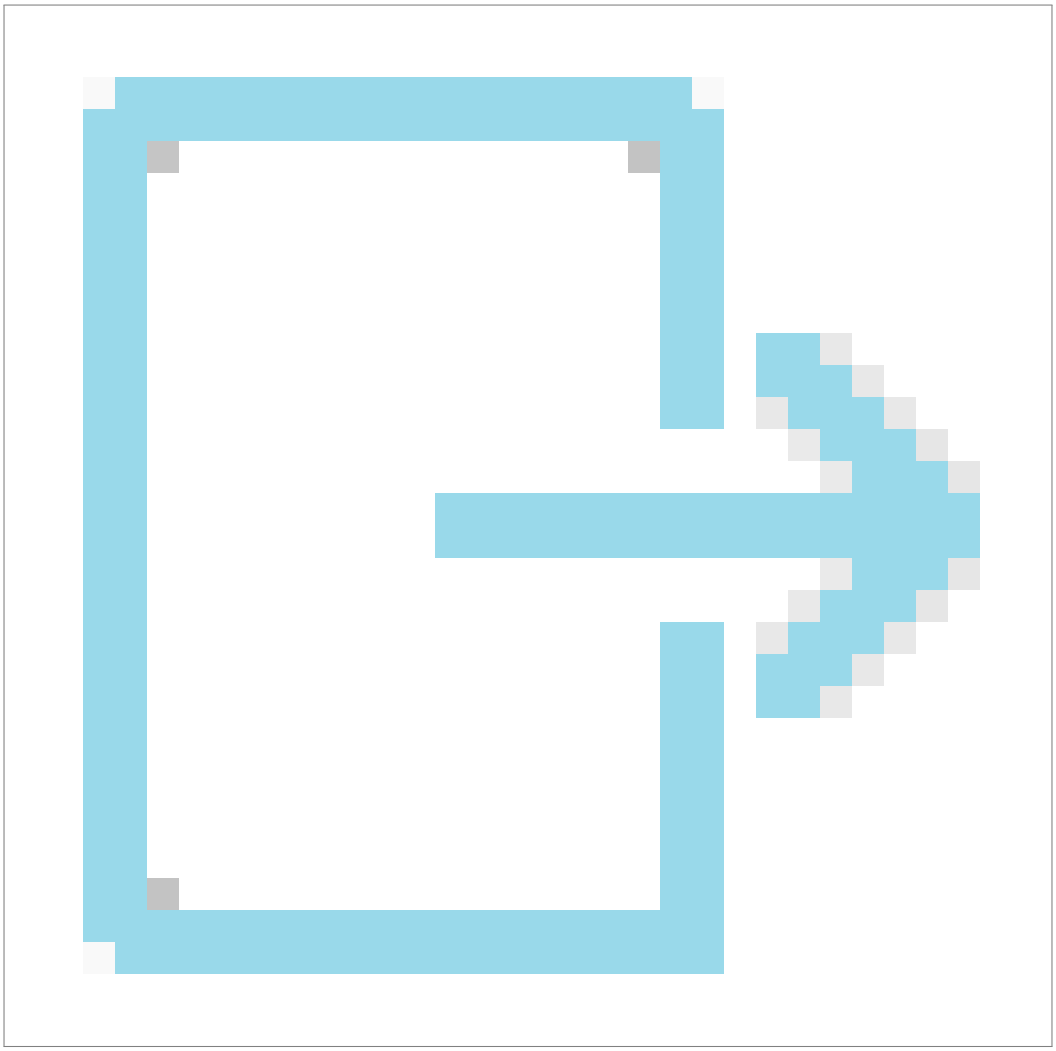
26.10 Absatz 7

so teilt sie dies den zuständigen Behörden der Mitgliedstaaten mit, in deren Hoheitsgebiet sich der Sitz oder der Vertreter befindet. Die letztgenannte zuständige Behörde teilt dem Diensteanbieter mit, dass er als Anbieter kritischer Dienste eingestuft wurde.



Input

- Identifizierte kritische IKT-Anbieter



Output

- Informationsaustausch

A

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA

Zu informieren: Critical ICT

Chapter 27

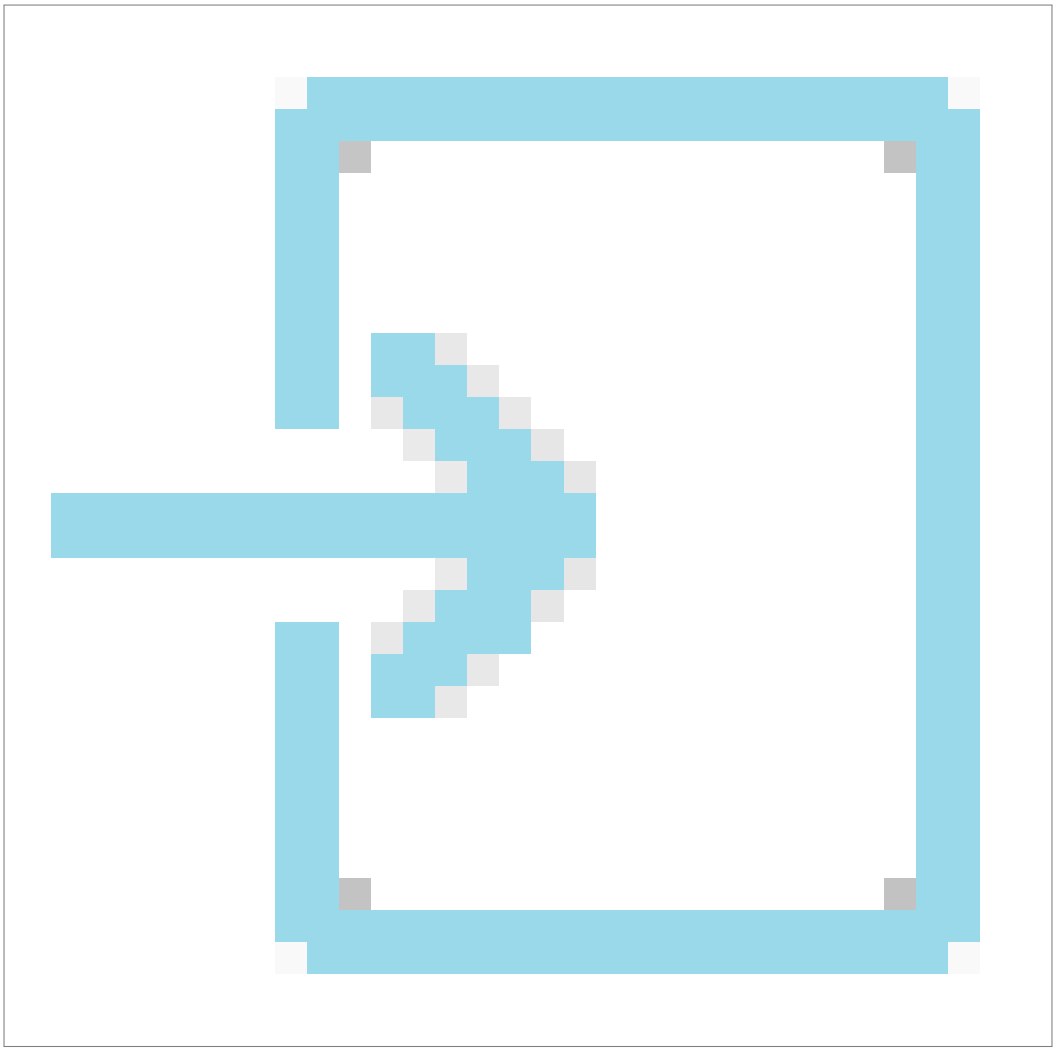
Artikel 25. : Nationale Überprüfungssysteme

27.1 Absatz 1

Die zuständigen Behörden können ein nationales Überprüfungssystem einrichten, um zu überprüfen, ob die gemäß Artikel 24 Absatz 1 ermittelten Einrichtungen mit kritischen Auswirkungen den nationalen Rechtsrahmen umgesetzt haben, der in der Vergleichsmatrix gemäß Artikel 34 aufgeführt ist. Das nationale Überprüfungssystem kann sich auf eine von der zuständigen Behörde durchgeführte Inspektion, unabhängige Sicherheitsaudits oder gegenseitige Peer Reviews durch Einrichtungen mit kritischen Auswirkungen in demselben Mitgliedstaat, die von der zuständigen Behörde beaufsichtigt werden, stützen.

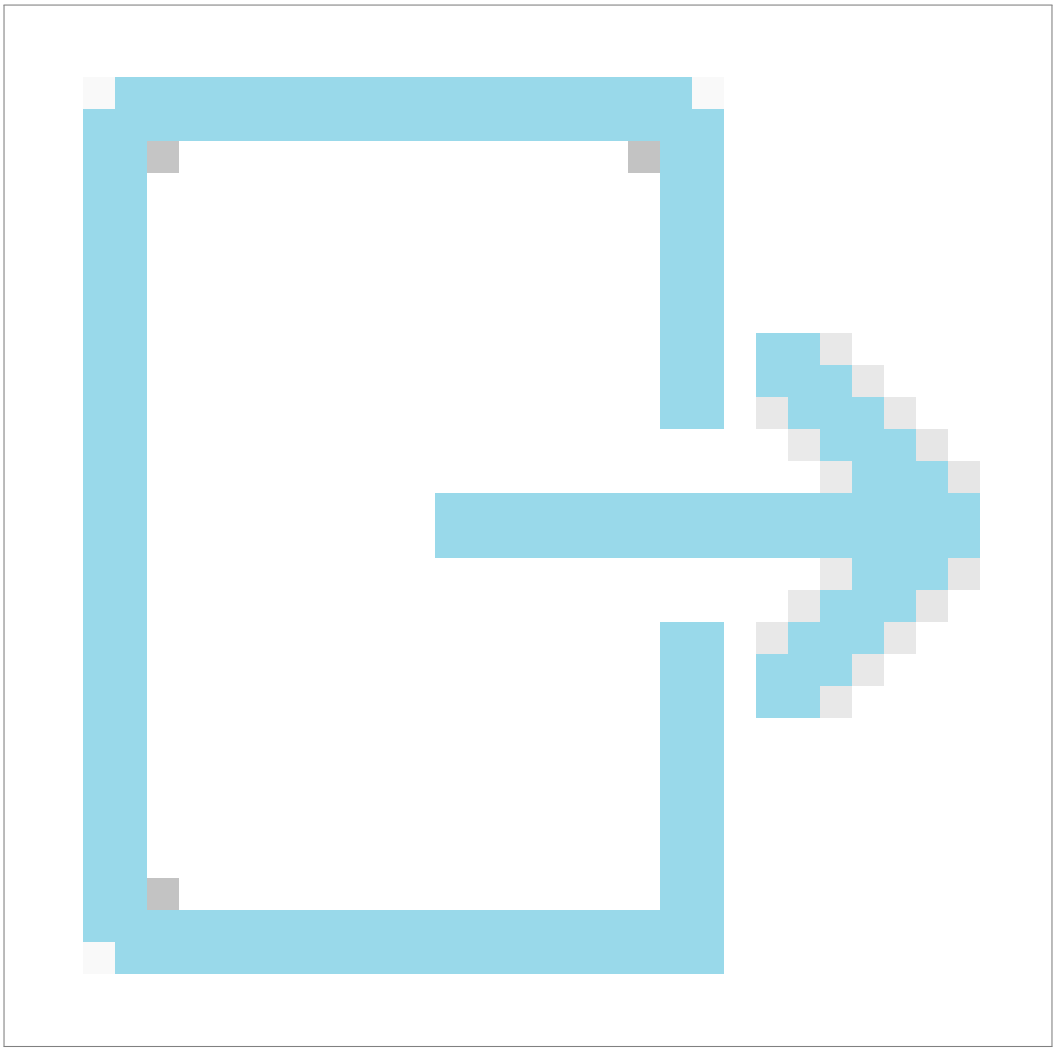
Relevante NCCS-Artikel

- Artikel 24 (1)
- Artikel 34



Input

- Identifizierte Unternehmen
- Zuordnungsmatrix
- Nationales Verifizierungssystem



Output

- Verifizierte Unternehmen

A

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: NCA

27.2 Absatz 2

Beschließt eine zuständige Behörde, ein nationales Überprüfungssystem einzurichten, so stellt sie sicher, dass die Überprüfung nach den folgenden Anforderungen durchgeführt wird:

a. Jede Partei, die die Peer Review, das Audit oder die Inspektion durchführt, muss von der zu überprüfenden Einrichtung mit kritischen Auswirkungen unabhängig sein und darf sich nicht in einem Interessenkonflikt befinden;

b. das Personal, das die Peer Reviews, Audits oder Inspektionen durchführt, muss nachweislich Kenntnisse haben über

   i. die Cybersicherheit im Elektrizitätssektor;
   ii. Cybersicherheitsmanagementsysteme;
   iii. Audit-Grundsätze;
   iv. die Bewertung von Cybersicherheitsrisiken;
   v. den gemeinsamen Rahmen für die Cybersicherheit im Elektrizitätssektor;
   vi. den nationalen Rechts- und Verwaltungsrahmen sowie europäische und internationale Normen, die für die Überprüfung relevant sind;
   vii. die Prozesse mit kritischen Auswirkungen, die Gegenstand der Überprüfung sind;

c. die Partei, die die Peer Reviews, Audits oder Inspektionen durchführt, erhält ausreichend Zeit für die Durchführung dieser Tätigkeiten;

d. die Partei, die die Peer Reviews, Audits oder Inspektionen durchführt, ergreift geeignete Maßnahmen, um die bei der Überprüfung erhobenen Informationen im Einklang mit ihrem Vertraulichkeitsgrad zu schützen, und

e. Peer Reviews, Audits oder Inspektionen werden mindestens einmal jährlich durchgeführt und umfassen mindestens alle drei Jahre den gesamten Prüfumfang.

GOOD TO KNOW

Rekurrenz

1 und 3 Jahre

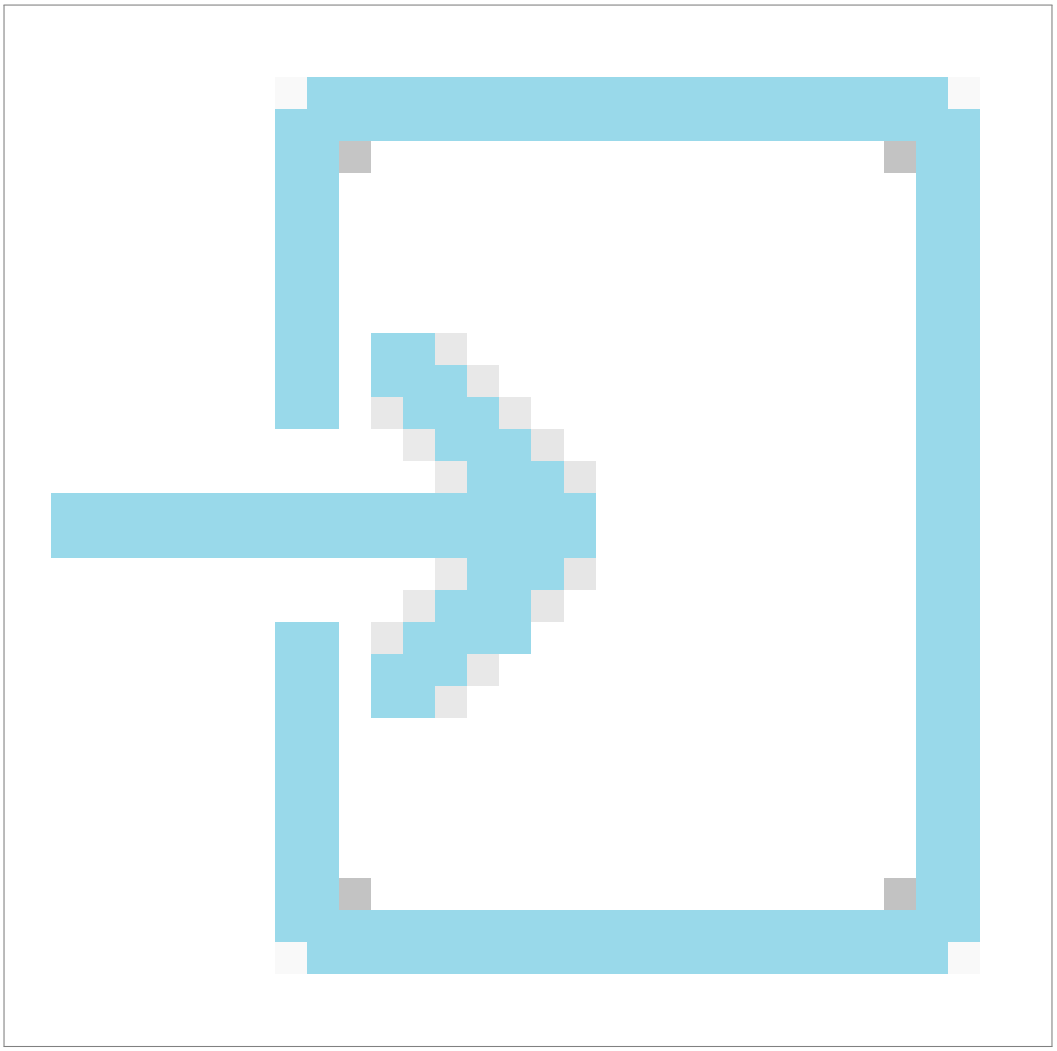
Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

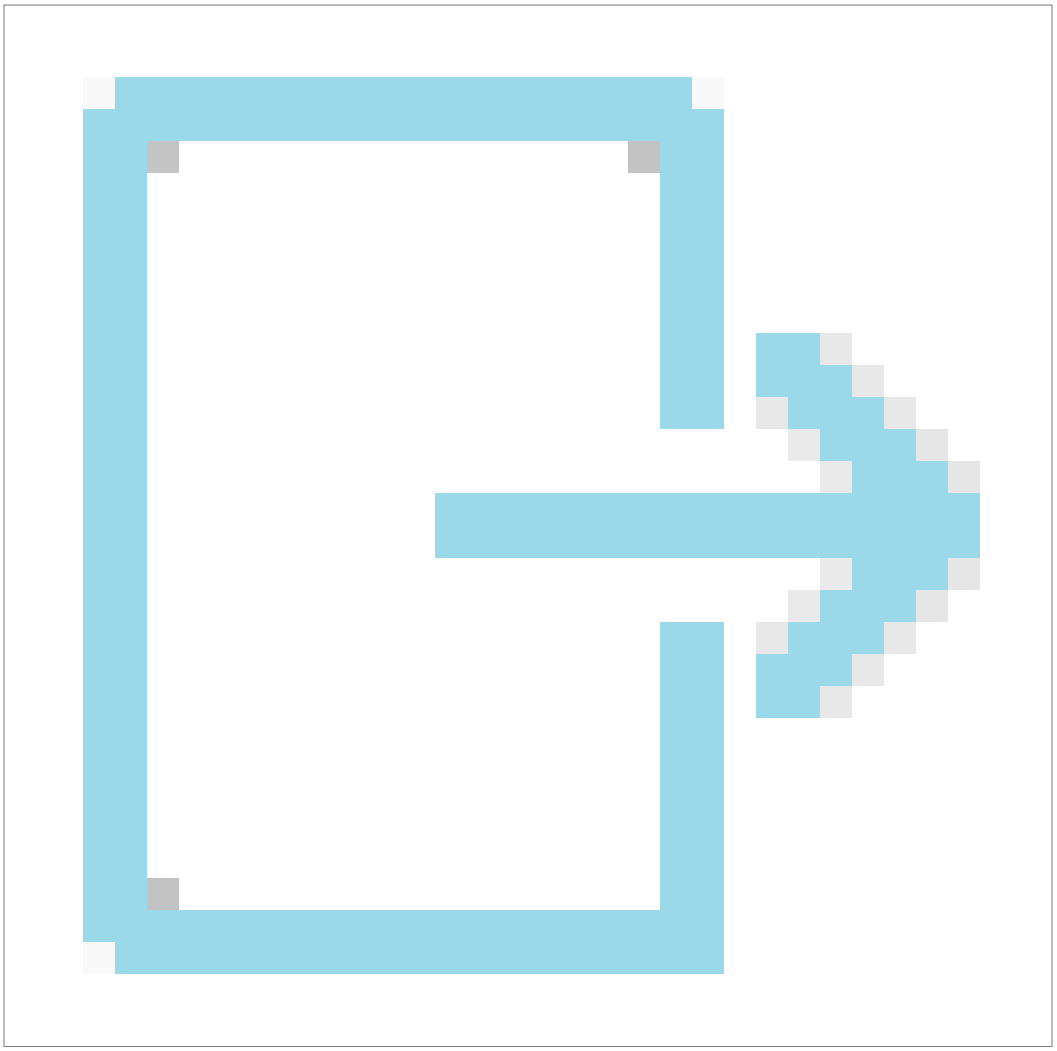
27.3 Absatz 3

Beschließt eine zuständige Behörde, ein nationales Überprüfungssystem einzurichten, so teilt sie der ACER jährlich mit, wie oft sie Inspektionen im Rahmen dieses Systems durchgeführt hat.



Input

- Nationales Verifizierungssystem



Output

- Bericht an ACER

GOOD TO KNOW

Rekurrenz

1 Jahr

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu informieren: ACER

Chapter 28

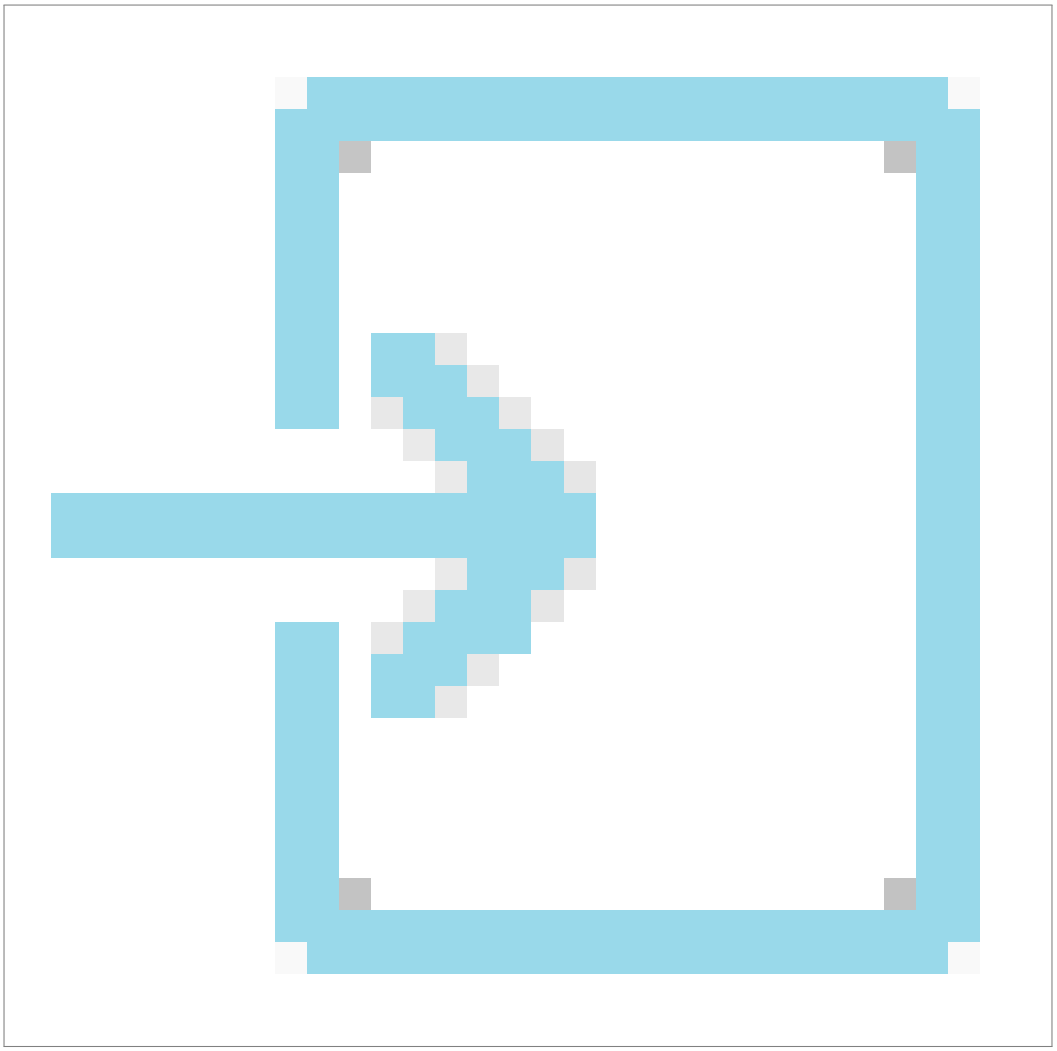
Artikel 26. : Cybersicherheitsrisikomanagement auf Ebene der Einrichtungen

28.1 Absatz 1

Jede von den zuständigen Behörden gemäß Artikel 24 Absatz 1 ermittelte Einrichtung mit erheblichen oder kritischen Auswirkungen führt das Cybersicherheitsrisikomanagement für alle ihre Vermögenswerte in ihren Perimetern mit erheblichen oder kritischen Auswirkungen durch. Jede Einrichtung mit erheblichen oder kritischen Auswirkungen führt alle drei Jahre ein Risikomanagement durch, das die in Absatz 2 genannten Phasen umfasst.

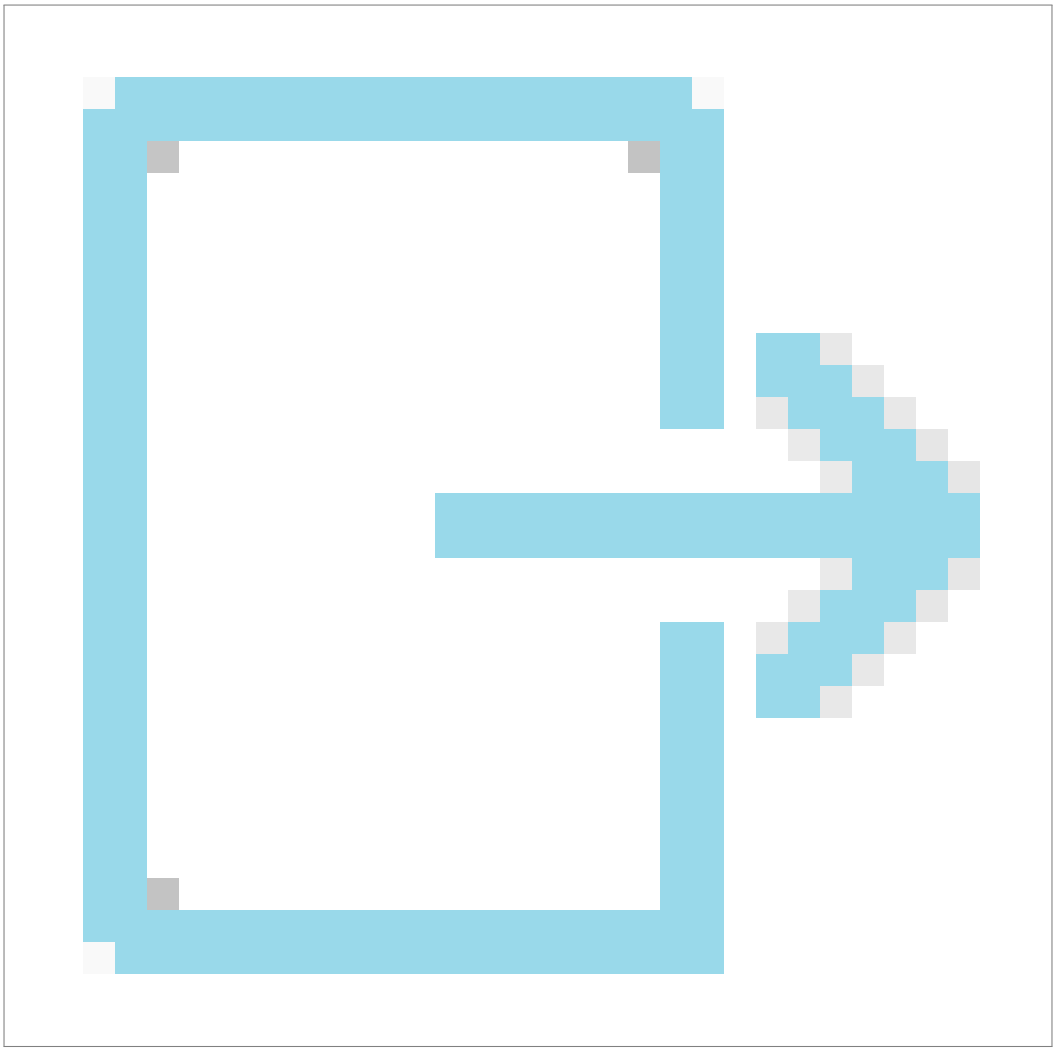
Relevante NCCS-Artikel

- Artikel 24 (1)
- Artikel 26 (2)



Input

- Unionsweite Prozesse mit erheblicher und kritischer Auswirkung
- Risikomatrix
- Umfassender grenzüberschreitender Bericht zur Bewertung der Cybersicherheitsrisiken im Stromsektor
- ECII
- Kriterien für die Risikoakzeptanz
- Cybersicherheitskontrollen
- Cybersicherheitsrahmenwerk



Output

- Risikobewertungsbericht auf Unternehmensebene
- Bestandsaufnahme der Vermögenswerte

GOOD TO KNOW

Rekurrenz

3 Jahre

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

28.2 Absatz 2

Jede Einrichtung mit erheblichen oder kritischen Auswirkungen stützt ihr Cybersicherheitsrisikomanagement auf einen Ansatz, der auf den Schutz ihrer Netz- und Informationssysteme abzielt und folgende Phasen umfasst:

a. Bestimmung des Kontexts;

b. Bewertung des Cybersicherheitsrisikos auf der Ebene der Einrichtung;

c. Behandlung von Cybersicherheitsrisiken;

d. Akzeptanz von Cybersicherheitsrisiken.

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

28.3 Absatz 3

Bei der Bestimmung des Kontexts trifft jede Einrichtung mit erheblichen oder kritischen Auswirkungen folgende Maßnahmen:

a. Festlegung des Umfangs der Bewertung des Cybersicherheitsrisikos, einschließlich der von ENTSO-E und der EU-VNBO ermittelten Prozesse mit erheblichen oder kritischen Auswirkungen sowie anderer Prozesse, die Ziel von Cyberangriffen mit erheblichen oder kritischen Auswirkungen auf grenzüberschreitende Stromflüsse sein können, und

b. Festlegung der Kriterien für die Risikobewertung und die Risikoakzeptanz im Einklang mit der Risiko-AuswirkungsMatrix, die Einrichtungen und die zuständigen Behörden nach den von ENTSO-E und der EU-VNBO gemäß Artikel 19 Absatz 2 entwickelten Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf Ebene der Mitgliedstaaten nutzen müssen, um Cybersicherheitsrisiken zu bewerten.

Relevante NCCS-Artikel

- Artikel 19 (2)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

28.4 Absatz 4

Bei der Bewertung des Cybersicherheitsrisikos muss jede Einrichtung mit erheblichen oder kritischen Auswirkungen

a. Cybersicherheitsrisiken unter Berücksichtigung folgender Aspekte ermitteln:

   i. aller Vermögenswerte, die unionsweite Prozesse mit erheblichen oder kritischen Auswirkungen unterstützen, wobei die möglichen Auswirkungen auf grenzüberschreitende Stromflüsse für den Fall einer Kompromittierung des Vermögenswerts zu bewerten sind;

   ii. möglicher Cyberbedrohungen unter Berücksichtigung der Cyberbedrohungen, die im jüngsten umfassenden Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23 ermittelt wurden, sowie Bedrohungen der Lieferkette;

   iii. Schwachstellen, einschließlich Schwachstellen in Altsystemen;

   iv. möglicher Szenarien von Cyberangriffen, einschließlich Cyberangriffen, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören;

   v. einschlägiger Risikobeurteilungen und -bewertungen auf Unionsebene, einschließlich koordinierter Risikobewertungen kritischer Lieferketten gemäß Artikel 22 der Richtlinie (EU) 2022/2555 [a], und

   vi. bestehender umgesetzter Kontrollen;

b. die Wahrscheinlichkeit und Folgen der unter Buchstabe a genannten Cybersicherheitsrisiken analysieren und das Ausmaß des Cybersicherheitsrisikos anhand der Risiko-Auswirkungs-Matrix bestimmen, die in den von den ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO gemäß Artikel 19 Absatz 2 entwickelten Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf Ebene der Mitgliedstaaten genutzt wird, um Cybersicherheitsrisiken zu bewerten;

c. Vermögenswerte nach den möglichen Folgen einer Beeinträchtigung der Cybersicherheit klassifizieren und Perimeter mit erheblichen oder kritischen Auswirkungen wie folgt ermitteln:

   i. Durchführung einer Folgenabschätzung für Geschäftsprozesse anhand des ECII für alle Prozesse, die Gegenstand der Bewertung des Cybersicherheitsrisikos sind;

   ii. Einstufung eines Prozesses als Prozess mit erheblichen oder kritischen Auswirkungen, wenn sein ECII über dem Schwellenwert für erhebliche bzw. kritische Auswirkungen liegt;

   iii. Bestimmung aller Vermögenswerte mit erheblichen oder kritischen Auswirkungen als die Vermögenswerte, die für Prozesse mit erheblichen bzw. kritischen Auswirkungen erforderlich sind;

   iv. Bestimmung der Perimeter mit erheblichen oder kritischen Auswirkungen als Perimeter, die alle Vermögenswerte mit erheblichen bzw. kritischen Auswirkungen umfassen, damit der Zugang zu diesen Perimetern kontrolliert werden kann;

d. Cybersicherheitsrisiken durch Priorisierung anhand von Risikobewertungs- und Risikoakzeptanzkriterien gemäß Absatz 3 Buchstabe b beurteilen.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_22

Relevante NCCS-Artikel

- Artikel 23
- Artikel 19 (2)
- Artikel 26 (3)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

28.5 Absatz 5

Bei der Behandlung des Cybersicherheitsrisikos erstellt jede Einrichtung mit erheblichen oder kritischen Auswirkungen einen Risikominderungsplan auf Ebene der Einrichtung, wobei sie geeignete Optionen für die Behandlung des Risikos wählt, um die Risiken zu bewältigen und das Restrisiko zu bestimmen.

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

28.6 Absatz 6

Bei der Akzeptanz von Cybersicherheitsrisiken entscheidet jede Einrichtung mit erheblichen oder kritischen Auswirkungen auf der Grundlage der in Absatz 3 Buchstabe b festgelegten Risikoakzeptanzkriterien, ob sie das Restrisiko akzeptiert.

Relevante NCCS-Artikel

- Artikel 26 (3)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

28.7 Absatz 7

Jede Einrichtung mit erheblichen oder kritischen Auswirkungen erfasst die in Absatz 1 genannten Vermögenswerte in einem Vermögensinventar. Dieses Vermögensinventar ist nicht Teil des Berichts über die Risikobewertung.

Relevante NCCS-Artikel

- Artikel 26 (1)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

28.8 Absatz 8

Die zuständige Behörde kann die im Vermögensinventar enthaltenen Vermögenswerte während der Inspektionen einsehen.

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA

Chapter 29

Artikel 27. : Berichterstattung über die Risikobewertung auf Ebene der Einrichtung

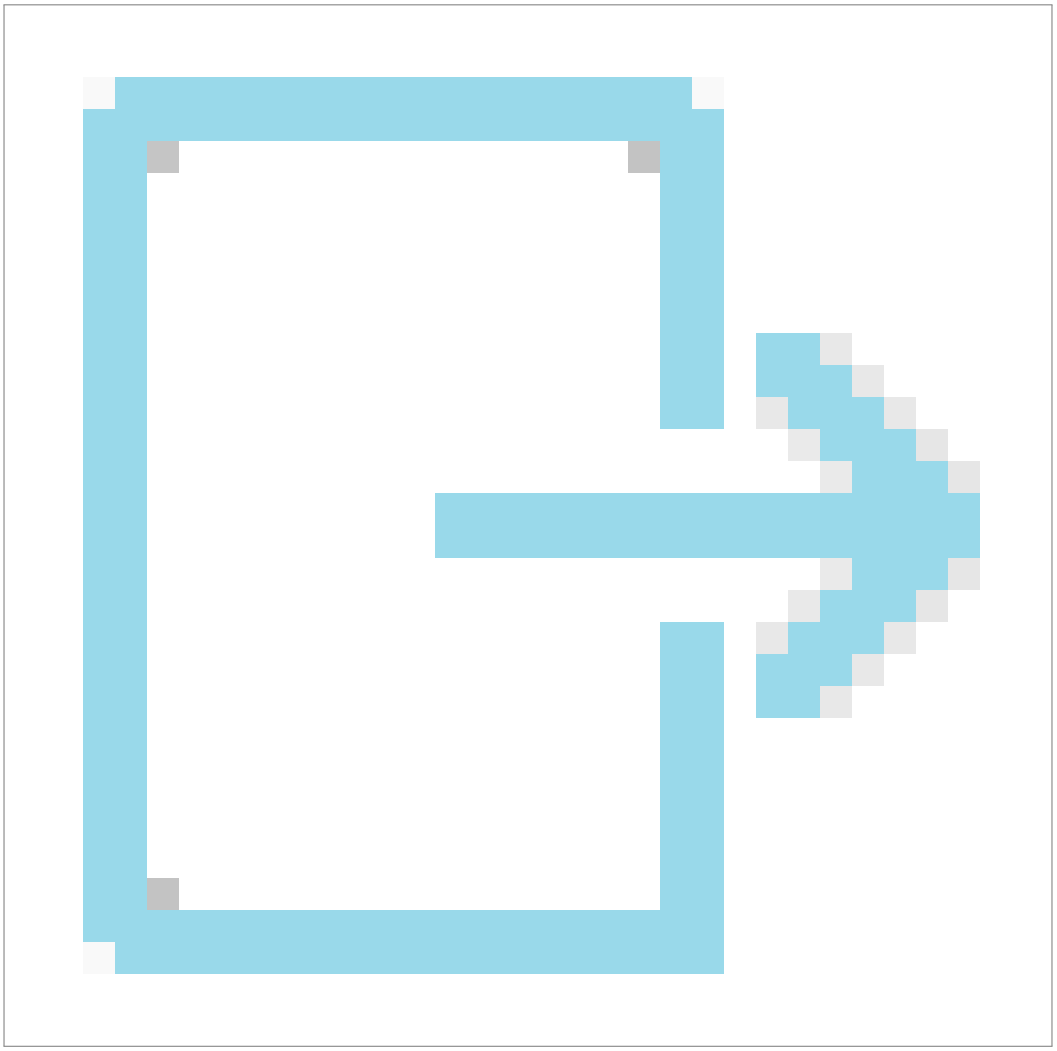
29.1 Absatz 1

Innerhalb von 12 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre legt jede Einrichtung mit erheblichen oder kritischen Auswirkungen der zuständigen Behörde einen Bericht vor, der folgende Informationen enthält:

1. eine Liste der für den Risikominderungsplan auf Ebene der Einrichtung gemäß Artikel 26 Absatz 5 ausgewählten Kontrollen mit dem aktuellen Stand der Umsetzung jeder Kontrolle;
2. für jeden unionsweiten Prozess mit erheblichen oder kritischen Auswirkungen eine Schätzung des Risikos einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten. Die Schätzung dieses Risikos ist im Einklang mit der Risiko-Auswirkungs-Matrix gemäß Artikel 19 Absatz 2 zu bestimmen;
3. für ihre Prozesse mit kritischen Auswirkungen eine Liste der Anbieter kritischer IKT-Dienste.

Relevante NCCS-Artikel

- Artikel 24 (6)
- Artikel 26 (5)
- Artikel 19 (2)



Output

- Risikobewertung auf Unternehmensebene

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

Spätestens im Juni 2030

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Zu informieren: NCA

Chapter 30

Artikel 28. : Zusammensetzung, Funktionsweise und Überprüfung des gemeinsamen Rahmens für die Cybersicherheit im Elektrizitätssektor

30.1 Absatz 1

Der gemeinsame Rahmen für die Cybersicherheit im Elektrizitätssektor umfasst die folgenden Kontrollen und Systeme für das Cybersicherheitsmanagement:

a. die gemäß Artikel 29 entwickelten Mindest-Cybersicherheitskontrollen;

b. die gemäß Artikel 29 entwickelten erweiterten Cybersicherheitskontrollen;

c. die gemäß Artikel 34 entwickelte Vergleichsmatrix, in der die Kontrollen gemäß den Buchstaben a und b anhand ausgewählter europäischer und internationaler Normen und nationaler Rechts- oder Verwaltungsrahmen verglichen werden;

d. das gemäß Artikel 32 eingerichtete Cybersicherheitsmanagementsystem.

Relevante NCCS-Artikel

- Artikel 29
- Artikel 34
- Artikel 32

Verantwortlich für die Aktivität: HIE, NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, NCA

30.2 Absatz 1

Der gemeinsame Rahmen für die Cybersicherheit im Elektrizitätssektor umfasst die folgenden Kontrollen und Systeme für das Cybersicherheitsmanagement:

a. die gemäß Artikel 29 entwickelten Mindest-Cybersicherheitskontrollen;

b. die gemäß Artikel 29 entwickelten erweiterten Cybersicherheitskontrollen;

c. die gemäß Artikel 34 entwickelte Vergleichsmatrix, in der die Kontrollen gemäß den Buchstaben a und b anhand ausgewählter europäischer und internationaler Normen und nationaler Rechts- oder Verwaltungsrahmen verglichen werden;

d. das gemäß Artikel 32 eingerichtete Cybersicherheitsmanagementsystem.

Relevante NCCS-Artikel

- Artikel 29
- Artikel 34
- Artikel 32

Verantwortlich für die Aktivität: CIE, TSO, NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, TSO, NCA

30.3 Absatz 2

Alle Einrichtungen mit erheblichen Auswirkungen wenden die Mindest-Cybersicherheitskontrollen gemäß Absatz 1 Buchstabe a innerhalb ihres Perimeters mit erheblichen Auswirkungen an.

Relevante NCCS-Artikel

- Artikel 28 (1)

Verantwortlich für die Aktivität: HIE

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE

30.4 Absatz 3

Alle Einrichtungen mit kritischen Auswirkungen wenden die erweiterten Cybersicherheitskontrollen gemäß Absatz 1 Buchstabe b innerhalb ihres Perimeters mit kritischen Auswirkungen an.

Relevante NCCS-Artikel

- Artikel 28 (1)

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

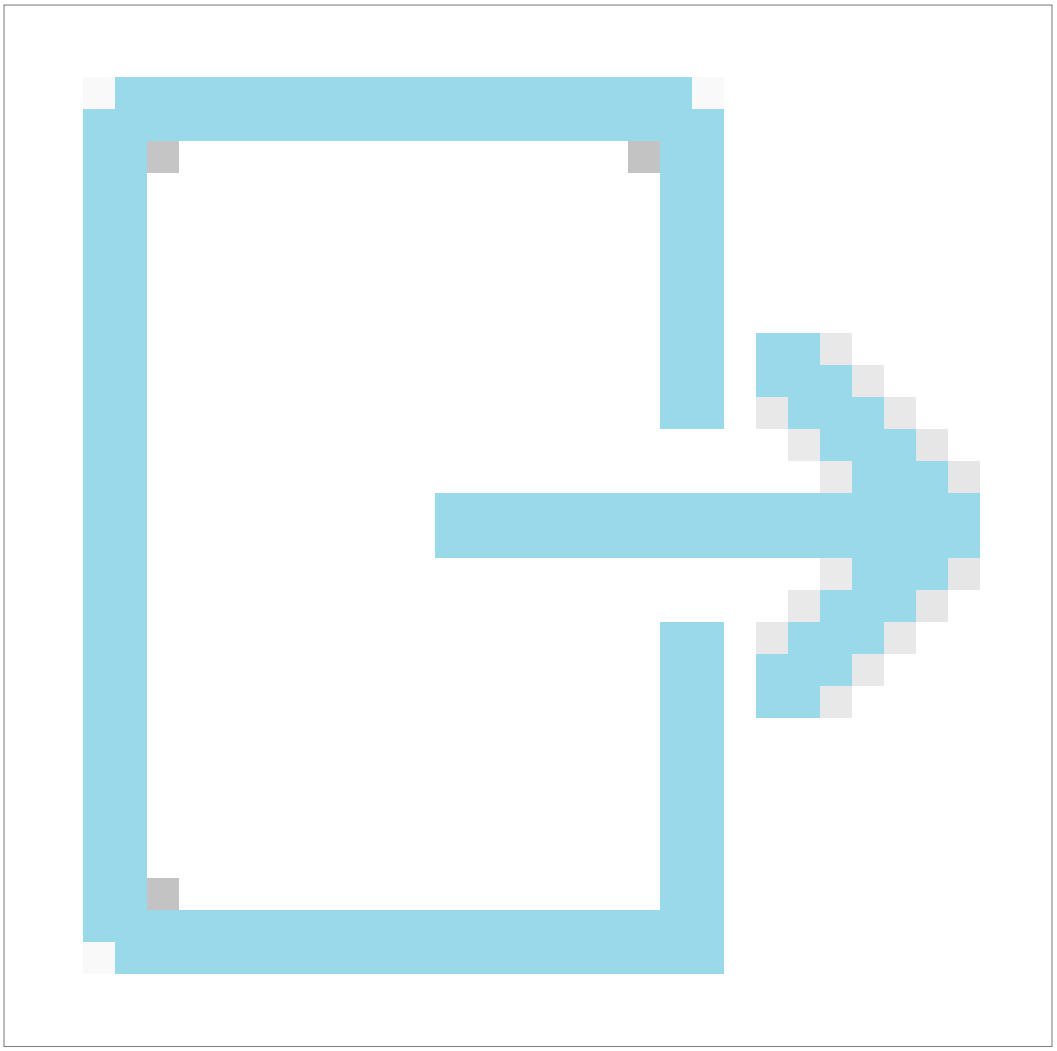
Beteiligt an der Aufgabenausführung: CIE, TSO

30.5 Absatz 4

Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 wird der in Absatz 1 genannte gemeinsame Rahmen für die Cybersicherheit im Elektrizitätssektor durch die gemäß Artikel 33 entwickelten Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen in der Lieferkette ergänzt.

Relevante NCCS-Artikel

- Artikel 19 (4)
- Artikel 28 (1)
- Artikel 33



Output

- Unionsweite Risikobewertung mit Kontrollen der Lieferkette

GOOD TO KNOW

Zeitpunkt

Spätestens im Oktober 2026

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Chapter 31

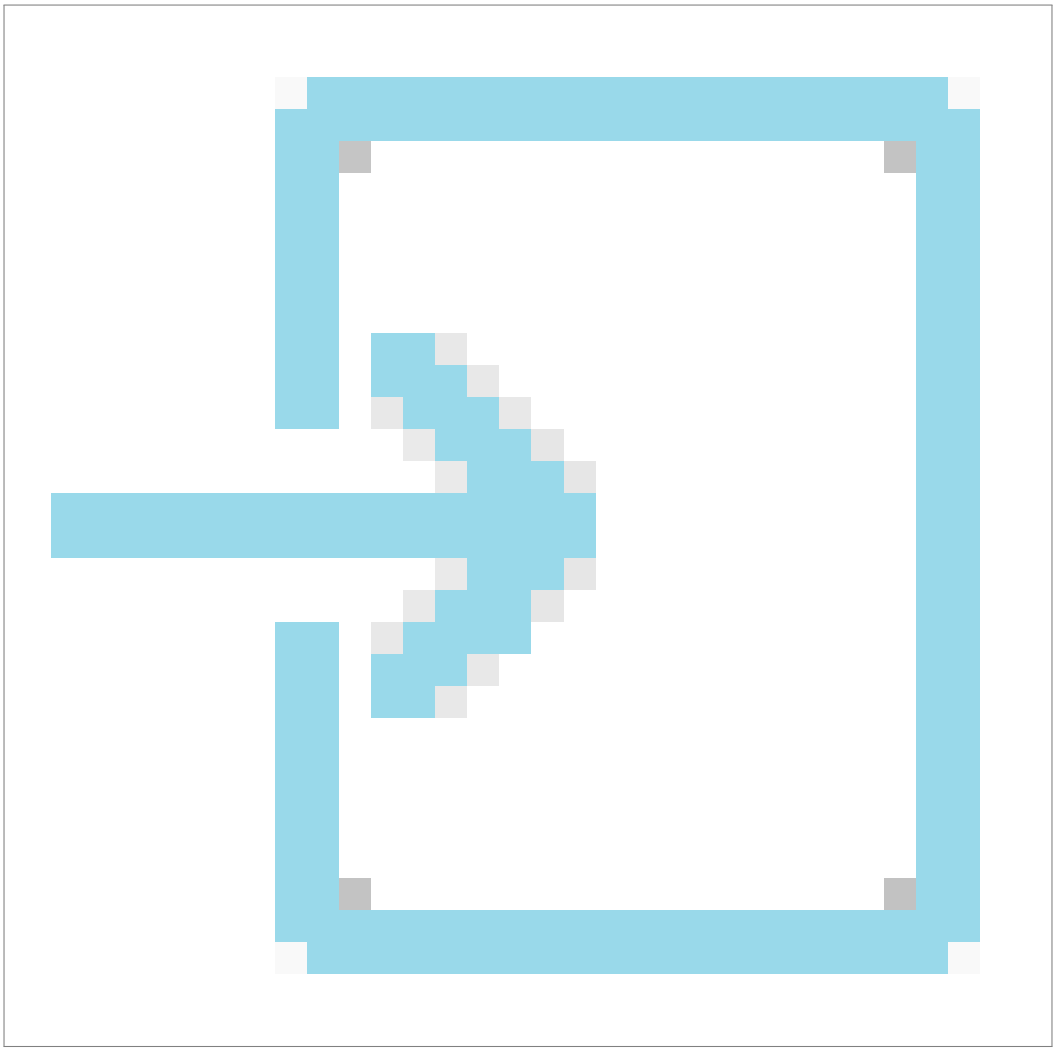
Artikel 29. : Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen

31.1 Absatz 1

Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO einen Vorschlag für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen.

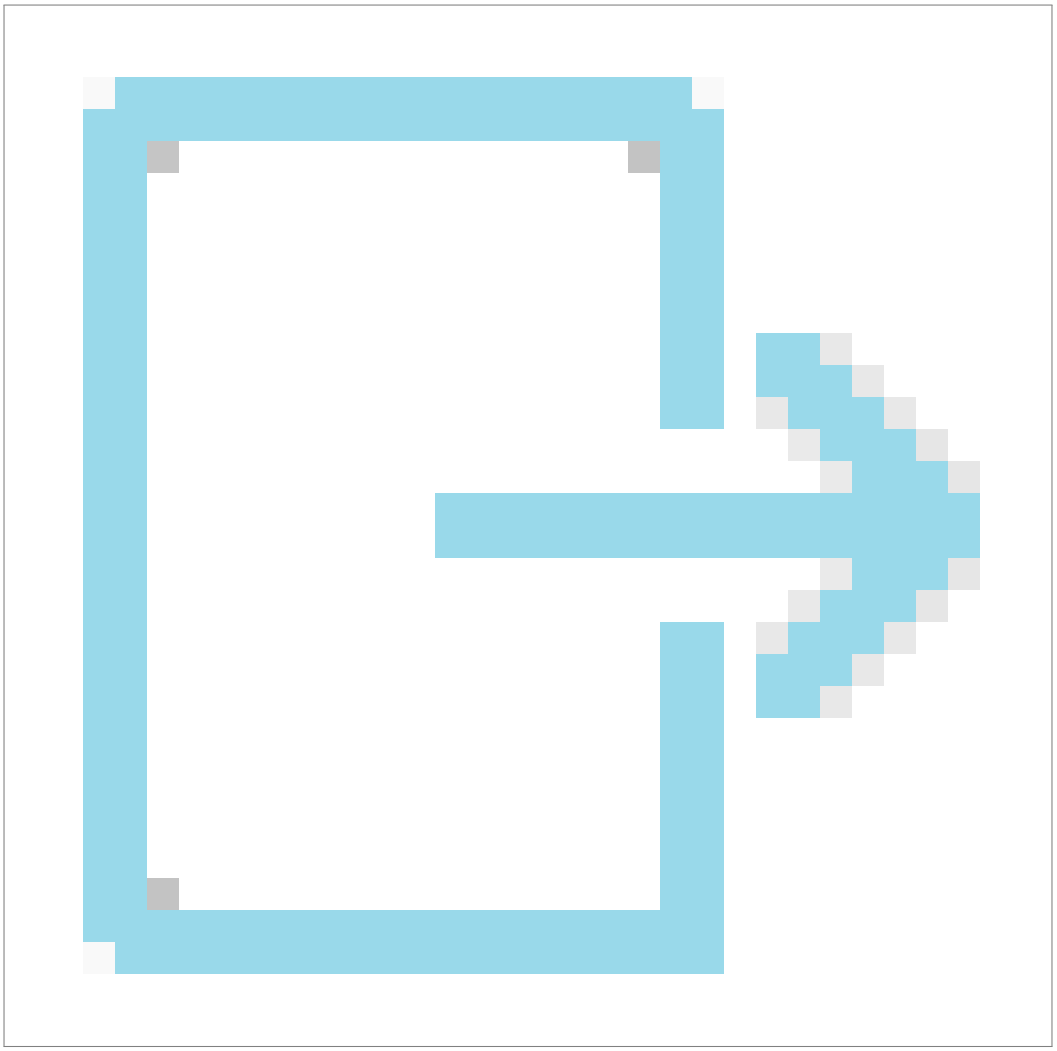
Relevante NCCS-Artikel

- Artikel 19 (4)



Input

- Unionsweite Risikobewertung
- Kontrollen zur Informationssicherheit



Output

- Mindest- und erweiterte Kontrollen (Entwurf)

GOOD TO KNOW

Zeitpunkt

Spätestens im Oktober 2026

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

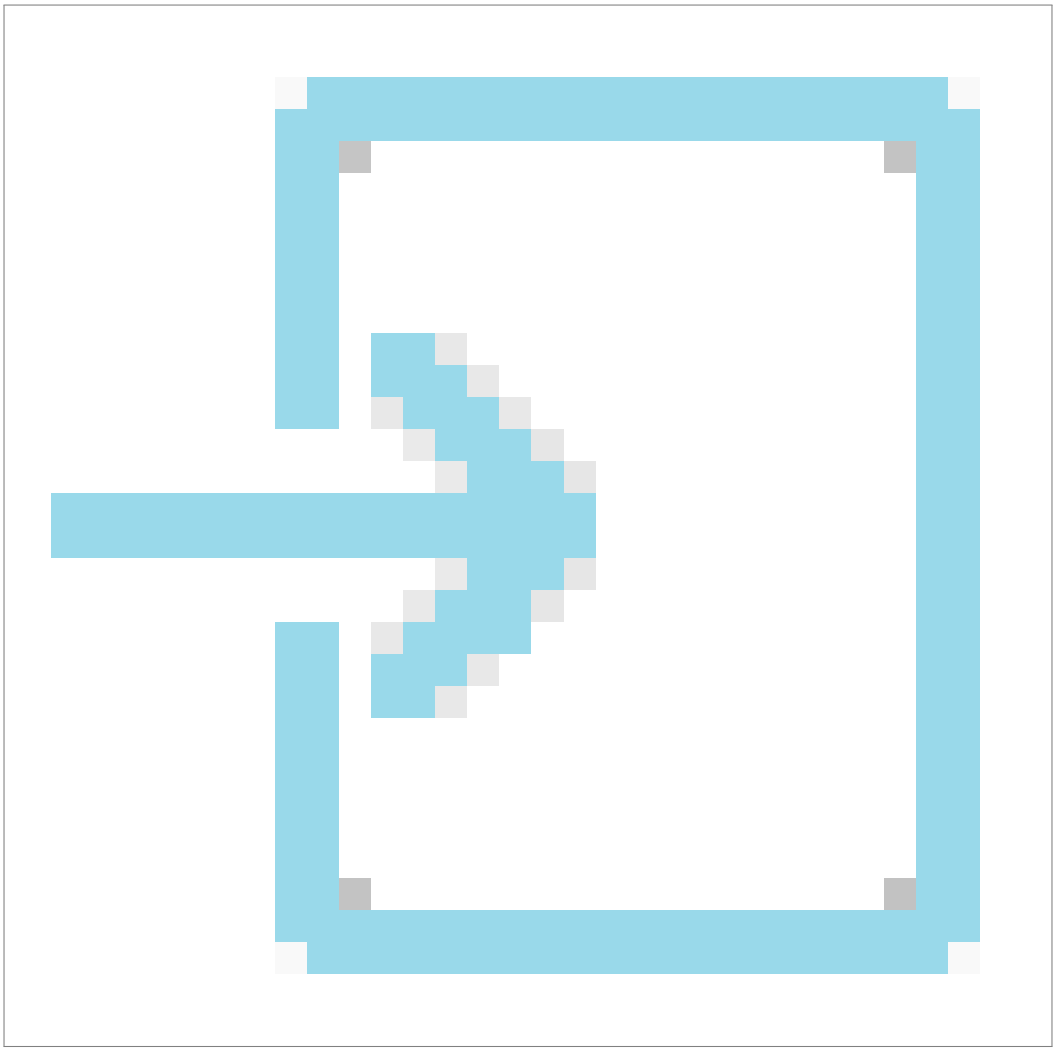
Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

31.2 Absatz 2

Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO der zuständigen Behörde eine Änderung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

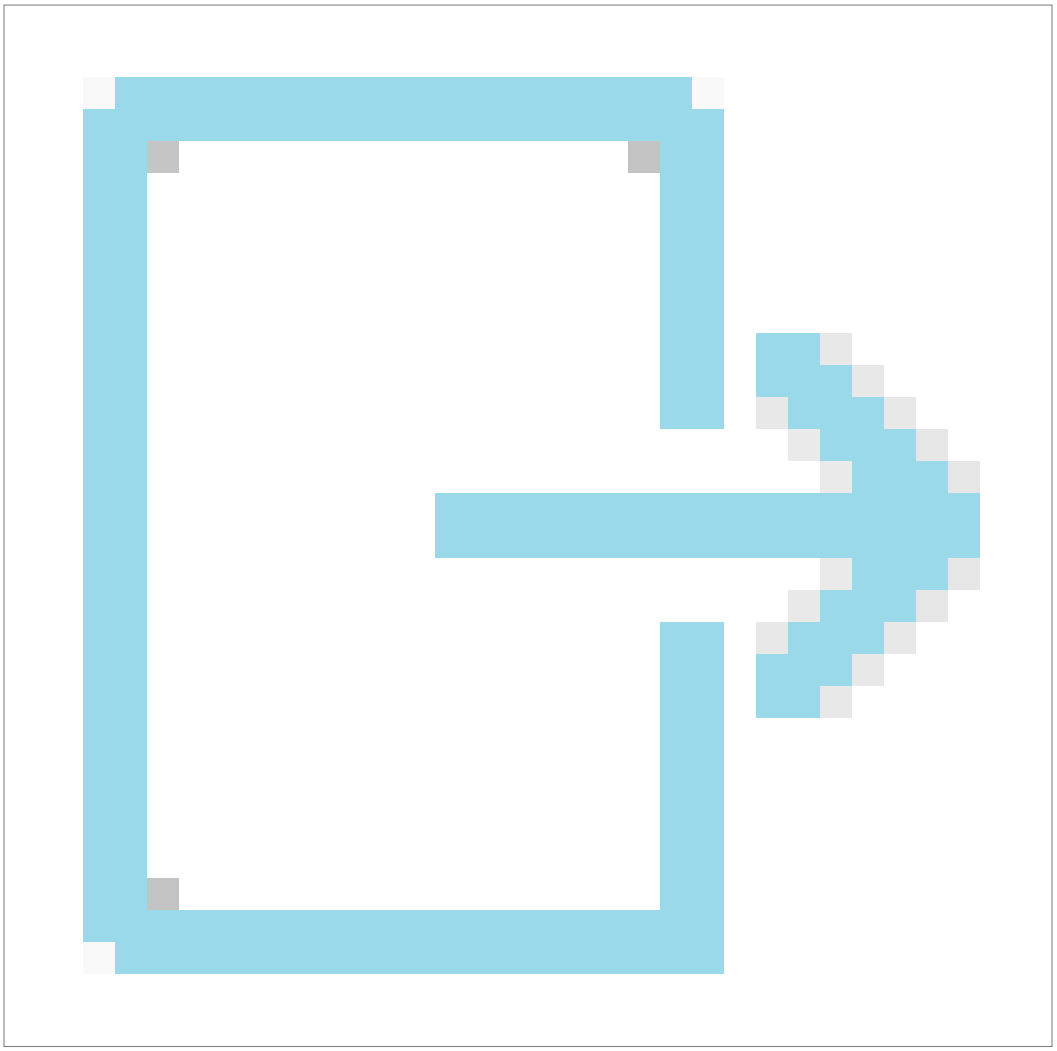
Relevante NCCS-Artikel

- Artikel 21 (2)
- Artikel 8 (10)



Input

- Risikobewertung auf regionaler Ebene



Output

- Mindest- und erweiterte Kontrollen

GOOD TO KNOW

Zeitpunkt

Spätestens im Juni 2031

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu informieren: NCA

31.3 Absatz 3

Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen müssen überprüft werden können; dazu werden sie entweder im Einklang mit dem Verfahren gemäß Artikel 31 in ein nationales Überprüfungssystem einbezogen oder Sicherheitsaudits durch unabhängige Dritte gemäß den in Artikel 25 Absatz 2 aufgeführten Anforderungen unterzogen.

Relevante NCCS-Artikel

- Artikel 31
- Artikel 25 (2)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

31.4 Absatz 4

Die gemäß Absatz 1 entwickelten anfänglichen Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen müssen auf den Risiken beruhen, die in dem Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 5 ermittelt wurden. Die gemäß Absatz 2 entwickelten geänderten MindestCybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen müssen auf dem in Artikel 21 Absatz 2 genannten Bericht über die regionale Bewertung des Cybersicherheitsrisikos beruhen.

Relevante NCCS-Artikel

- Artikel 29 (1)
- Artikel 19 (5)
- Artikel 29 (2)
- Artikel 21 (2)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

31.5 Absatz 5

Die Mindest-Cybersicherheitskontrollen müssen im Einklang mit Artikel 46 Kontrollen zum Schutz der ausgetauschten Informationen umfassen.

Relevante NCCS-Artikel

- Artikel 46

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

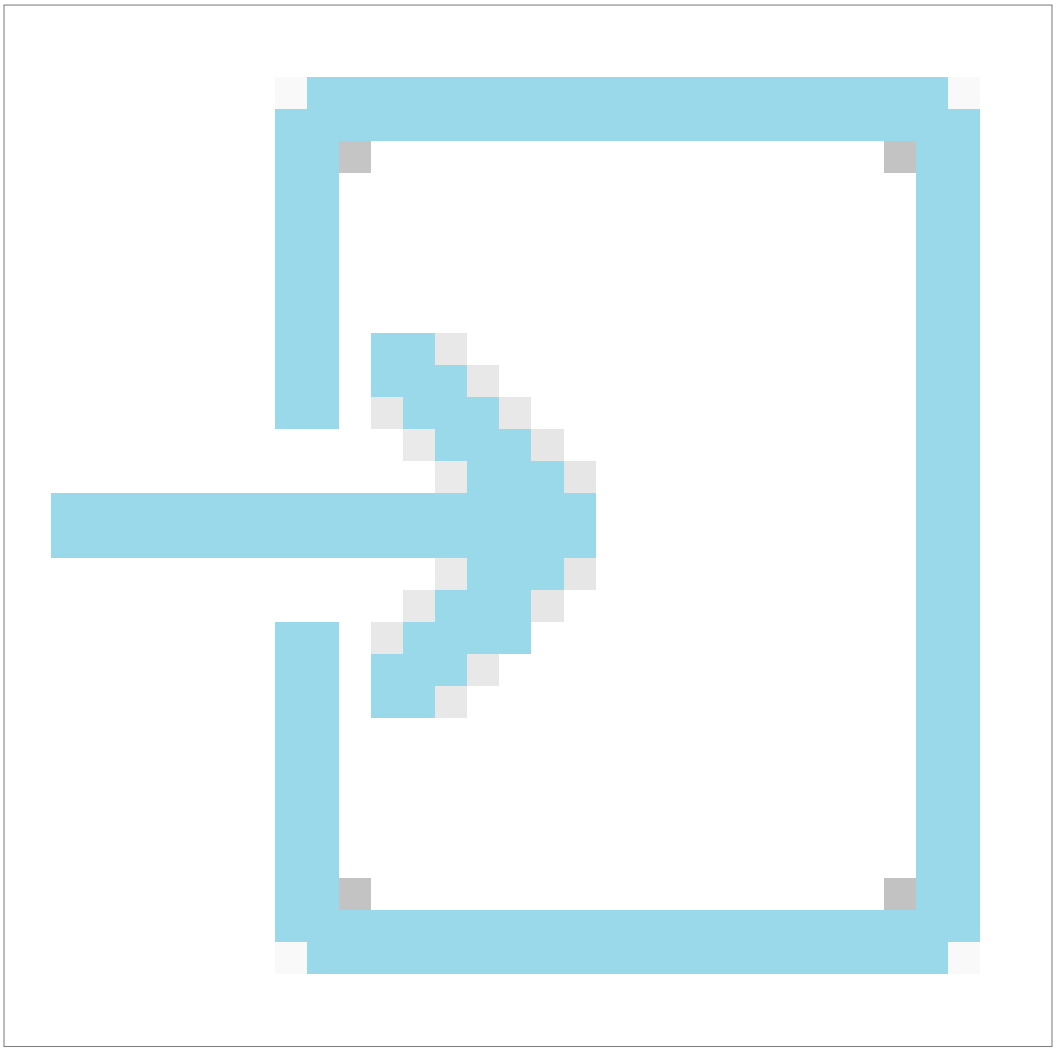
Zu informieren: NCA

31.6 Absatz 6

Innerhalb von 12 Monaten nach der Genehmigung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 8 Absatz 5 und nach jeder Aktualisierung gemäß Artikel 8 Absatz 10 wenden die in Artikel 2 Absatz 1 genannten Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden, bei der Festlegung des Risikominderungsplans auf Ebene der Einrichtung gemäß Artikel 26 Absatz 5 innerhalb der Perimeter mit erheblichen Auswirkungen die Mindest-Cybersicherheitskontrollen und innerhalb der Perimeter mit kritischen Auswirkungen die erweiterten Cybersicherheitskontrollen an.

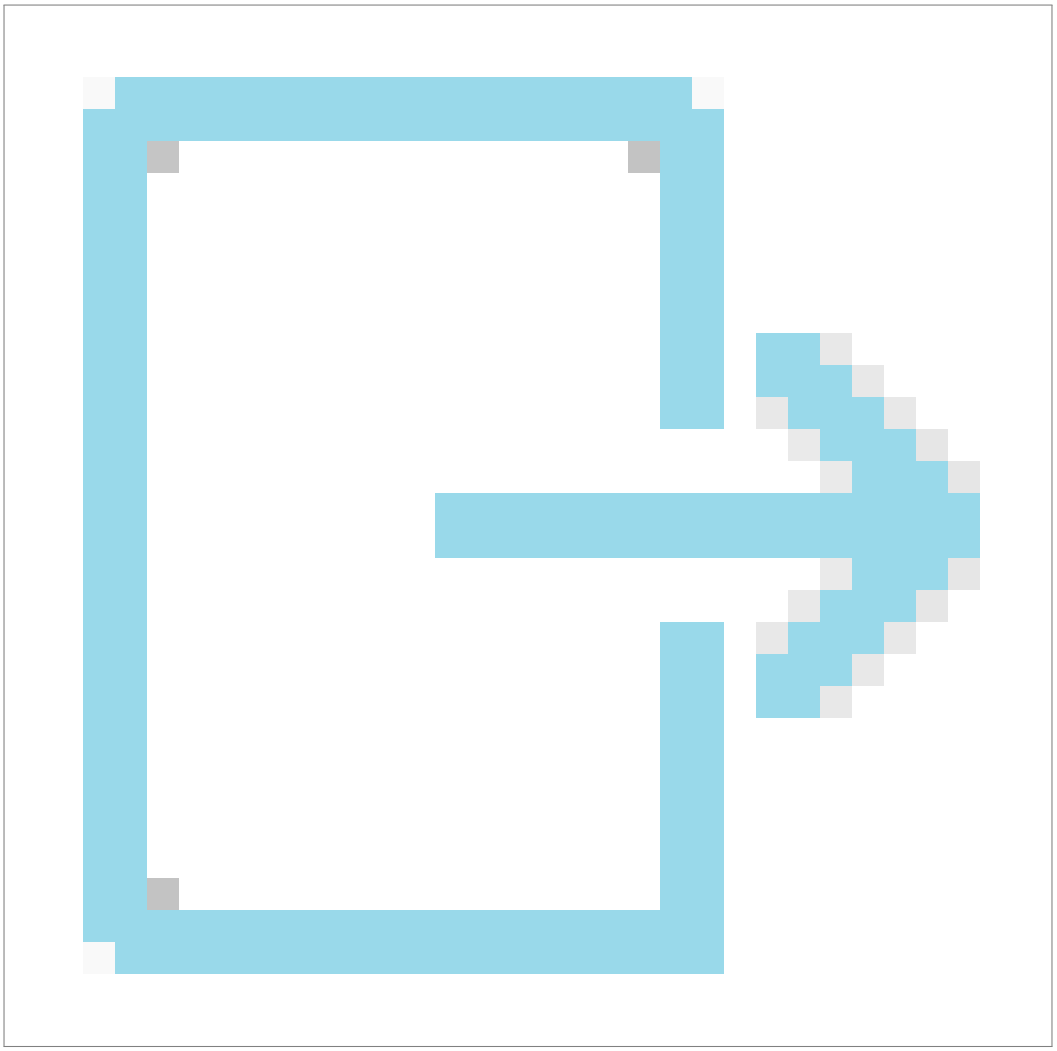
Relevante NCCS-Artikel

- Artikel 8 (5)
- Artikel 8 (10)
- Artikel 2 (1)
- Artikel 24
- Artikel 26 (5)



Input

- Minimale Kontrollen



Output

- Mindest- und erweiterte Kontrollen

GOOD TO KNOW

Zeitpunkt

12 Monate

Verantwortlich für die Aktivität: HIE

Beteiligte Stakeholder:

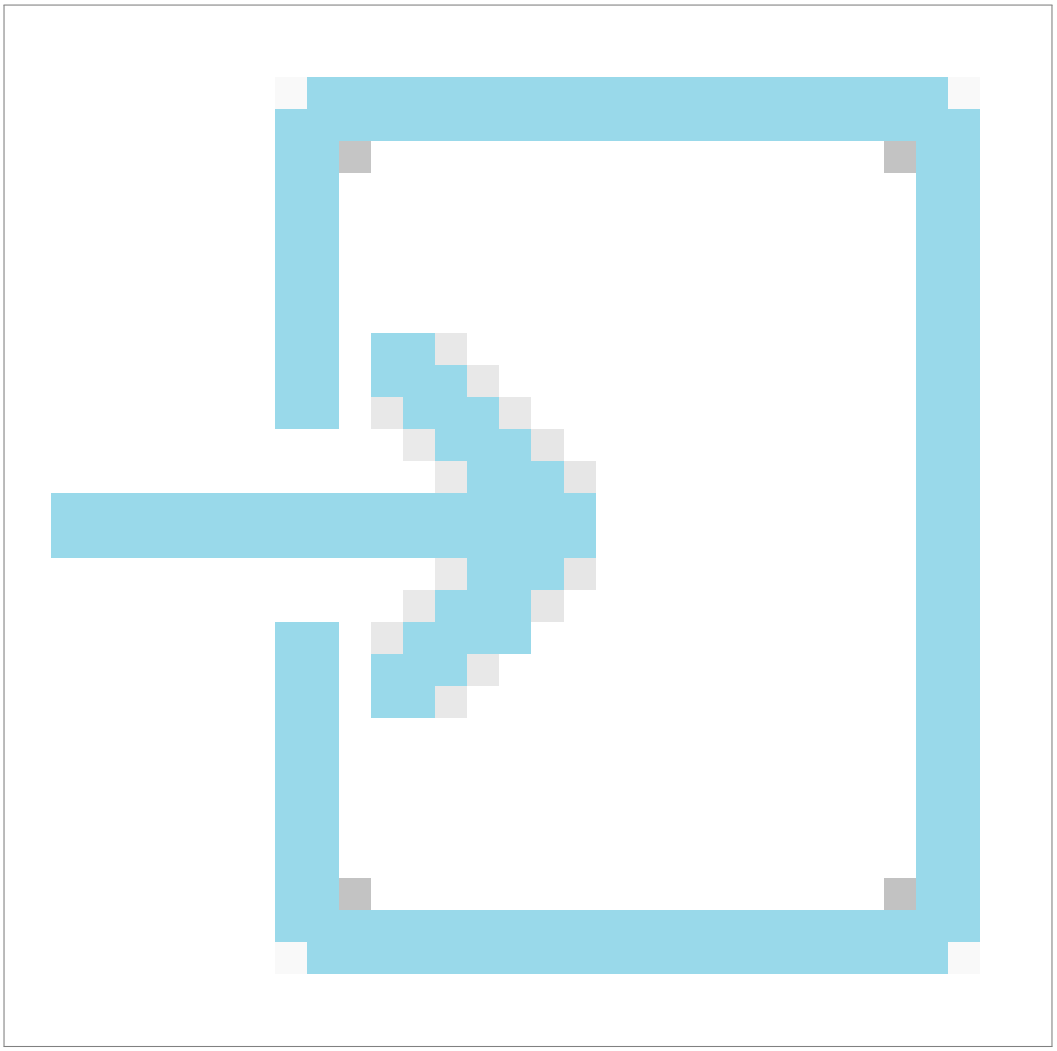
Beteiligt an der Aufgabenausführung: HIE

31.7 Absatz 6

Innerhalb von 12 Monaten nach der Genehmigung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 8 Absatz 5 und nach jeder Aktualisierung gemäß Artikel 8 Absatz 10 wenden die in Artikel 2 Absatz 1 genannten Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden, bei der Festlegung des Risikominderungsplans auf Ebene der Einrichtung gemäß Artikel 26 Absatz 5 innerhalb der Perimeter mit erheblichen Auswirkungen die Mindest-Cybersicherheitskontrollen und innerhalb der Perimeter mit kritischen Auswirkungen die erweiterten Cybersicherheitskontrollen an.

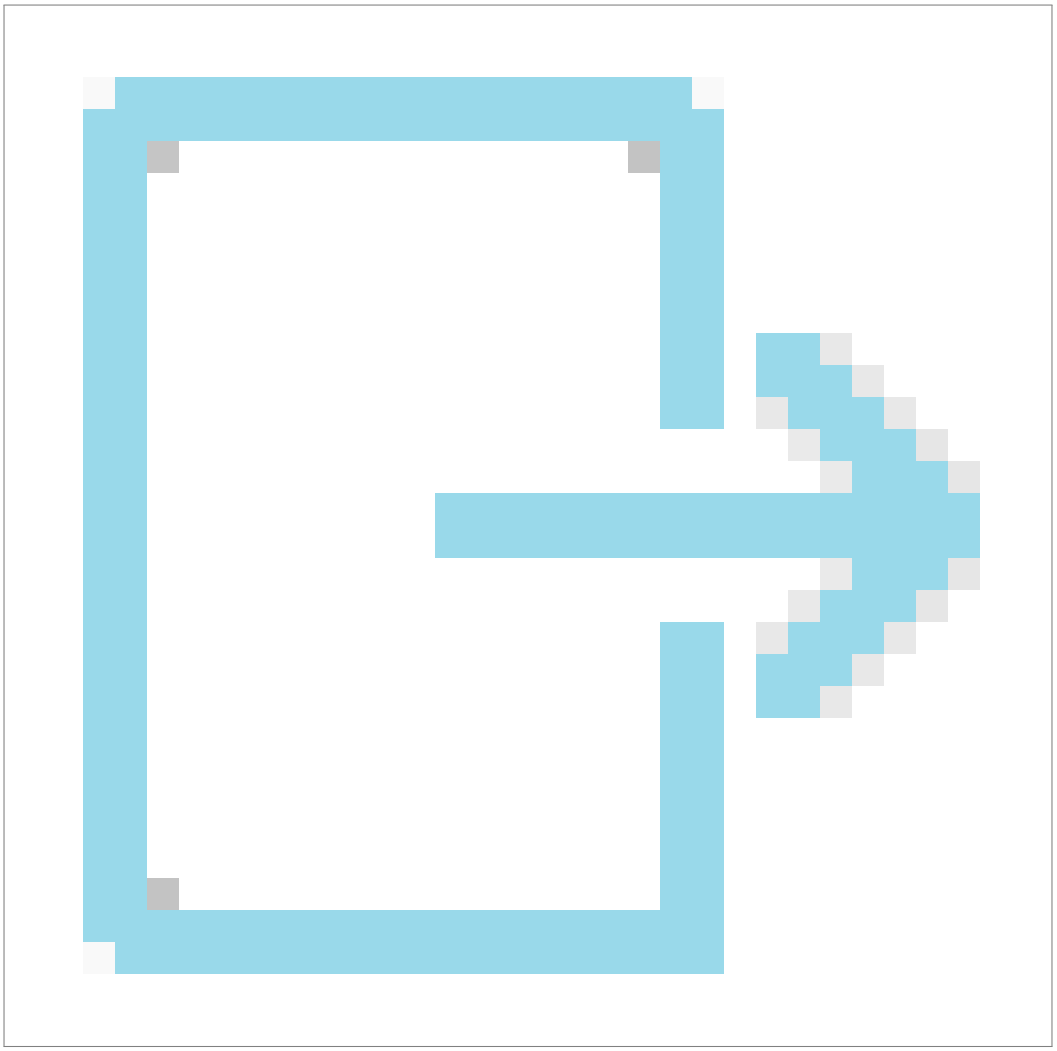
Relevante NCCS-Artikel

- Artikel 8 (5)
- Artikel 8 (10)
- Artikel 2 (1)
- Artikel 24
- Artikel 26 (5)



Input

- Mindest- und erweiterte Kontrollen



Output

- Erweiterte Kontrollen

GOOD TO KNOW

Zeitpunkt

12 Monate

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, TSO

Chapter 32

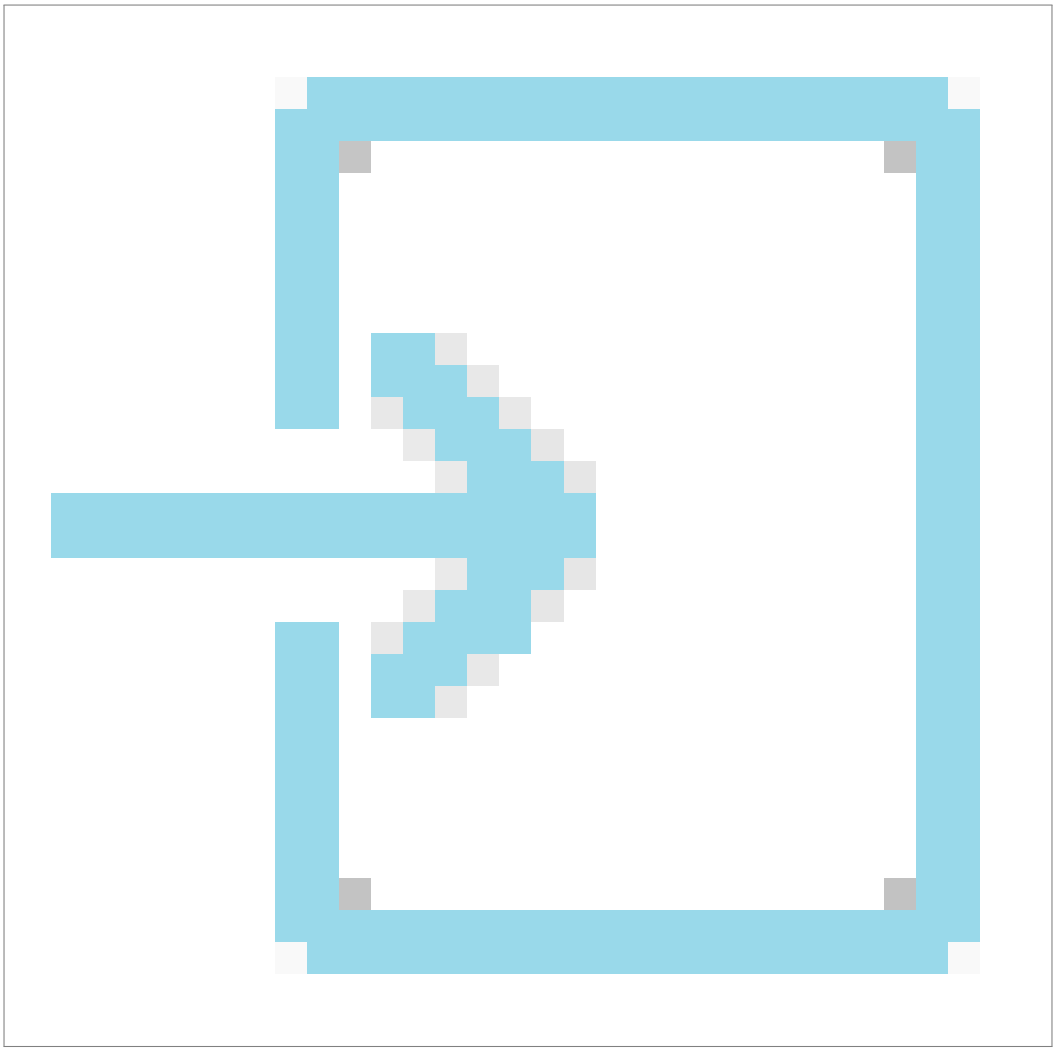
Artikel 30. : Ausnahmen von den Mindest-Cybersicherheitskontrollen und den erweiterten Cybersicherheitskontrollen

32.1 Absatz 1

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen können bei der jeweils zuständigen Behörde eine Ausnahme von ihrer Verpflichtung zur Anwendung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 29 Absatz 6 beantragen.

Relevante NCCS-Artikel

- Artikel 2 (1)
- Artikel 29 (6)



Input

- Ausnahme von den Kontrollen

A

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

32.2 Absatz 1

Die zuständige Behörde kann eine solche Ausnahme aus folgenden Gründen gewähren:

a. unter außergewöhnlichen Umständen, wenn die Einrichtung nachweisen kann, dass die Kosten für die Durchführung geeigneter Cybersicherheitskontrollen den Nutzen erheblich übersteigen. Die ACER und ENTSO-E können in Zusammenarbeit mit der EU-VNBO zur Unterstützung der Einrichtungen gemeinsam Leitlinien für die Schätzung der Kosten von Cybersicherheitskontrollen ausarbeiten;

b. bei Vorlage eines Risikobehandlungsplans auf Ebene der Einrichtung, mit dem die Cybersicherheitsrisiken durch alternative Kontrollen auf ein Niveau verringert werden, das nach den in Artikel 26 Absatz 3 Buchstabe b genannten Risikoakzeptanzkriterien akzeptiert werden kann.

Relevante NCCS-Artikel

- Artikel 26 (3)

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

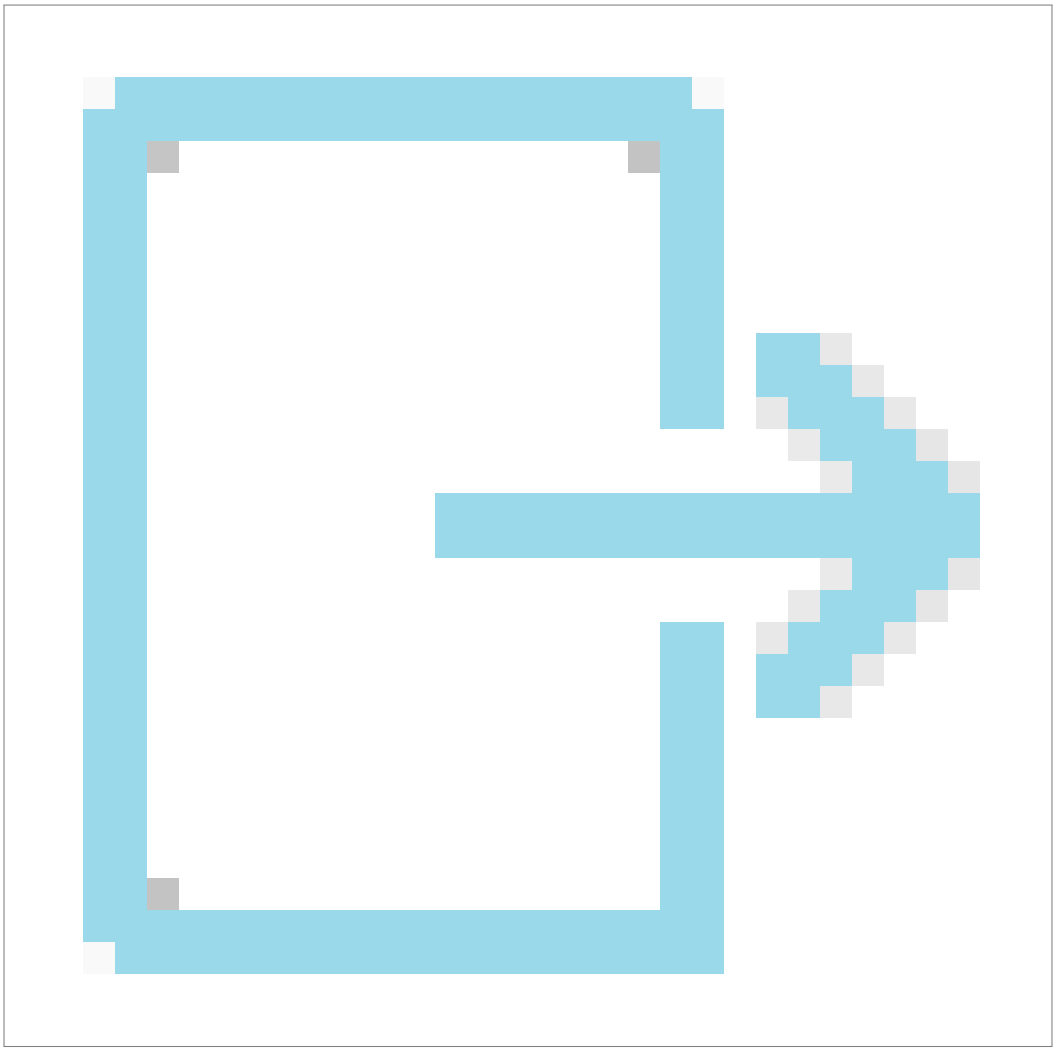
Beteiligt an der Aufgabenausführung: NCA

32.3 Absatz 2

Innerhalb von drei Monaten nach Eingang des in Absatz 1 genannten Antrags entscheidet jede zuständige Behörde, ob eine Ausnahme von den Mindest-Cybersicherheitskontrollen und den erweiterten Cybersicherheitskontrollen gewährt wird. Ausnahmen von den Mindest-Cybersicherheitskontrollen oder den erweiterten Cybersicherheitskontrollen werden für höchstens drei Jahre gewährt und können verlängert werden.

Relevante NCCS-Artikel

- Artikel 30 (1)



Output

- Genehmigung für Abweichungen von den Kontrollen

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

3 Monate

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

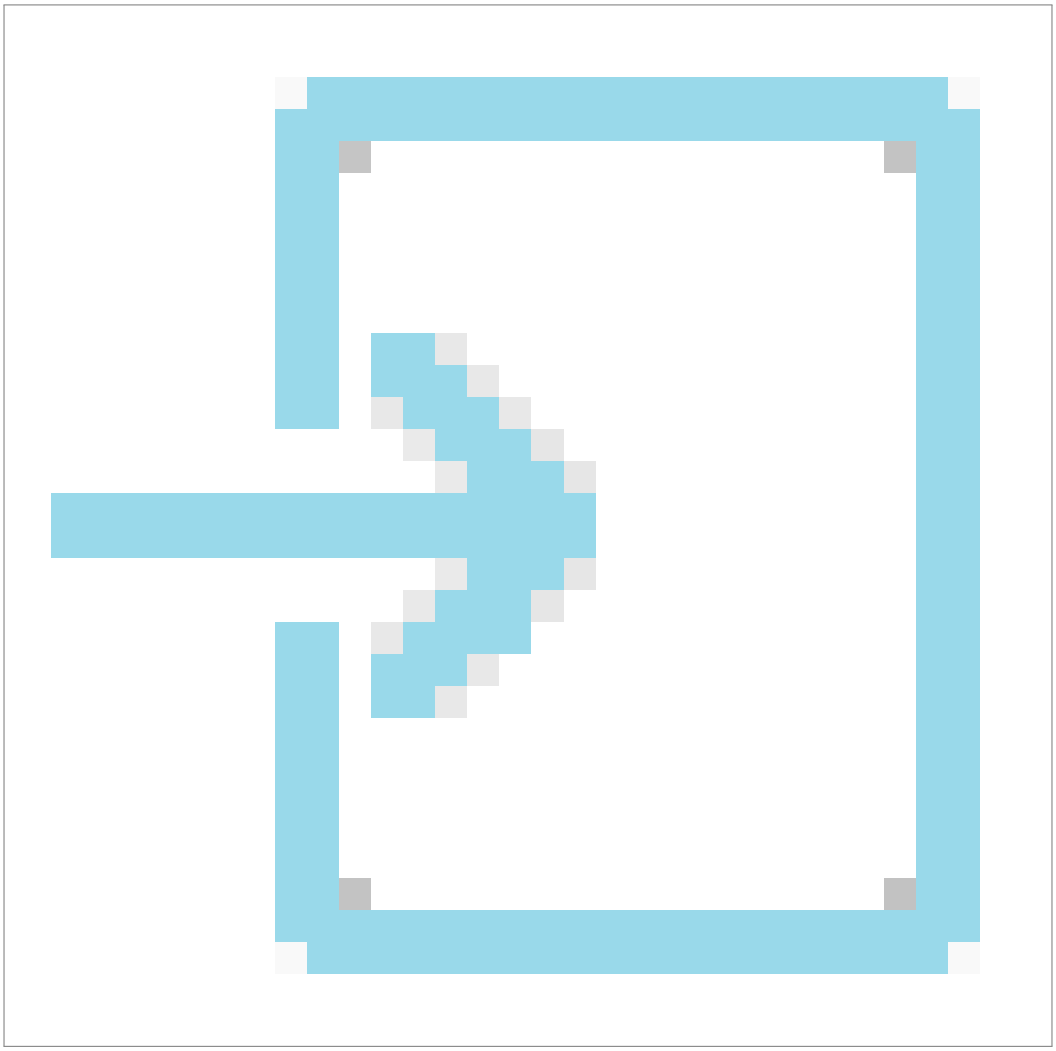
Zu informieren: HIE, CIE, TSO

32.4 Absatz 3

Aggregierte und anonymisierte Informationen zu den gewährten Ausnahmen werden dem umfassenden Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23 als Anhang beigefügt. ENTSO-E und die EU-VNBO aktualisieren die Liste bei Bedarf gemeinsam.

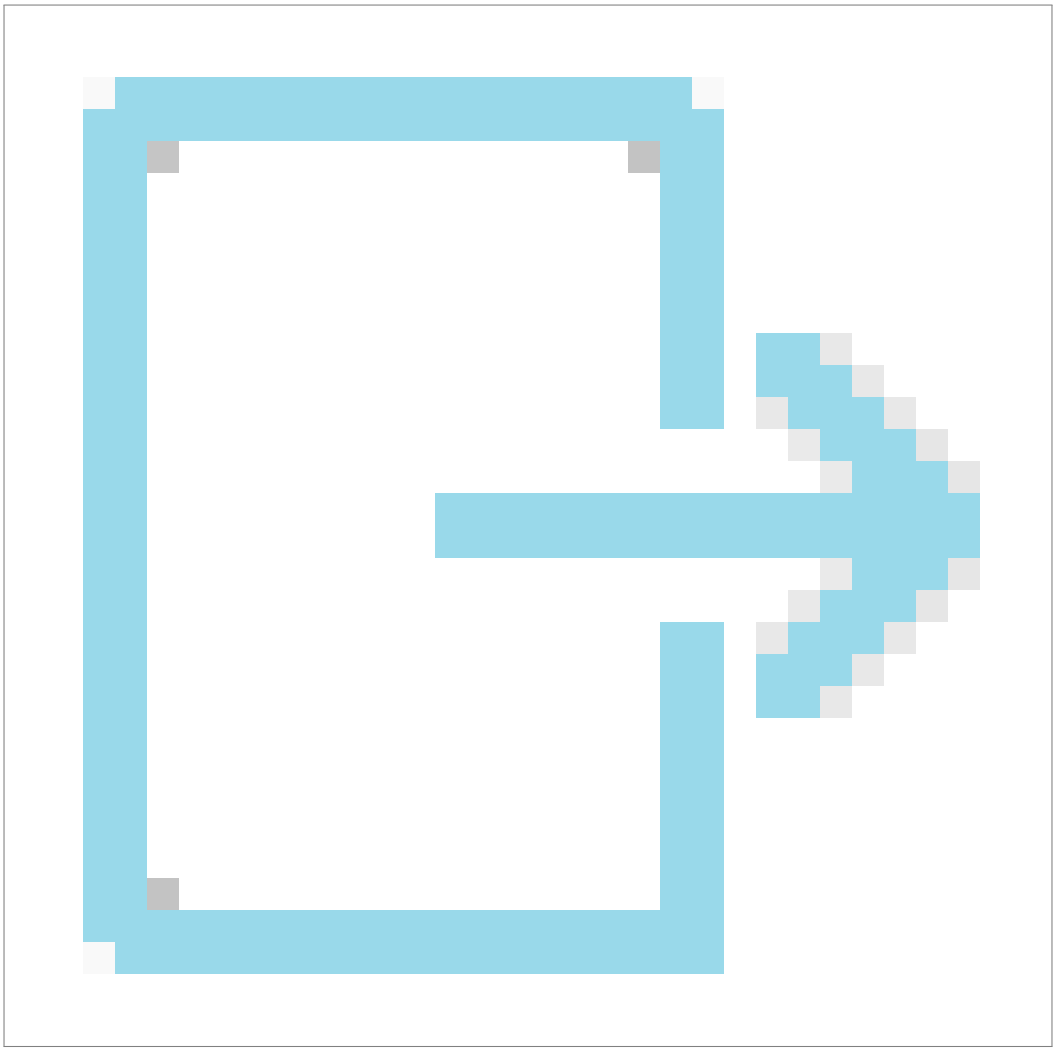
Relevante NCCS-Artikel

- Artikel 23



Input

- Genehmigung für Abweichungen von den Kontrollen



Output

- Gemeinsame Bewertung der Cybersicherheitsrisiken im Stromsektor

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Chapter 33

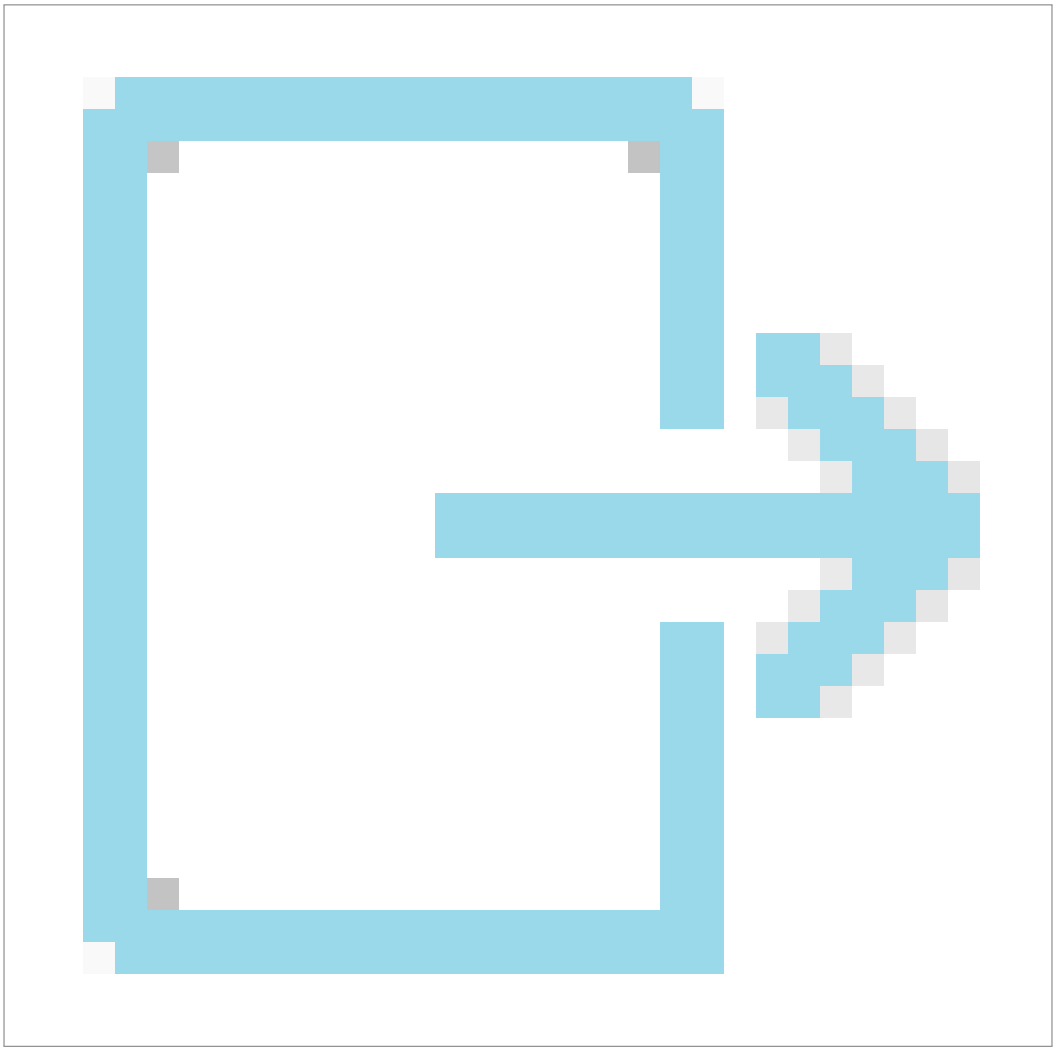
Artikel 31. : Überprüfung des gemeinsamen Rahmens für die Cybersicherheit im Elektrizitätssektor

33.1 Absatz 1

Spätestens 24 Monate nach der Annahme der in Artikel 28 Absatz 1 Buchstaben a, b und c genannten Kontrollen und der Einrichtung des in Buchstabe d jenes Artikels genannten Cybersicherheitsmanagementsystems muss jede gemäß Artikel 24 Absatz 1 ermittelte Einrichtung mit kritischen Auswirkungen in der Lage sein, auf Verlangen der zuständigen Behörde nachzuweisen, dass sie das Cybersicherheitsmanagementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet.

Relevante NCCS-Artikel

- Artikel 28 (1)
- Artikel 24 (1)



Output

- Überprüfung der Einhaltung der Kontrollen

GOOD TO KNOW

Zeitpunkt

24 Monate

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, TSO, NCA

33.2 Absatz 2

Jede Einrichtung mit kritischen Auswirkungen muss die in Absatz 1 genannte Verpflichtung erfüllen, indem sie sich einem von unabhängigen Dritten durchgeführten Sicherheitsaudit gemäß den Anforderungen aus Artikel 25 Absatz 2 unterzieht oder sich an einem nationalen Überprüfungssystem gemäß Artikel 25 Absatz 1 beteiligt.

Relevante NCCS-Artikel

- Artikel 25 (2)
- Artikel 25 (1)
- Artikel 31 (1)

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, TSO

Zu informieren: NCA

33.3 Absatz 3

Die Überprüfung, ob eine Einrichtung mit kritischen Auswirkungen das Cybersicherheits-managementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet, erstreckt sich auf alle Vermögenswerte der Einrichtung mit kritischen Auswirkungen innerhalb ihres Perimeters mit kritischen Auswirkungen.

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, TSO

Zu informieren: NCA

33.4 Absatz 4

Die Überprüfung, ob eine Einrichtung mit kritischen Auswirkungen das Cybersicherheits-managementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet, erstreckt sich auf alle Vermögenswerte der Einrichtung mit kritischen Auswirkungen innerhalb ihres Perimeters mit kritischen Auswirkungen.

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

36 Monate

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, TSO

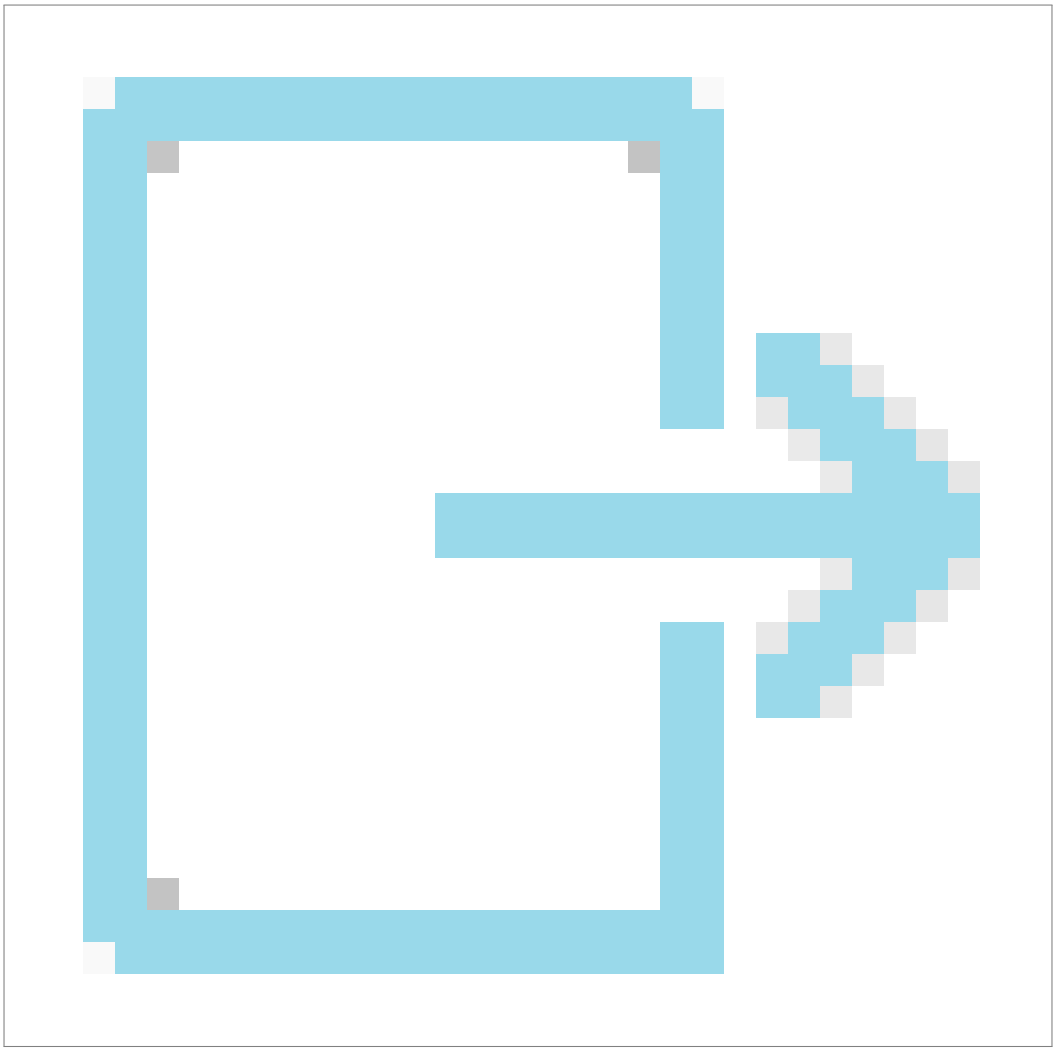
Zu informieren: NCA

33.5 Absatz 5

Jede gemäß Artikel 24 ermittelte Einrichtung mit kritischen Auswirkungen muss die Einhaltung der in Artikel 28 Absatz 1 Buchstaben a, b und c genannten Kontrollen und die Einrichtung des unter Buchstabe d jenes Artikels genannten Cybersicherheitsmanagementsystems nachweisen, indem sie der zuständigen Behörde über das Ergebnis der Überprüfung der Einhaltung Bericht erstattet.

Relevante NCCS-Artikel

- Artikel 24
- Artikel 28 (1)



Output

- Bericht über die Prüfungsergebnisse

A

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: CIE, TSO

Zu informieren: NCA

Chapter 34

Artikel 32. : Cybersicherheitsmanagementsystem

34.1 Absatz 1

Innerhalb von 24 Monaten, nachdem sie von der zuständigen Behörde darüber unterrichtet wurde, dass sie gemäß Artikel 24 Absatz 6 als Einrichtung mit erheblichen oder kritischen Auswirkungen eingestuft wurde, richtet jede Einrichtung mit erheblichen oder kritischen Auswirkungen ein Cybersicherheitsmanagementsystem ein, das sie danach alle drei Jahre überprüft, um

a. den Umfang des Cybersicherheitsmanagementsystems unter Berücksichtigung von Schnittstellen und Abhängigkeiten mit anderen Einrichtungen festzulegen;

b. sicherzustellen, dass die gesamte obere Führungsebene über einschlägige rechtliche Verpflichtungen informiert ist und durch rechtzeitige Entscheidungen und rasche Reaktionen aktiv zur Umsetzung des Cybersicherheitsmanagementsystems beiträgt;

c. sicherzustellen, dass die für das Cybersicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen;

d. ein Cybersicherheitskonzept festzulegen, das dokumentiert und innerhalb der Einrichtung sowie den von den Sicherheitsrisiken betroffenen Parteien bekannt gegeben wird;

e. Zuständigkeiten für Aufgaben, die für die Cybersicherheit relevant sind, zuzuweisen und bekannt zu geben;

f. das Cybersicherheitsrisikomanagement auf der Ebene der Einrichtungen gemäß Artikel 26 durchzuführen;

g. die für die Umsetzung, Pflege und kontinuierliche Verbesserung des Cybersicherheitsmanagementsystems erforderlichen Ressourcen festzulegen und bereitzustellen, wobei die erforderlichen Kompetenzen und die Sensibilisierung für Cybersicherheitsressourcen zu berücksichtigen sind; h) die für die Cybersicherheit relevante interne und externe Kommunikation festzulegen;

h. dokumentierte Informationen im Zusammenhang mit dem Cybersicherheitsmanagementsystem zu erstellen, zu aktualisieren und zu kontrollieren;

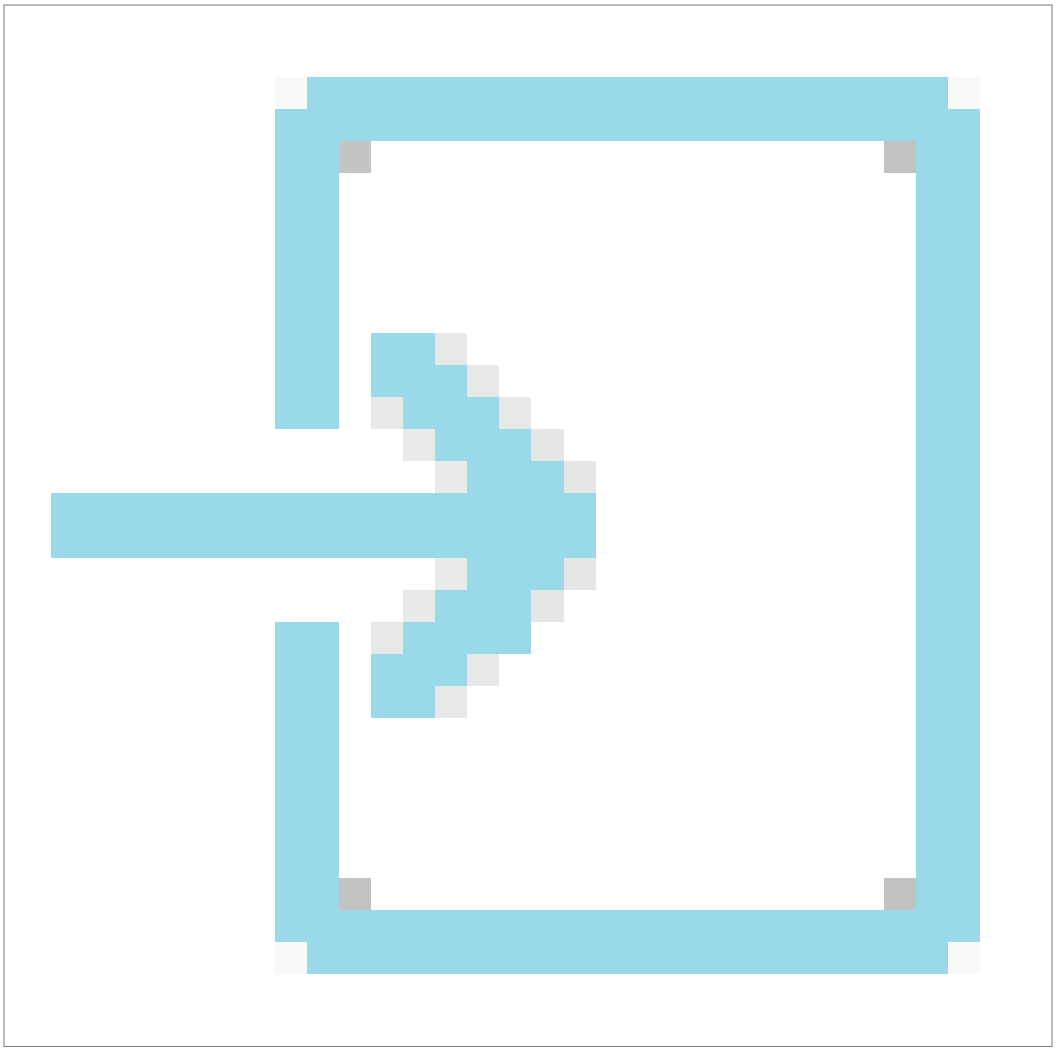
i. die Ergebnisse und Wirksamkeit des Cybersicherheitsmanagementsystems zu beurteilen;

j. in geplanten Zeitabständen interne Audits durchzuführen, um sicherzustellen, dass das Cybersicherheitsmanagementsystem wirksam umgesetzt und gepflegt wird;

k. die Umsetzung des Cybersicherheitsmanagementsystems in geplanten Zeitabständen zu überprüfen und Abweichungen der Ressourcen und Tätigkeiten von den Konzepten, Verfahren und Leitlinien des Cybersicherheitsmanagementsystems zu kontrollieren und zu beheben.

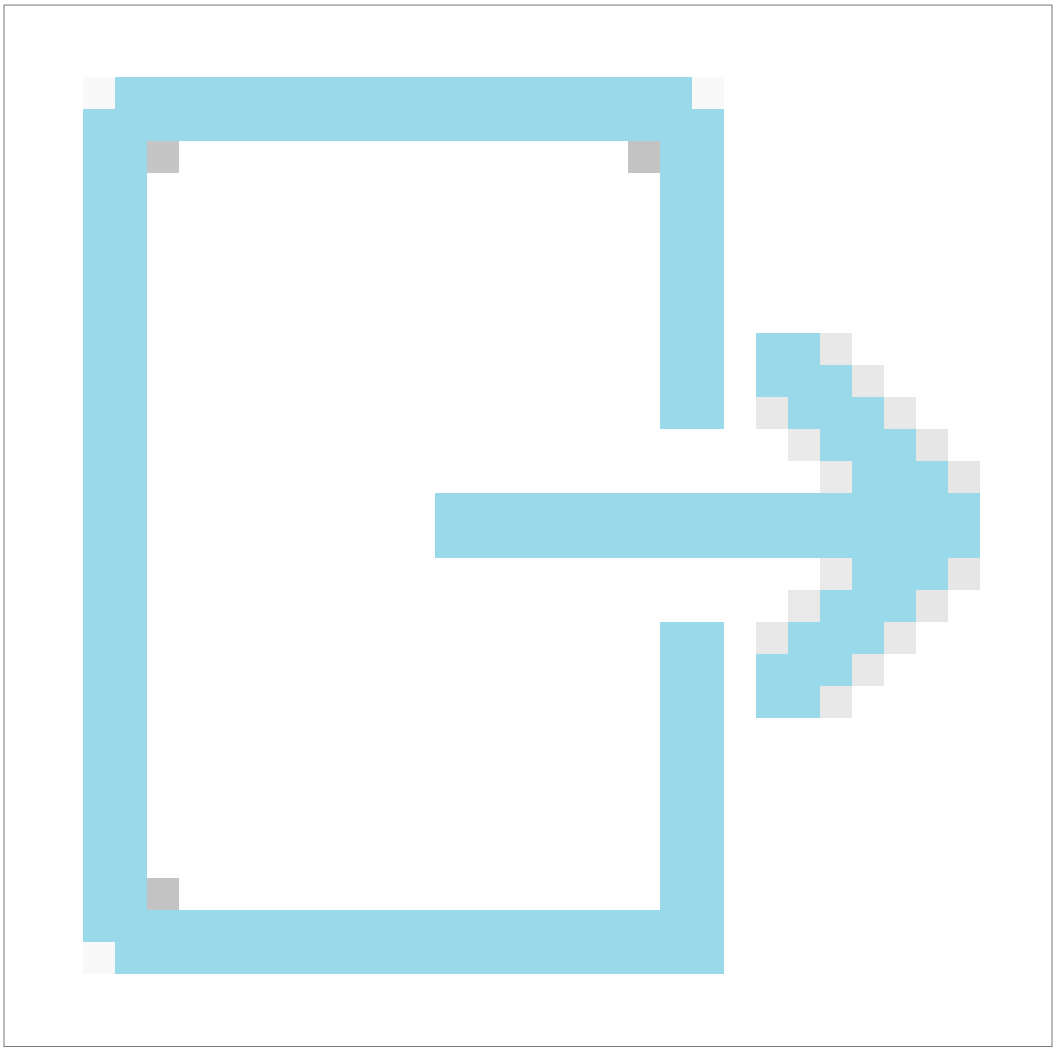
Relevante NCCS-Artikel

- Artikel 24 (6)
- Artikel 26



Input

- Internationale Normen



Output

- Cybersicherheits-Rahmenwerk

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

24 Monate

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

34.2 Absatz 2

Der Anwendungsbereich des Cybersicherheitsmanagementsystems der Einrichtung mit erheblichen Auswirkungen umfasst alle Vermögenswerte innerhalb ihres Perimeters mit erheblichen Auswirkungen.

Verantwortlich für die Aktivität: HIE

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE

34.3 Absatz 3

Die zuständigen Behörden regen an, für die Sicherheit von Netz- und Informationssystemen relevante europäische oder internationaler Normen und Spezifikationen anzuwenden, ohne dabei die Nutzung einer bestimmten Technologie vorzuschreiben oder zu begünstigen.

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA

Chapter 35

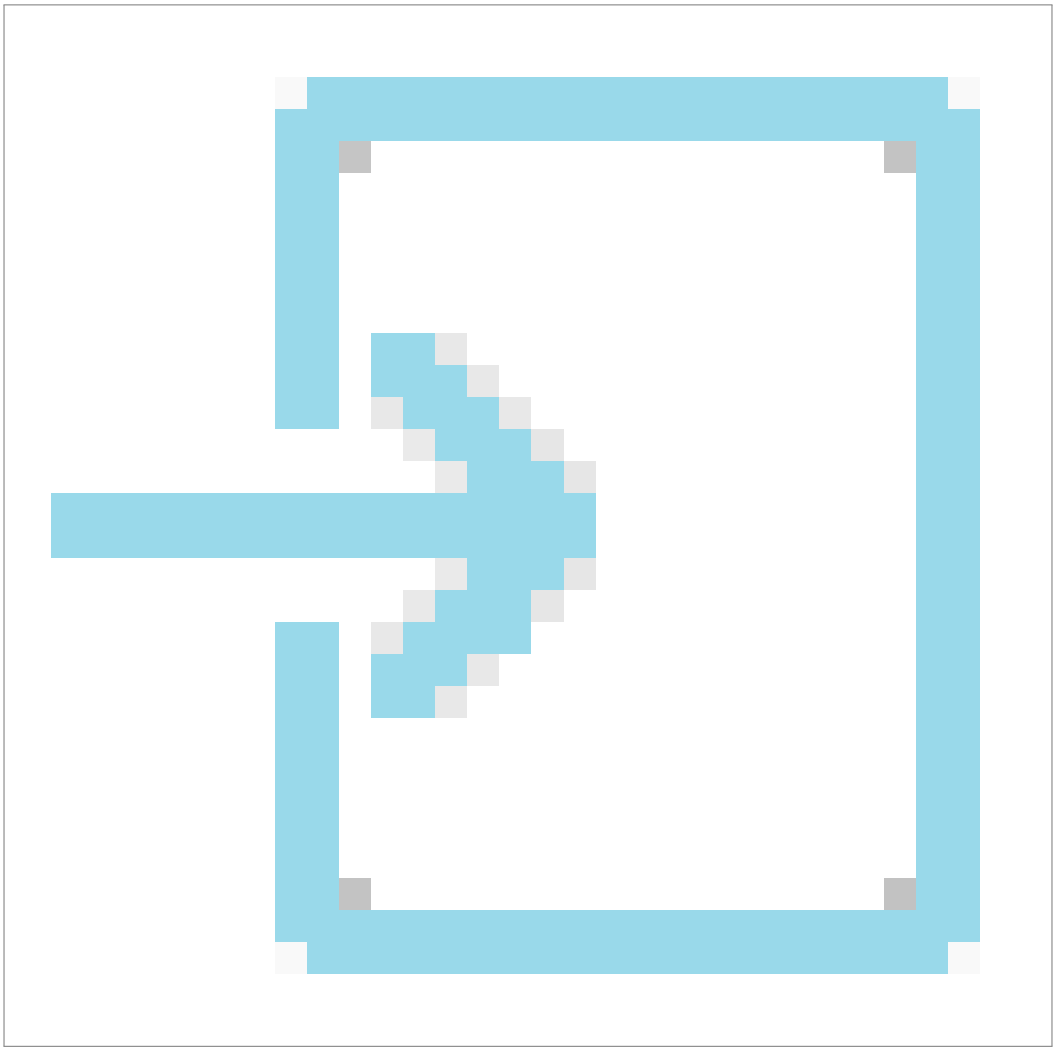
Artikel 33. : Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen in der Lieferkette

35.1 Absatz 1

Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO einen Vorschlag für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen in der Lieferkette, mit denen die in den unionsweiten Bewertungen des Cybersicherheitsrisikos ermittelten Risiken für die Lieferketten gemindert werden, um die gemäß Artikel 29 entwickelten Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen zu ergänzen. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette werden zusammen mit den Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen gemäß Artikel 29 entwickelt. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette erstrecken sich auf den gesamten Lebenszyklus aller IKT-Produkte, -Dienste und -Prozesse einer Einrichtung mit erheblichen oder kritischen Auswirkungen innerhalb ihrer Perimeter mit erheblichen oder kritischen Auswirkungen. Bei der Entwicklung des Vorschlags für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen in der Lieferkette wird die NIS-Kooperationsgruppe konsultiert.

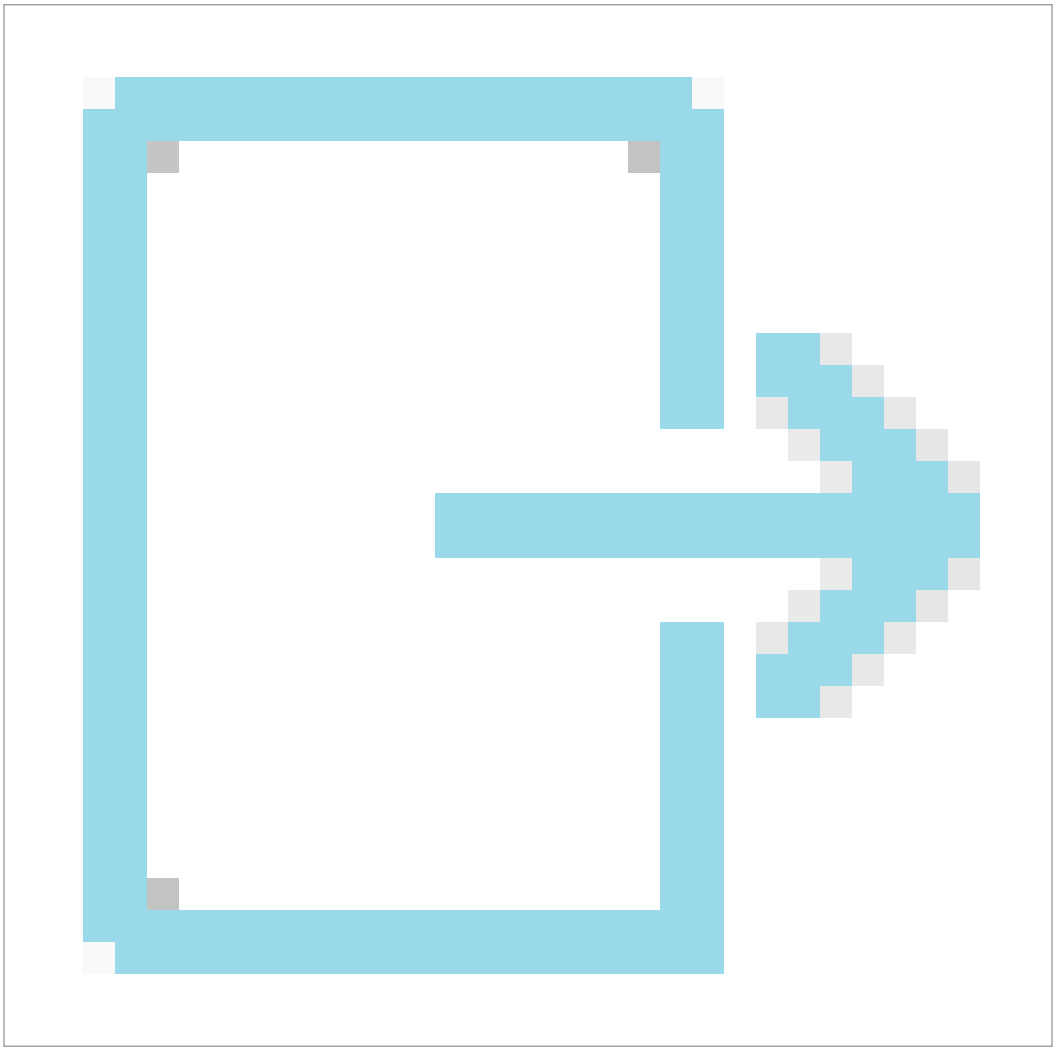
Relevante NCCS-Artikel

- Artikel 19 (4)
- Artikel 29



Input

- Mindest- und erweiterte Cybersicherheitskontrollen



Output

- Mindest- und erweiterte Cybersicherheitskontrollen in der Lieferkette (Entwurf)

GOOD TO KNOW

Zeitpunkt

Innerhalb von 7 Monaten nach Einreichung des ersten Entwurfs des EU-weiten Berichts zur

> Bewertung der Cybersicherheitsrisiken

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: NIS CG

35.2 Absatz 2

Die Mindest-Cybersicherheitskontrollen in der Lieferkette bestehen aus Kontrollen für Einrichtungen mit erheblichen oder kritischen Auswirkungen, die

a. auf Cybersicherheitsspezifikationen bezogene Empfehlungen für die Beschaffung von IKT-Produkten, -Diensten und -Prozessen enthalten und mindestens Folgendes abdecken:

   i. Zuverlässigkeitsüberprüfungen der Mitarbeiter des Anbieters, die an der Lieferkette beteiligt sind und sich mit sensiblen Informationen befassen oder Zugang zu Vermögenswerten mit erheblichen oder kritischen Auswirkungen der Einrichtung haben. Die Zuverlässigkeitsüberprüfung kann eine Überprüfung der Identität und des Hintergrunds von Mitarbeitern oder Auftragnehmern einer Einrichtung im Einklang mit den nationalen Rechtsvorschriften und Verfahren sowie dem einschlägigen und geltenden Unionsrecht umfassen, einschließlich der Verordnung (EU) 2016/679 [a] und der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates [b] Zuverlässigkeitsüberprüfungen müssen verhältnismäßig und strikt auf das Notwendige beschränkt sein. Sie werden ausschließlich zum Zweck der Bewertung eines potenziellen Sicherheitsrisikos für die betreffende Einrichtung durchgeführt. Sie müssen in einem angemessenen Verhältnis zu den Geschäftserfordernissen, der Klassifizierung der einzusehenden Informationen und den wahrgenommenen Risiken stehen und können von der Einrichtung selbst, einem externen Unternehmen, das ein Screening

durchführt, oder durch staatliches Clearing vorgenommen werden;

ii. die Prozesse für eine sichere und kontrollierte Gestaltung, Entwicklung und Herstellung von IKT-Produkten, -Diensten und -Prozessen, die Förderung der Gestaltung und Entwicklung von IKT-Produkten, -Diensten und -Prozessen, die geeignete technische Maßnahmen zur Gewährleistung der Cybersicherheit umfassen;

iii. die Gestaltung von Netz- und Informationssystemen, in denen Geräte selbst dann nicht als vertrauenswürdig gelten, wenn sie sich in einem sicheren Perimeter befinden, eine Überprüfung aller eingegangenen Anfragen erfordern und das Prinzip der minimalen Berechtigung angewandt wird;

iv. den Zugang des Anbieters zu den Vermögenswerten der Einrichtung;

v. die vertraglichen Verpflichtungen des Anbieters zum Schutz sensibler Informationen der Einrichtung und zur Beschränkung des Zugangs zu diesen Informationen;

vi. die zugrunde liegenden Spezifikationen für die Cybersicherheit bei der Auftragsvergabe an Unterauftragnehmer des Anbieters;

vii. die Rückverfolgbarkeit der Anwendung der Cybersicherheitsspezifikationen von der Entwicklung über die Produktion bis zur Bereitstellung von IKT-Produkten, -Diensten oder -Prozessen;

viii. die Unterstützung von Sicherheitsaktualisierungen während der gesamten Lebensdauer von IKT-Produkten, -Diensten oder -Prozessen;

ix. das Recht auf Prüfung der Cybersicherheit in den Konzeptions-, Entwicklungs- und Produktionsprozessen des Anbieters sowie

x. die Bewertung des Risikoprofils des Anbieters;

b. diese Einrichtungen dazu verpflichten, die unter Buchstabe a genannten Empfehlungen für die Auftragsvergabe zu berücksichtigen, wenn sie Verträge mit Anbietern, Kooperationspartnern und anderen Parteien in der Lieferkette schließen, sowohl in Bezug auf normale Lieferungen von IKT-Produkten, -Diensten und -Prozessen als auch in Bezug auf ungeplante Ereignisse und Umstände wie die Kündigung und den Übergang von Verträgen im Falle von Fahrlässigkeit des Vertragspartners;

c. diese Einrichtungen dazu verpflichten, die Ergebnisse einschlägiger koordinierter Sicherheitsrisikobewertungen kritischer Lieferketten gemäß Artikel 22 Absatz 1 der Richtlinie (EU) 2022/2555 zu berücksichtigen;

d. Kriterien für die Auswahl von Anbietern und die Auftragsvergabe an Anbieter enthalten, die die unter Buchstabe a genannten Cybersicherheitsspezifikationen erfüllen können und über ein Maß an Cybersicherheit verfügen, das den Cybersicherheitsrisiken des vom Anbieter bereitgestellten IKT-Produkts, -Dienstes oder -Prozesses angemessen ist;

e. Kriterien für die Diversifizierung der Bezugsquellen für IKT-Produkte, -Dienste und -Prozesse und zur Verringerung des Risikos eines Anbieter-Lock-ins enthalten;

f. Kriterien für die regelmäßige Überwachung, Überprüfung oder Prüfung der Cybersicherheitsspezifikationen für interne Betriebsprozesse des Anbieters während des gesamten Lebenszyklus jedes IKT-Produkts, -Dienstes und -Prozesses enthalten.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016L0680

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, Critical ICT

35.3 Absatz 3

Für die Cybersicherheitsspezifikationen in der in Absatz 2 Buchstabe a genannten Empfehlung zur Cybersicherheit bei der Auftragsvergabe wenden Einrichtungen mit erheblichen Auswirkungen im Einklang mit Artikel 35 Absatz 4 die Grundsätze der Auftragsvergabe aus der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates [a] an oder legen ihre eigenen Spezifikationen auf der Grundlage der Ergebnisse der Bewertung des Cybersicherheitsrisikos auf der Ebene der Einrichtung fest.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014L0024#d1e3478-65-1

Relevante NCCS-Artikel

- Artikel 33 (2)
- Artikel 35 (4)

Verantwortlich für die Aktivität: HIE

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE

35.4 Absatz 3

Für die Cybersicherheitsspezifikationen in der in Absatz 2 Buchstabe a genannten Empfehlung zur Cybersicherheit bei der Auftragsvergabe wenden Einrichtungen mit erheblichen oder kritischen Auswirkungen im Einklang mit Artikel 35 Absatz 4 die Grundsätze der Auftragsvergabe aus der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates [a] an oder legen ihre eigenen Spezifikationen auf der Grundlage der Ergebnisse der Bewertung des Cybersicherheitsrisikos auf der Ebene der Einrichtung fest.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014L0024#d1e3478-65-1

Relevante NCCS-Artikel

- Artikel 33 (2)
- Artikel 35 (4)

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, TSO

35.5 Absatz 4

Die erweiterten Cybersicherheitskontrollen in der Lieferkette müssen Kontrollen für Einrichtungen mit kritischen Auswirkungen umfassen, um bei der Auftragsvergabe zu überprüfen, ob IKT-Produkte, -Dienste und -Prozesse, die als Vermögenswerte mit kritischen Auswirkungen verwendet werden sollen, den Cybersicherheitsspezifikationen entsprechen. Das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess wird entweder durch ein europäisches Schema für die Cybersicherheitszertifizierung gemäß Artikel 31 oder mit von der Einrichtung ausgewählten und organisierten Überprüfungsmaßnahmen überprüft. Die Überprüfungsmaßnahmen müssen ausreichend gründlich und umfassend sein, um zu gewährleisten, dass das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess genutzt werden kann, um die in der Risikobewertung auf Ebene der Einrichtung ermittelten Risiken zu mindern. Die Einrichtung mit kritischen Auswirkungen dokumentiert die Maßnahmen zur Verringerung der ermittelten Risiken.

Relevante NCCS-Artikel

- Artikel 36

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

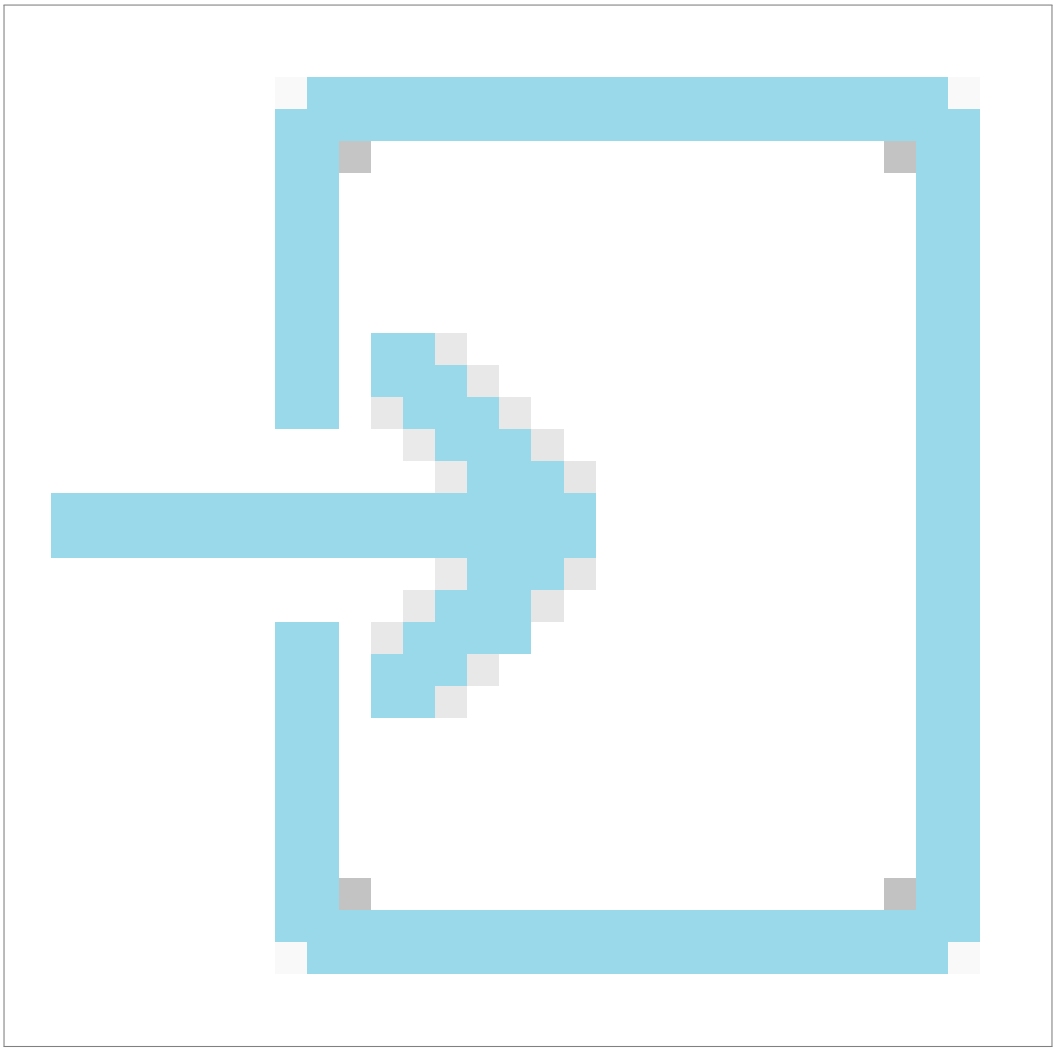
Beteiligt an der Aufgabenausführung: CIE, TSO

35.6 Absatz 5

Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für die Beschaffung relevanter IKT-Produkte, -Dienste und -Prozesse. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit kritischen oder erheblichen Auswirkungen ermittelt wurden, bei der Auftragsvergabe ab sechs Monaten nach der Annahme oder Aktualisierung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 29.

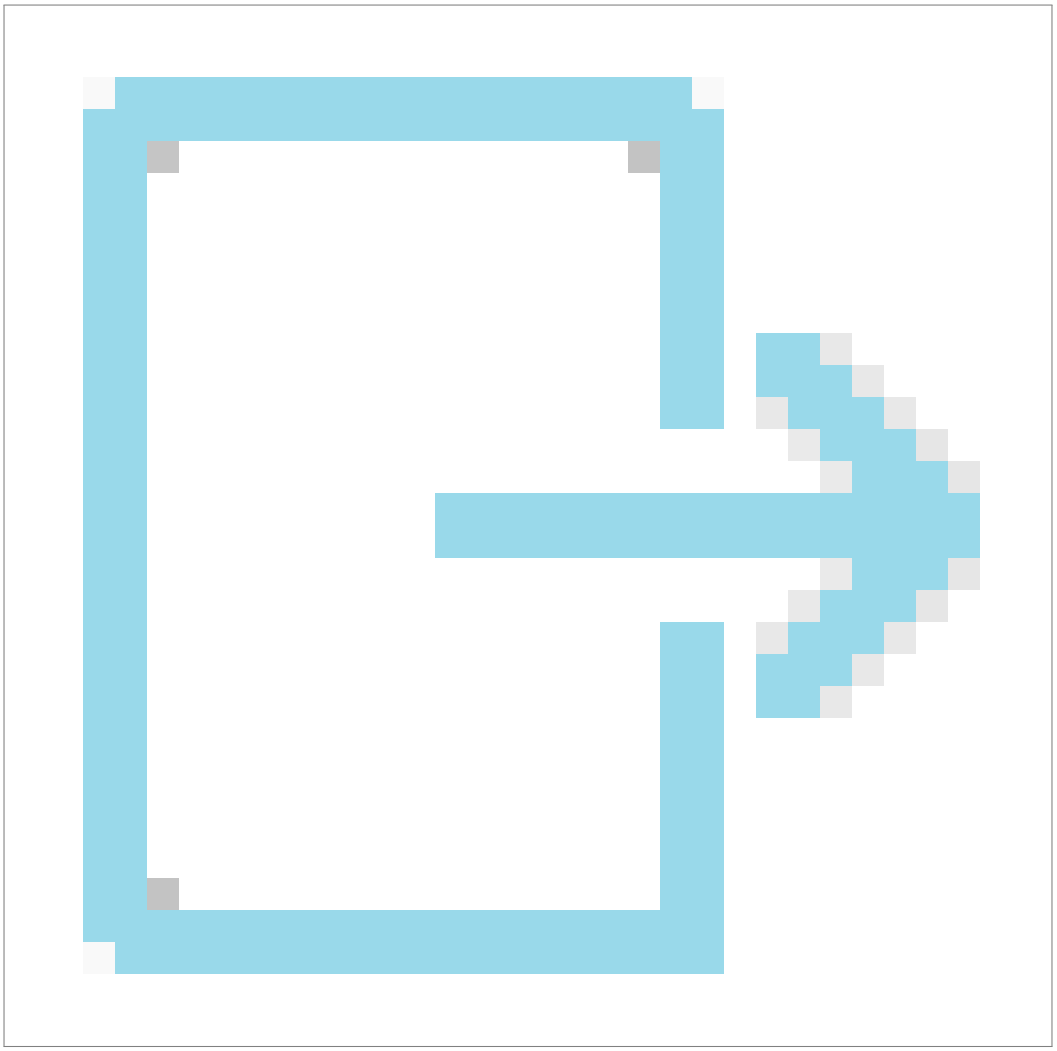
Relevante NCCS-Artikel

- Artikel 24
- Artikel 29



Input

- Mindest- und erweiterte Cybersicherheitskontrollen



Output

- Anwendung von Mindest- und erweiterten Cybersicherheitskontrollen

GOOD TO KNOW

Zeitpunkt

Sechs Monate nach der Annahme oder Aktualisierung der Mindest- und erweiterten Cybersicherheitskontrollen

Verantwortlich für die Aktivität: HIE

Beteiligte Stakeholder:

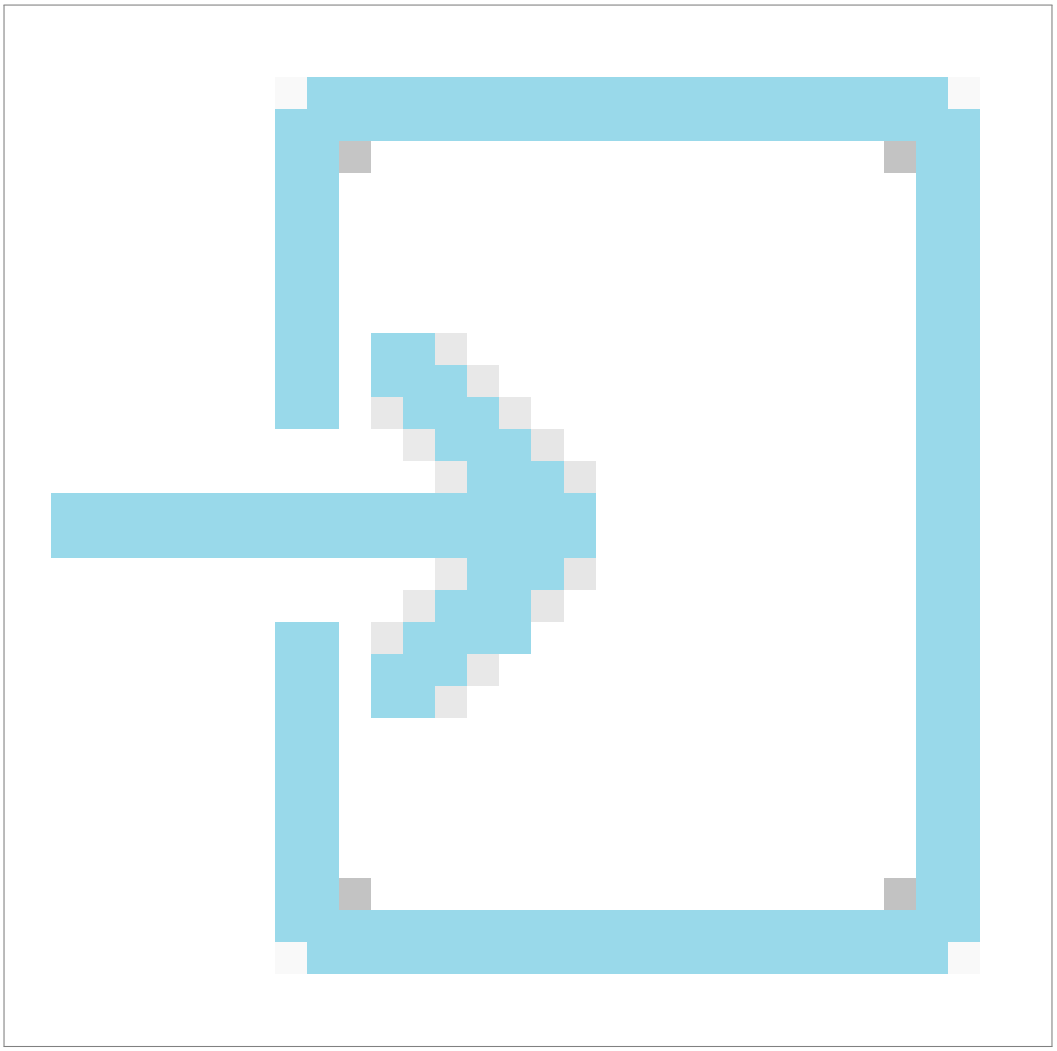
Beteiligt an der Aufgabenausführung: HIE

35.7 Absatz 5

Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für die Beschaffung relevanter IKT-Produkte, -Dienste und -Prozesse. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit kritischen oder erheblichen Auswirkungen ermittelt wurden, bei der Auftragsvergabe ab sechs Monaten nach der Annahme oder Aktualisierung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 29.

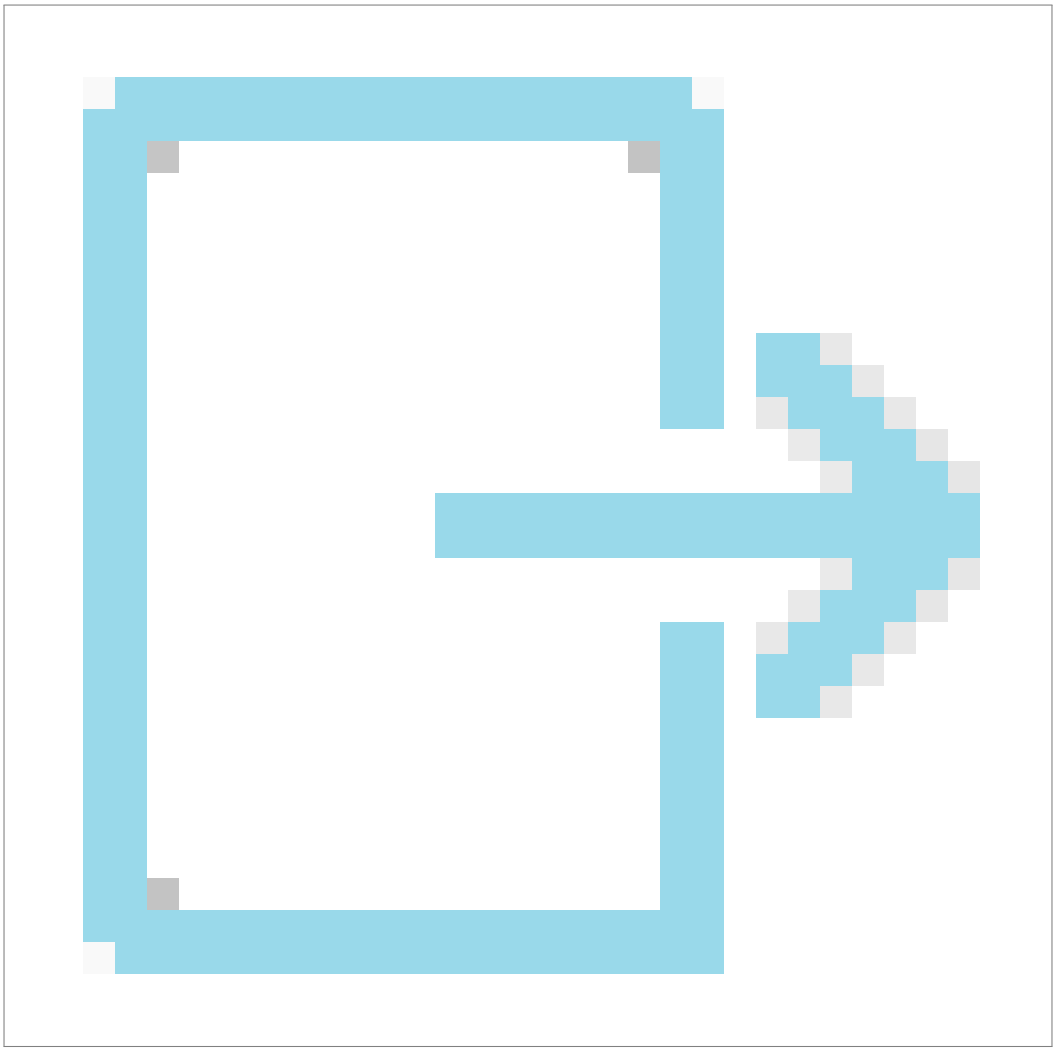
Relevante NCCS-Artikel

- Artikel 24
- Artikel 29



Input

- Mindest- und erweiterte Cybersicherheitskontrollen



Output

- Mindest- und erweiterte Cybersicherheitskontrollen in der Lieferkette

GOOD TO KNOW

Zeitpunkt

Sechs Monate nach der Annahme oder Aktualisierung der Mindest- und erweiterten Cybersicherheitskontrollen

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

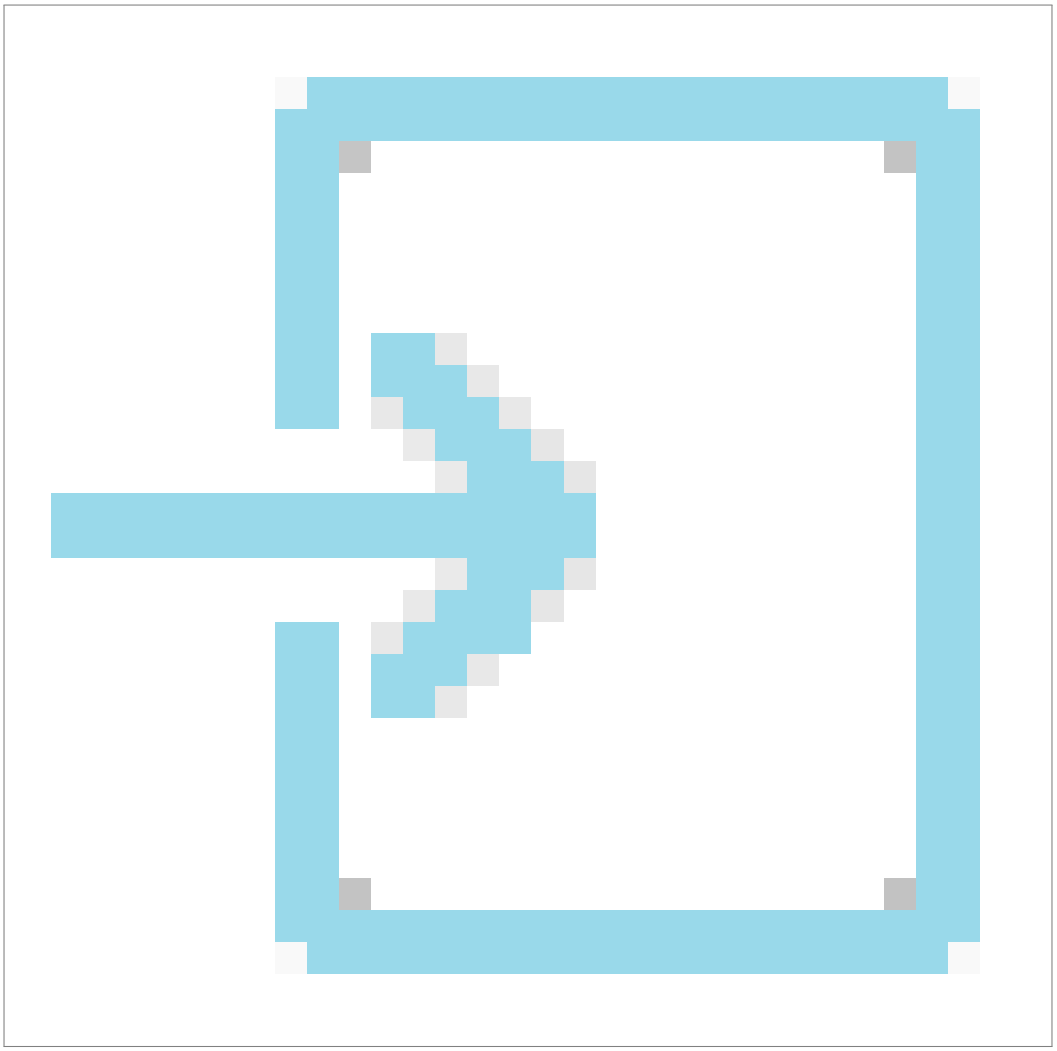
Beteiligt an der Aufgabenausführung: CIE, TSO

35.8 Absatz 6

Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO der zuständigen Behörde eine Änderung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen in der Lieferkette vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

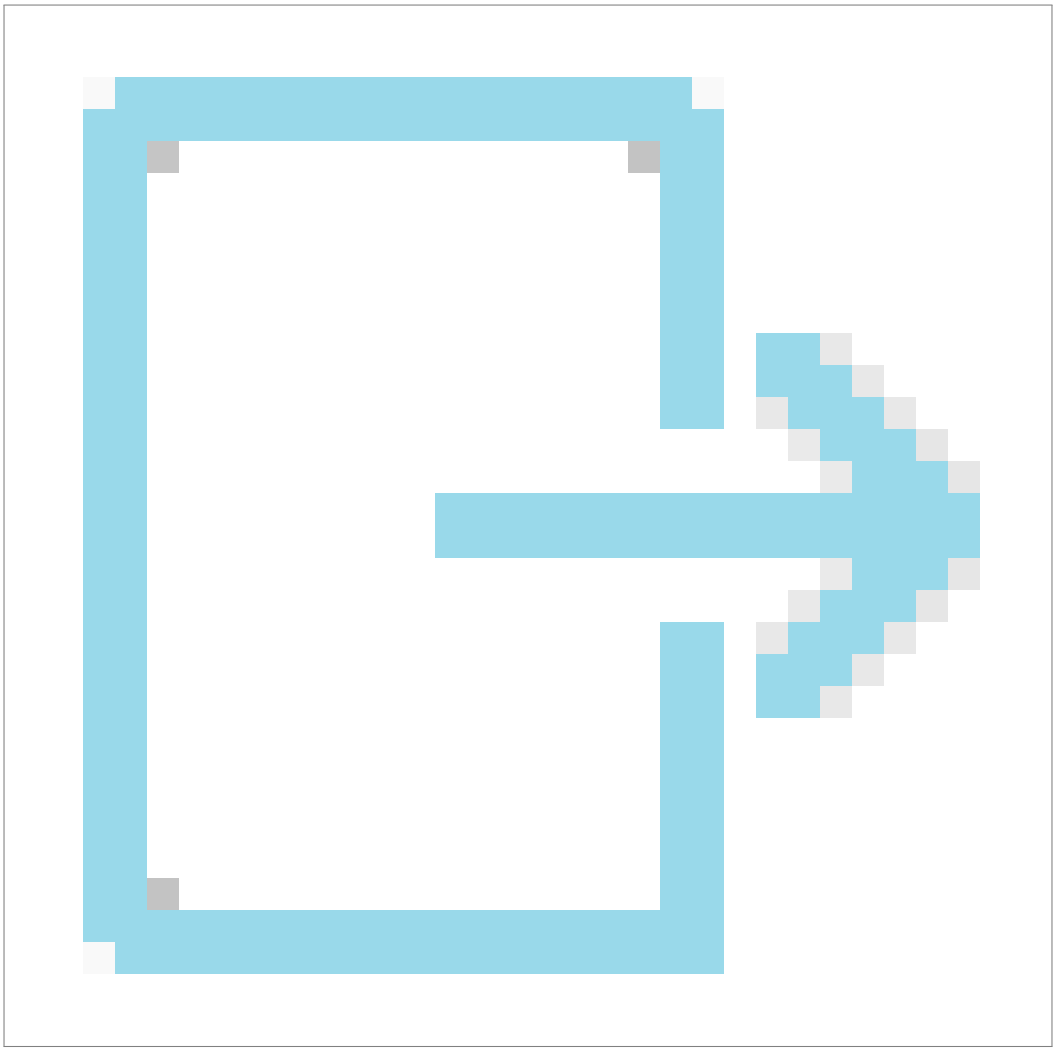
Relevante NCCS-Artikel

- Artikel 21 (2)
- Artikel 8 (10)



Input

- Mindest- und erweiterte Cybersicherheitskontrollen



Output

- Mindest- und erweiterte Cybersicherheitskontrollen (modifiziert)

GOOD TO KNOW

Zeitpunkt

Innerhalb von 6 Monaten nach Erstellung des regionalen Berichts zur Bewertung der Cybersicherheitsrisiken

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu informieren: NCA

Chapter 36

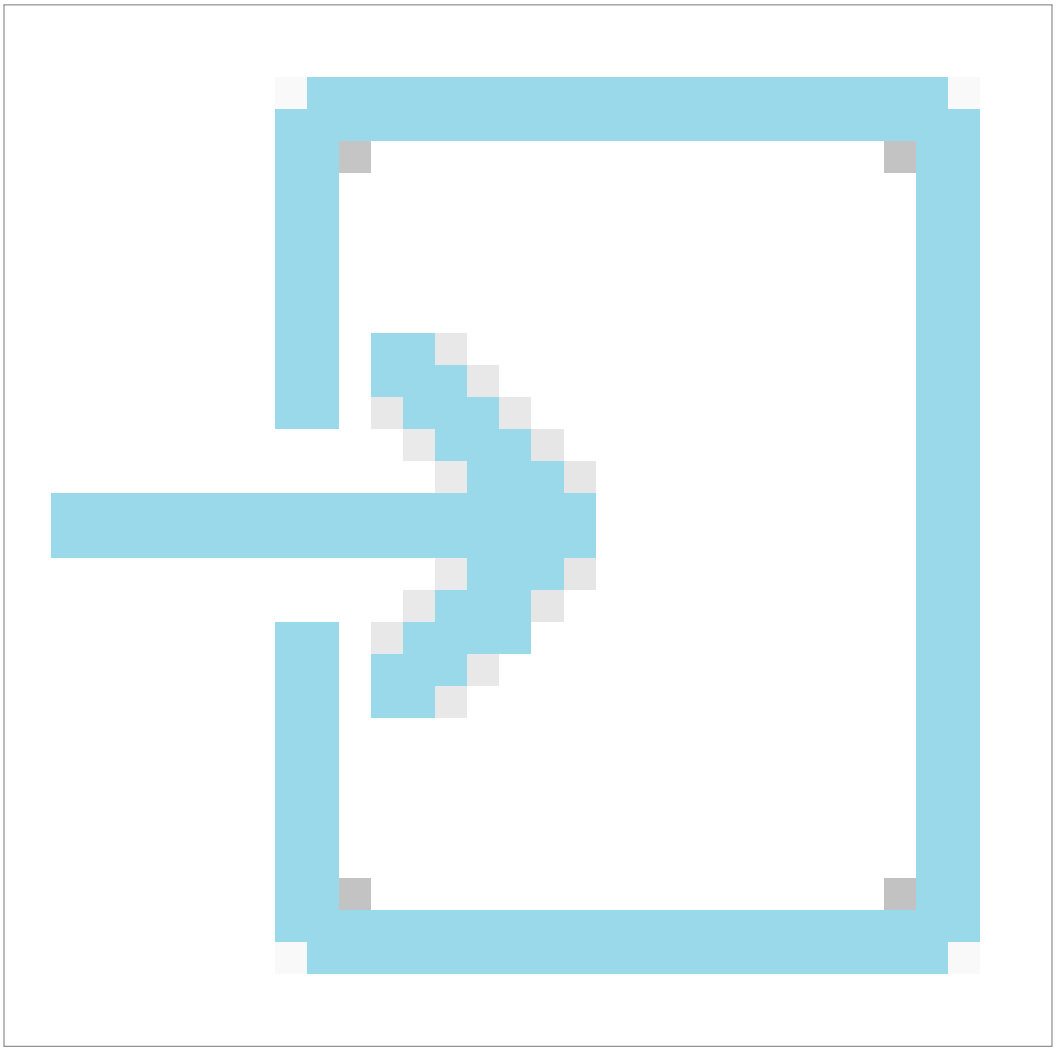
Artikel 34. : Vergleichsmatrix für Cybersicherheitskontrollen im Elektrizitätssektor anhand von Normen

36.1 Absatz 1

Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der ENISA einen Vorschlag für eine Matrix, mit der die Kontrollen gemäß Artikel 28 Absatz 1 Buchstaben a und b anhand ausgewählter europäischer und internationaler Normen sowie einschlägiger technischer Spezifikationen verglichen werden (im Folgenden „Vergleichsmatrix“).

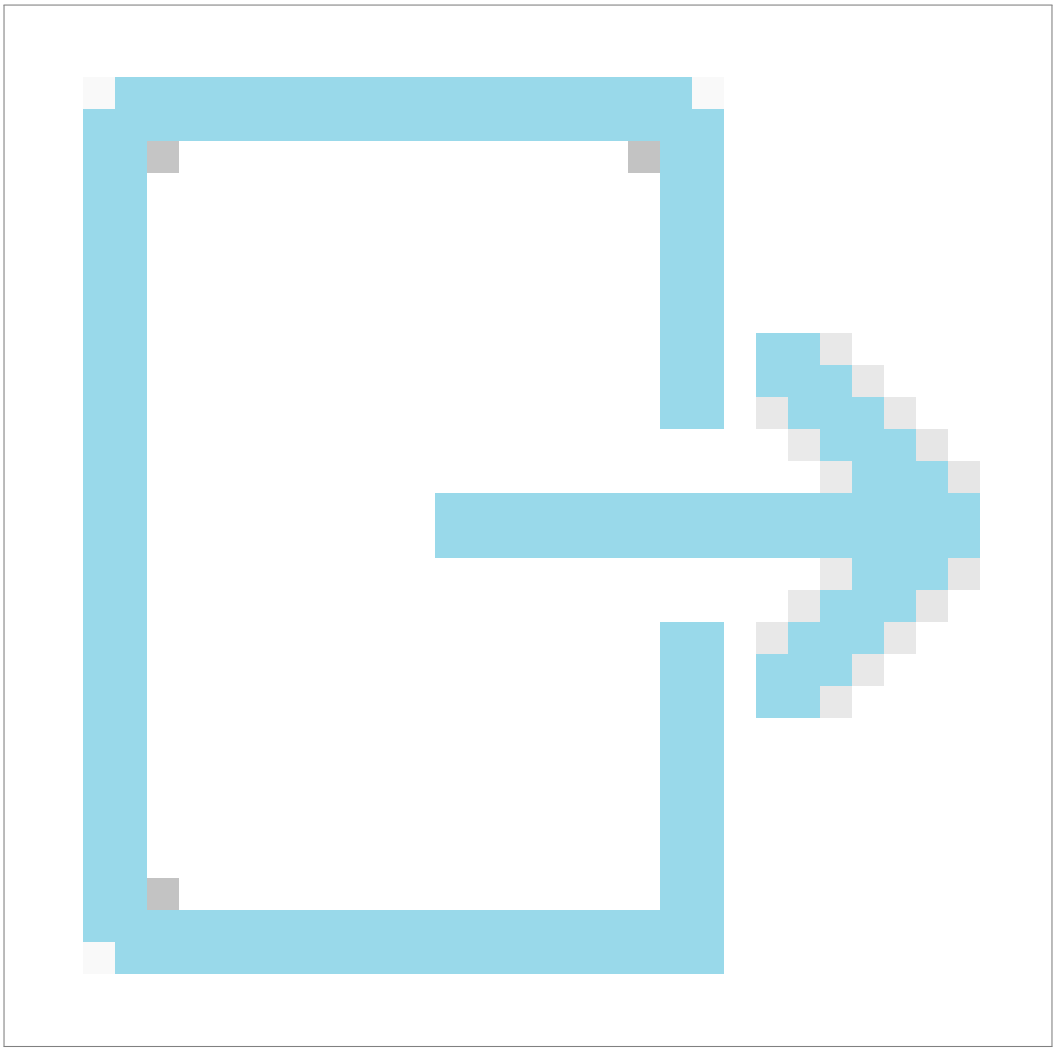
Relevante NCCS-Artikel

- Artikel 19 (4)
- Artikel 28 (1)



Input

- Nationale Normen und Kontrollen
- Vorläufige Liste europäischer und internationaler Normen und Kontrollen



Output

- Zuordnungsmatrix (Entwurf)

GOOD TO KNOW

Zeitpunkt

Innerhalb von 7 Monaten nach Einreichung des ersten Entwurfs des Berichts zur Bewertung der Cybersicherheitsrisiken

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: ENISA

36.2 Absatz 1

ENTSO-E und die EU-VNBO dokumentieren die Gleichwertigkeit der verschiedenen Kontrollen mit den in Artikel 28 Absatz 1 Buchstaben a und b genannten Kontrollen.

Relevante NCCS-Artikel

- Artikel 28 (1)

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

36.3 Absatz 2

Die zuständigen Behörden können ENTSO-E und der EU-VNBO einen Vergleich der in Artikel 28 Absatz 1 Buchstaben a und b genannten Kontrollen mit dem entsprechenden nationalen Rechts- und Verwaltungsrahmen, einschließlich der einschlägigen nationalen Normen der Mitgliedstaaten gemäß Artikel 25 der Richtlinie (EU) 2022/2555 [a], übermitteln.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid=1733994458451#art_25

Relevante NCCS-Artikel

- Artikel 28 (1)

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO, NCA

36.4 Absatz 2

Stellt die zuständige Behörde eines Mitgliedstaats einen solchen Vergleich bereit, so integrieren ENTSO-E und die EU-VNBO diesen nationalen Vergleich in die Vergleichsmatrix.

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

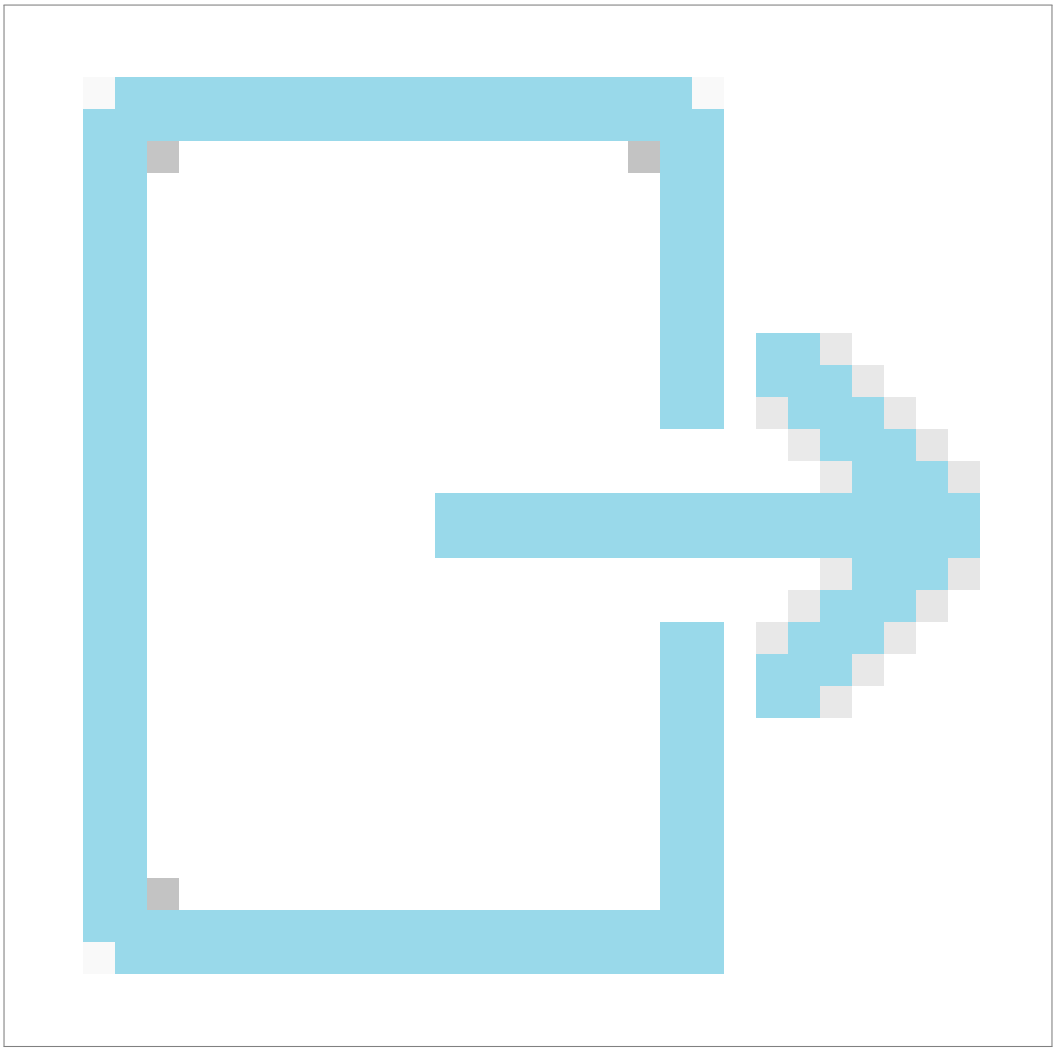
Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO, NCA

36.5 Absatz 3

Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sowie in Absprache mit der ENISA der zuständigen Behörde eine Änderung der Vergleichsmatrix vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

Relevante NCCS-Artikel

- Artikel 21 (2)
- Artikel 8 (10)



Output

- Zuordnungsmatrix (Änderungsvorschlag)

GOOD TO KNOW

Zeitpunkt

Innerhalb von 6 Monaten nach Erstellung der regionalen Berichte zur Bewertung der Cybersicherheitsrisiken

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: ENISA

Zu informieren: NCA

Chapter 37

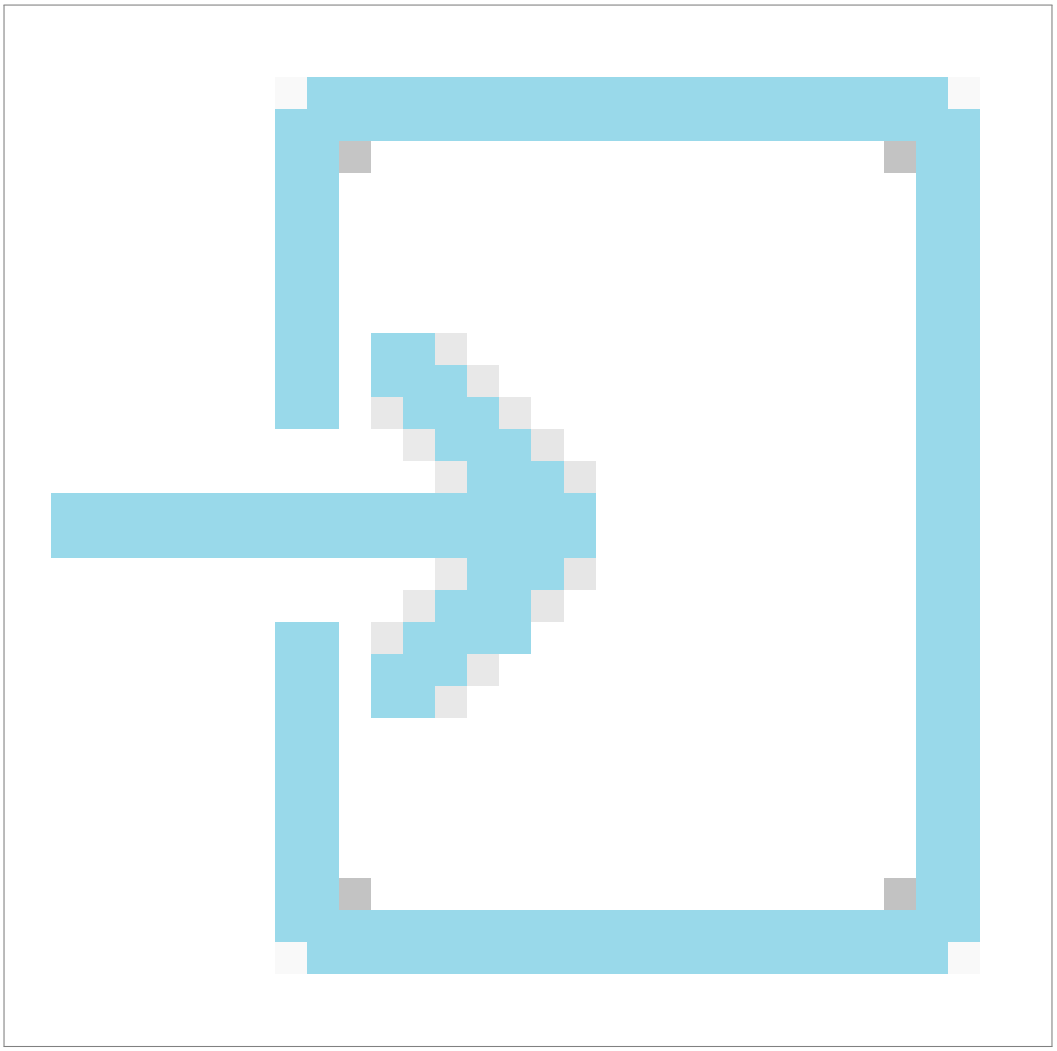
Artikel 35. : Empfehlungen für die Cybersicherheit bei der Auftragsvergabe

37.1 Absatz 1

Die ÜNB entwickeln mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO in einem Arbeitsprogramm, das jedes Mal bei der Annahme eines Berichts über die regionale Bewertung des Cybersicherheitsrisikos erstellt und aktualisiert wird, eine Reihe von unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe, die Einrichtungen mit erheblichen oder kritischen Auswirkungen als Grundlage für die Beschaffung von IKT-Produkten, -Diensten und -Prozessen in den Perimetern mit erheblichen oder kritischen Auswirkungen nutzen können. Dieses Arbeitsprogramm umfasst

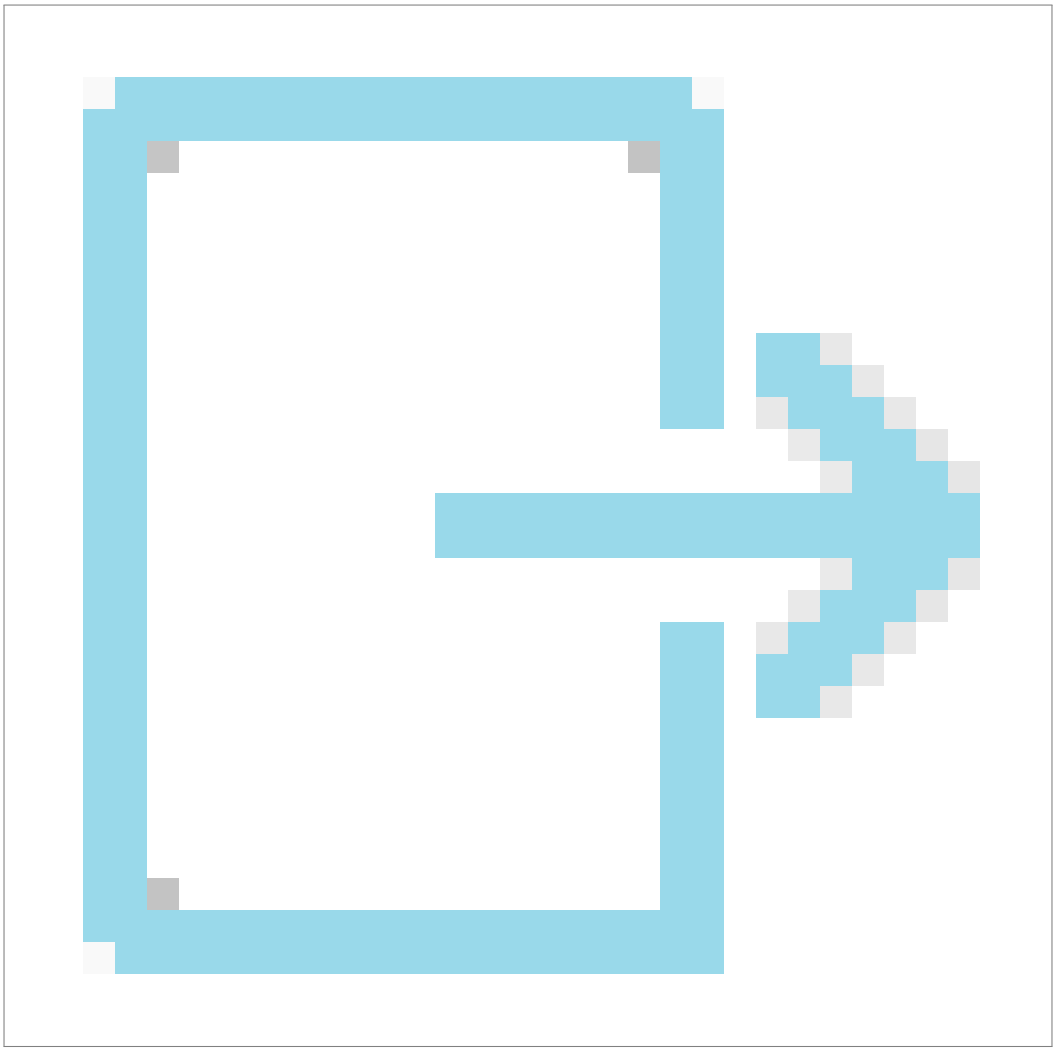
a. eine Beschreibung und Klassifizierung der Arten von IKT-Produkten, -Diensten und -Prozessen, die von Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Perimeter mit erheblichen oder kritischen Auswirkungen verwendet werden;

b. eine Liste der Arten von IKT-Produkten, -Diensten und -Prozessen, für die eine Reihe unverbindlicher Cybersicherheitsempfehlungen auf der Grundlage der einschlägigen Berichte über die regionale Bewertung des Cybersicherheitsrisikos und der Prioritäten von Einrichtungen mit erheblichen oder kritischen Auswirkungen zu erstellen sind.



Input

- Vorläufige Liste europäischer und internationaler Normen und Kontrollen
- Regionaler Bericht zur Bewertung von Cybersicherheitsrisiken



Output

- Empfehlungen für die Beschaffung im Bereich Cybersicherheit

GOOD TO KNOW

Zeitpunkt

6 Monate nach der Genehmigung oder Aktualisierung des regionalen Berichts zur Bewertung der Cybersicherheitsrisiken

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu informieren: HIE, CIE

37.2 Absatz 2

ENTSO-E übermittelt der ACER in Zusammenarbeit mit der EU-VNBO innerhalb von sechs Monaten nach Annahme oder Aktualisierung des Berichts über die regionale Bewertung des Cybersicherheitsrisikos eine Zusammenfassung dieses Arbeitsprogramms.

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu informieren: ACER

37.3 Absatz 3

Die ÜNB bemühen sich mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sicherzustellen, dass die auf der Grundlage der einschlägigen regionalen Bewertung des Cybersicherheitsrisikos entwickelten unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe in allen Netzbetriebsregionen ähnlich oder vergleichbar sind. Die Empfehlungen für die Cybersicherheit bei der Auftragsvergabe müssen mindestens die in Artikel 33 Absatz 2 Buchstabe a genannten Spezifikationen umfassen. Soweit möglich, werden die Spezifikationen aus europäischen und internationalen Normen ausgewählt.

Relevante NCCS-Artikel

- Artikel 33 (2)

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

37.4 Absatz 4

Die ÜNB stellen mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sicher, dass die Empfehlungen für die Cybersicherheit bei der Auftragsvergabe

a. den Grundsätzen der Auftragsvergabe aus der Richtlinie 2014/24/EU entsprechen und

b. mit den neuesten verfügbaren europäischen Schemata für die Cybersicherheitszertifizierung, die für das IKT-Produkt, den IKT-Dienst oder den IKT-Prozess relevant sind, vereinbar sind und diesen Rechnung tragen.

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Chapter 38

Artikel 36. : Leitlinien für die Nutzung europäischer Schemata für die Cybersicherheitszertifizierung bei der Beschaffung von IKT-Produkten, -Diensten und -Prozessen

38.1 Absatz 1

Unbeschadet des Rahmens für die Schaffung europäischer Schemata für die Cybersicherheitszertifizierung gemäß Artikel 46 der Verordnung (EU) 2019/881 [a] können die gemäß Artikel 35 entwickelten unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe sektorspezifische Leitlinien für die Verwendung europäischer Schemata für die Cybersicherheitszertifizierung umfassen, wenn für eine von Einrichtungen mit kritischen Auswirkungen verwendete Art von IKT-Produkten, -Diensten oder -Prozessen ein geeignetes Schema zur Verfügung steht.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e3205-15-1

Relevante NCCS-Artikel

- Artikel 35

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

38.2 Absatz 2

Die ÜNB arbeiten mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO eng mit der ENISA zusammen, um die sektorspezifischen Leitlinien bereitzustellen, die in den unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe gemäß Absatz 1 enthalten sind.

Relevante NCCS-Artikel

- Artikel 36 (1)

Verantwortlich für die Aktivität: TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, ENISA, EU DSO

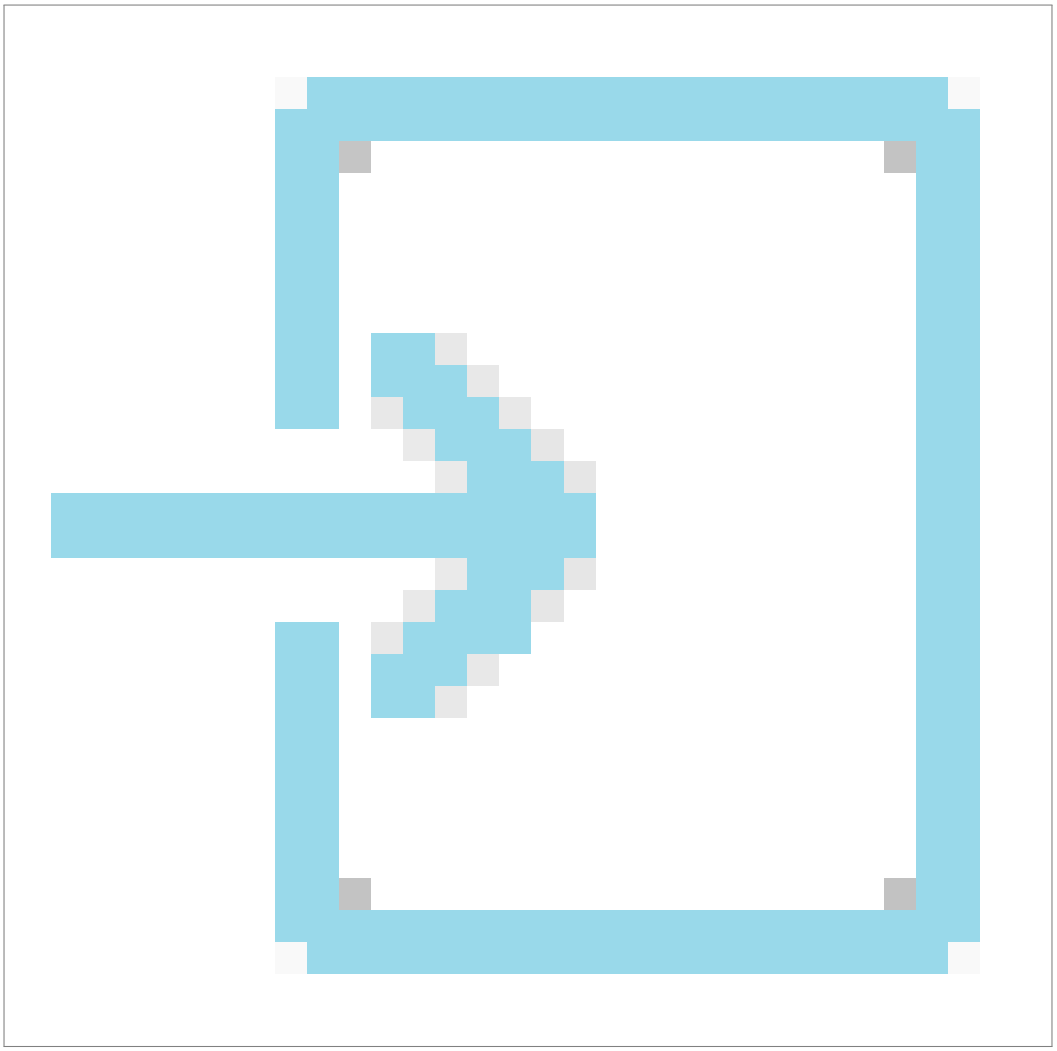
Chapter 39

Artikel 37. : Vorschriften für den Informationsaustausch

39.1 Absatz 1

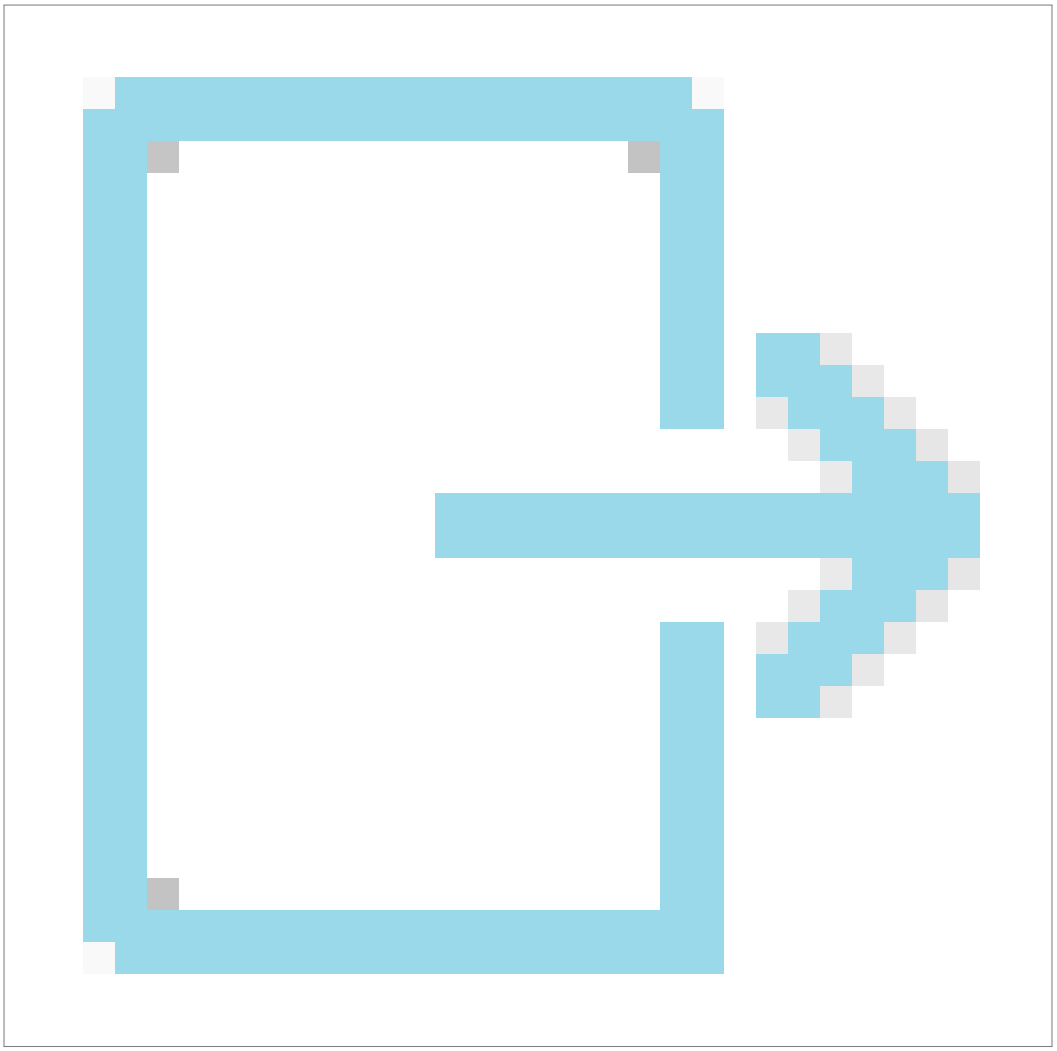
Erhält eine zuständige Behörde Informationen über einen meldepflichtigen Cyberangriff,

a. bewertet sie den Grad der Vertraulichkeit dieser Informationen und unterrichtet die Einrichtung unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Eingang der Informationen, über das Ergebnis ihrer Bewertung;



Input

- Klassifizierungsskala für Cyberangriffe
- Erkannter Cyberangriff



Output

- Bewertete Informationen zu Cyberangriffen

GOOD TO KNOW

Zeitpunkt

Spätestens 24 Stunden nach Bekanntgabe

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu informieren: HIE, CIE, ENISA, CSIRT, CS NCA

39.2 Absatz 1

b) versucht sie, andere ähnliche Cyberangriffe in der Union zu ermitteln, die anderen zuständigen Behörden gemeldet wurden, um die zu dem meldepflichtigen Cyberangriff eingegangenen Informationen mit Informationen zu vergleichen, die zu anderen Cyberangriffen bereitgestellt wurden, und um vorhandene Informationen zu ergänzen sowie die Reaktion im Bereich der Cybersicherheit zu stärken und zu koordinieren;

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

39.3 Absatz 1

c) ist sie für die Entfernung von Geschäftsgeheimnissen und die Anonymisierung der Informationen im Einklang mit den einschlägigen nationalen Vorschriften und Unionsvorschriften verantwortlich;

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

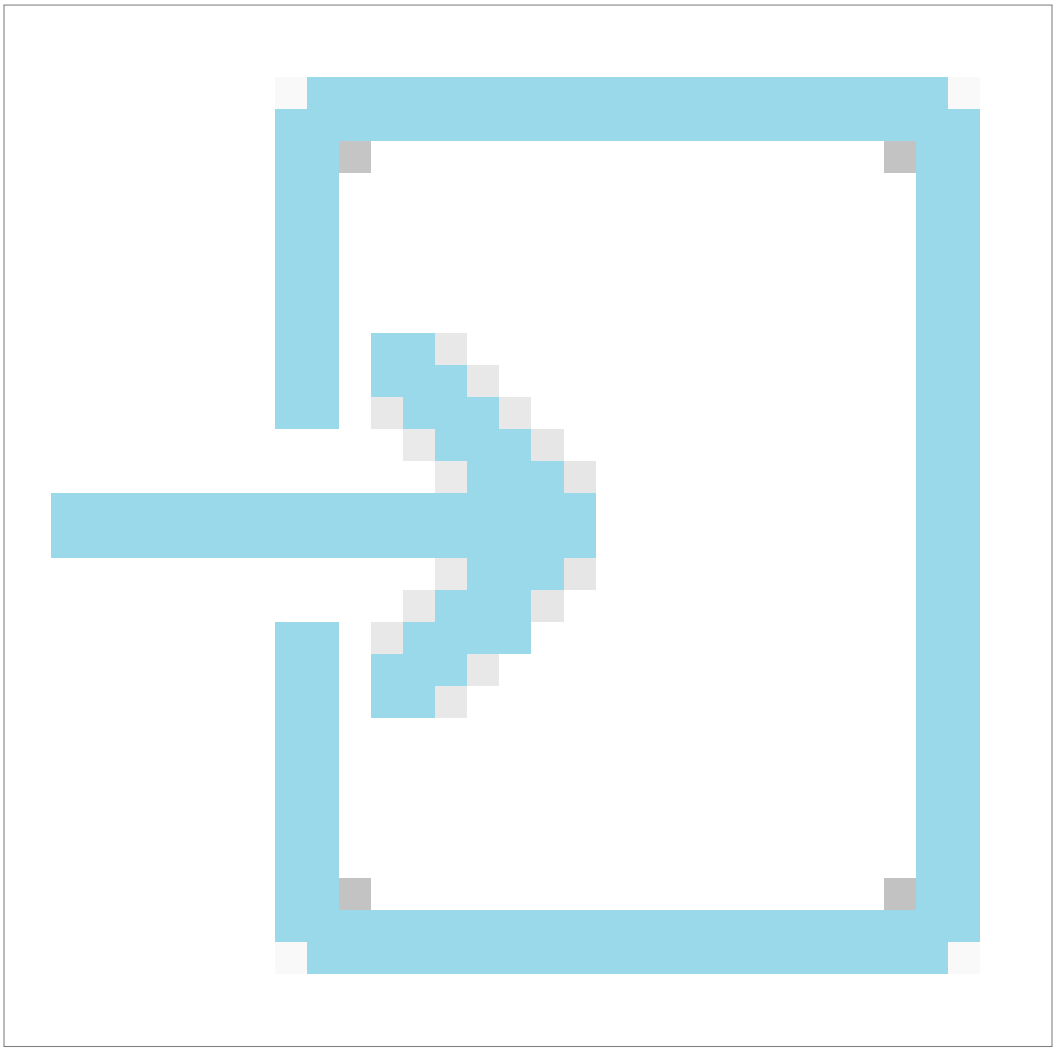
Beteiligt an der Aufgabenausführung: NCA

39.4 Absatz 1

d) übermittelt sie die Informationen unverzüglich, spätestens jedoch 24 Stunden nach Eingang der Informationen über einen meldepflichtigen Cyberangriff, den nationalen zentralen Anlaufstellen, den CSIRTs und allen gemäß Artikel 4 benannten zuständigen Behörden anderer Mitgliedstaten und stellt diesen Behörden oder Stellen regelmäßig aktualisierte Informationen zur Verfügung;

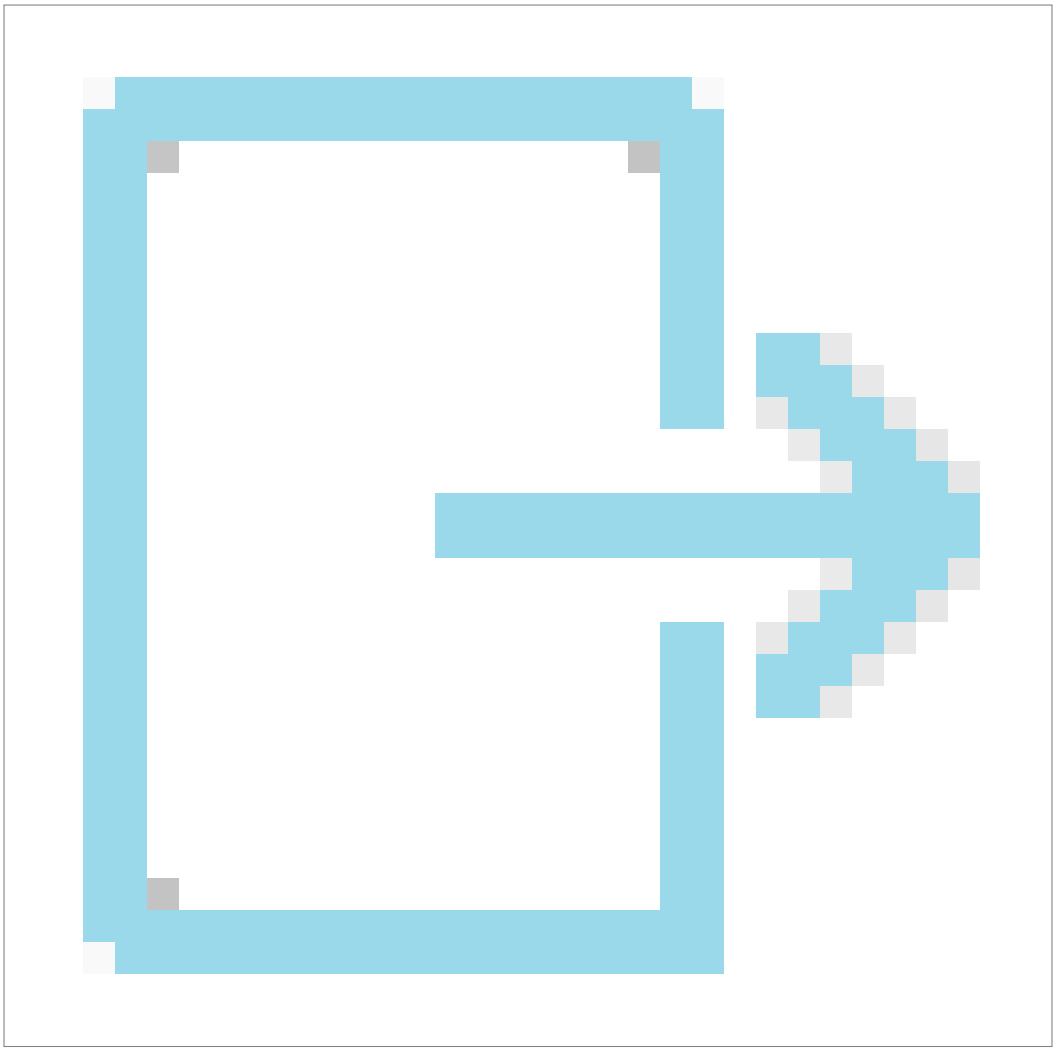
Relevante NCCS-Artikel

- Artikel 4



Input

- Bewertete Informationen zu Cyberangriffen



Output

- Informationsaustausch zu Cyberangriffen

GOOD TO KNOW

Zeitpunkt

Spätestens 24 Stunden nach Bekanntgabe

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

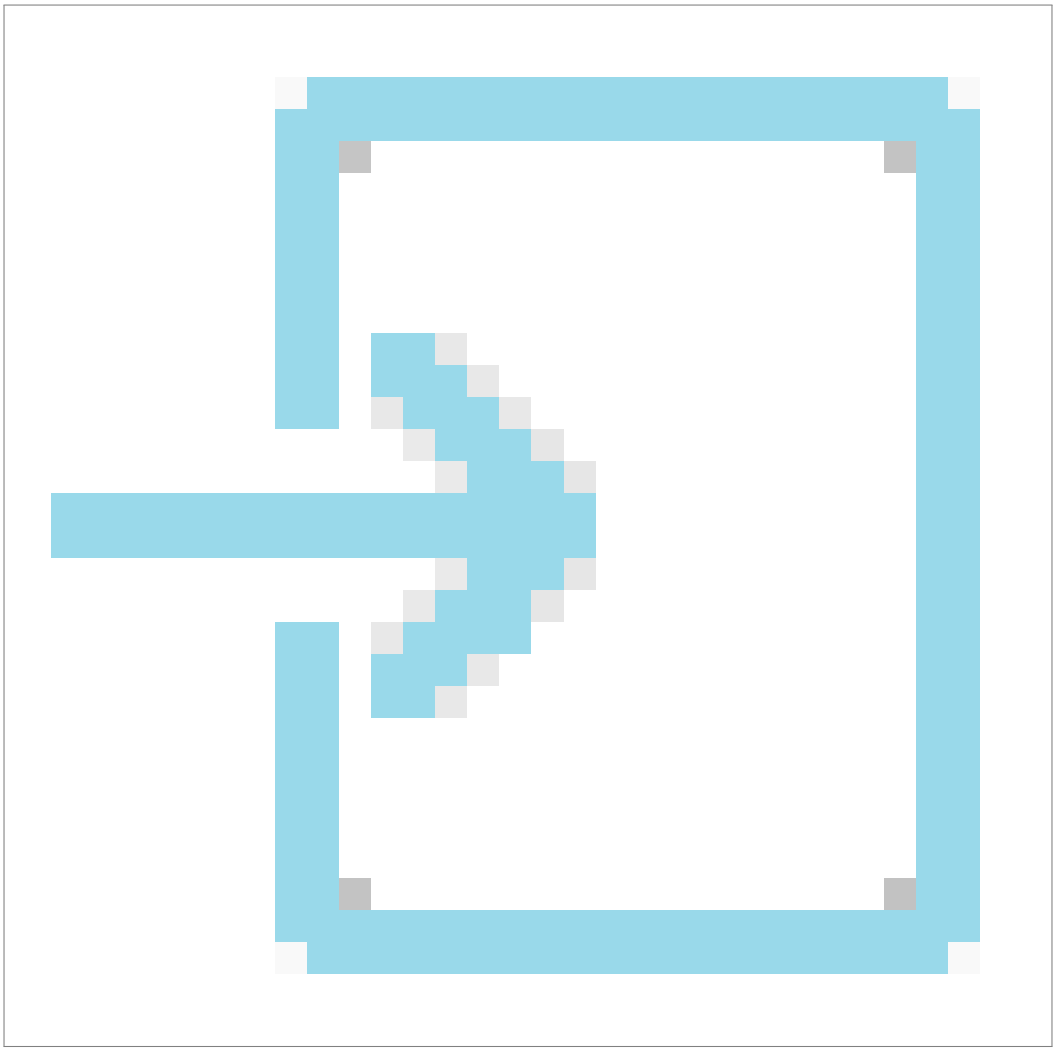
Beteiligt an der Aufgabenausführung: NCA

39.5 Absatz 1

e) übermittelt sie die Informationen über den Cyberangriff nach Anonymisierung und Entfernung von Geschäftsgeheimnissen gemäß Absatz 1 Buchstabe c unverzüglich, spätestens jedoch 24 Stunden nach Eingang der Informationen gemäß Absatz 1 Buchstabe a, den Einrichtungen mit kritischen oder erheblichen Auswirkungen in ihrem Mitgliedstaat und stellt regelmäßig aktualisierte Informationen bereit, um den Einrichtungen einen wirksamen Schutz zu ermöglichen;

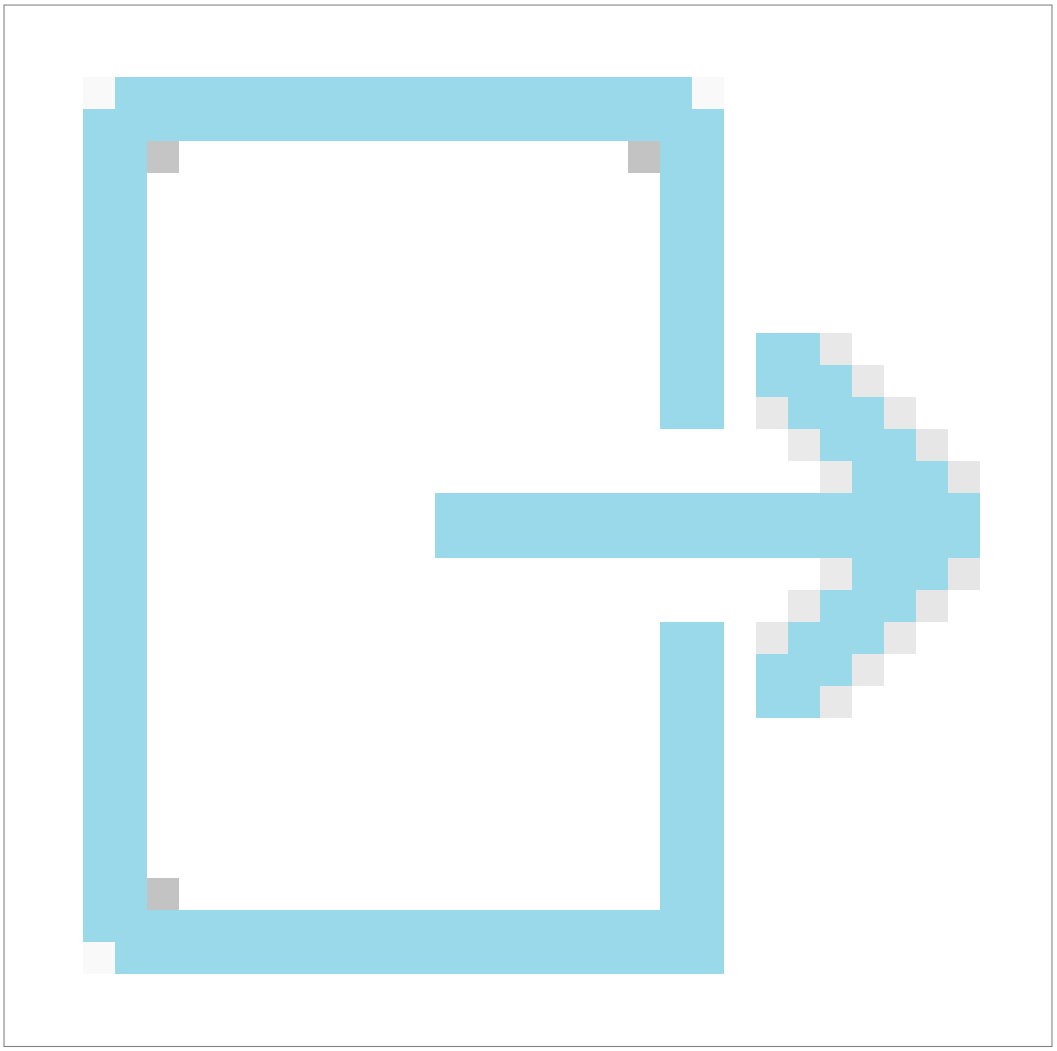
Relevante NCCS-Artikel

- Artikel 37 (1)



Input

- Bewertete Informationen zu Cyberangriffen



Output

- Informationsaustausch zu Cyberangriffen

GOOD TO KNOW

Zeitpunkt

Spätestens 24 Stunden nach Bekanntgabe

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu informieren: HIE, CIE

39.6 Absatz 1

f) kann sie die meldende Einrichtung mit erheblichen oder kritischen Auswirkungen auffordern, die meldepflichtigen Informationen über Cyberangriffe auf sichere Weise an andere möglicherweise betroffene Einrichtungen weiterzuleiten, um den Elektrizitätssektor für die Lage zu sensibilisieren und zu verhindern, dass ein Risiko eintritt, das dort zu einem grenzüberschreitenden Cybersicherheitsvorfall eskalieren könnte;

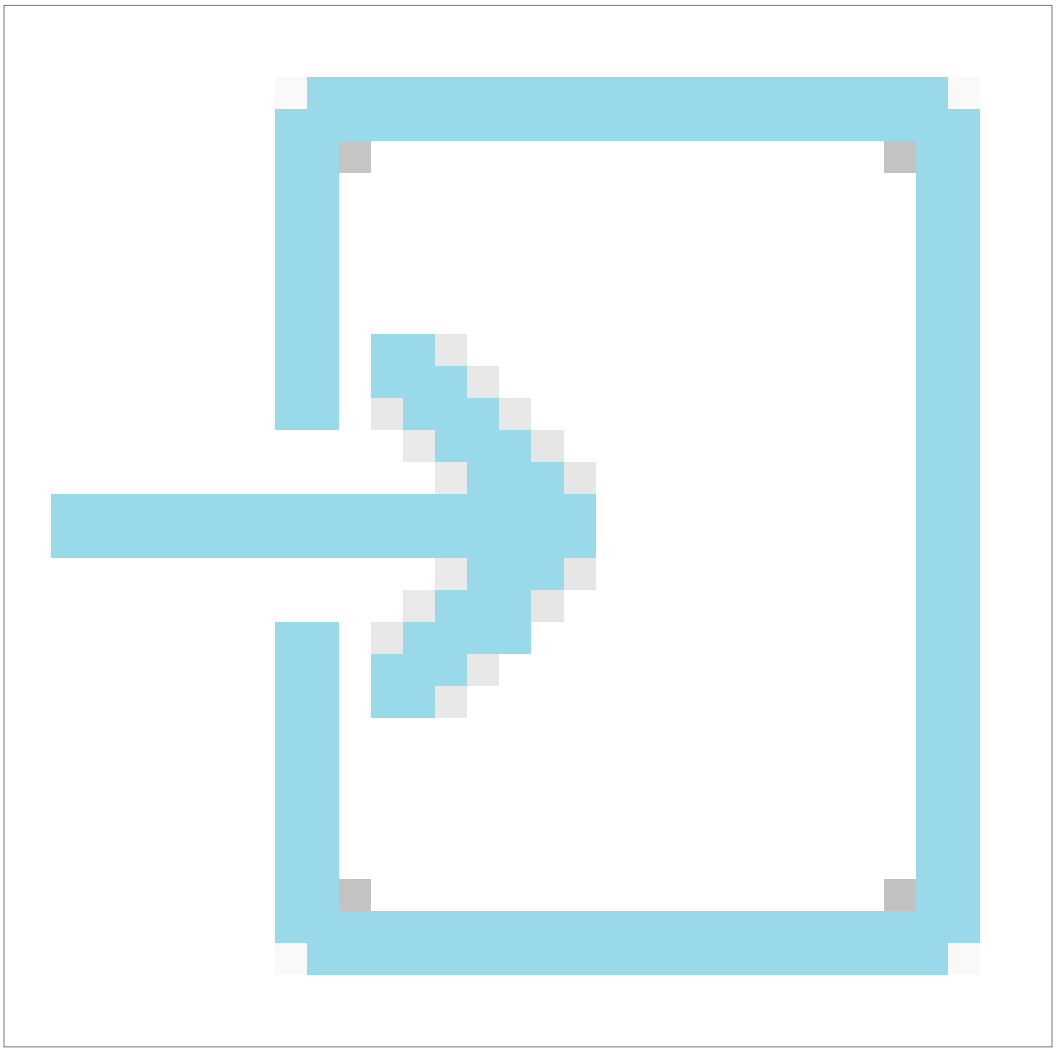
Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA

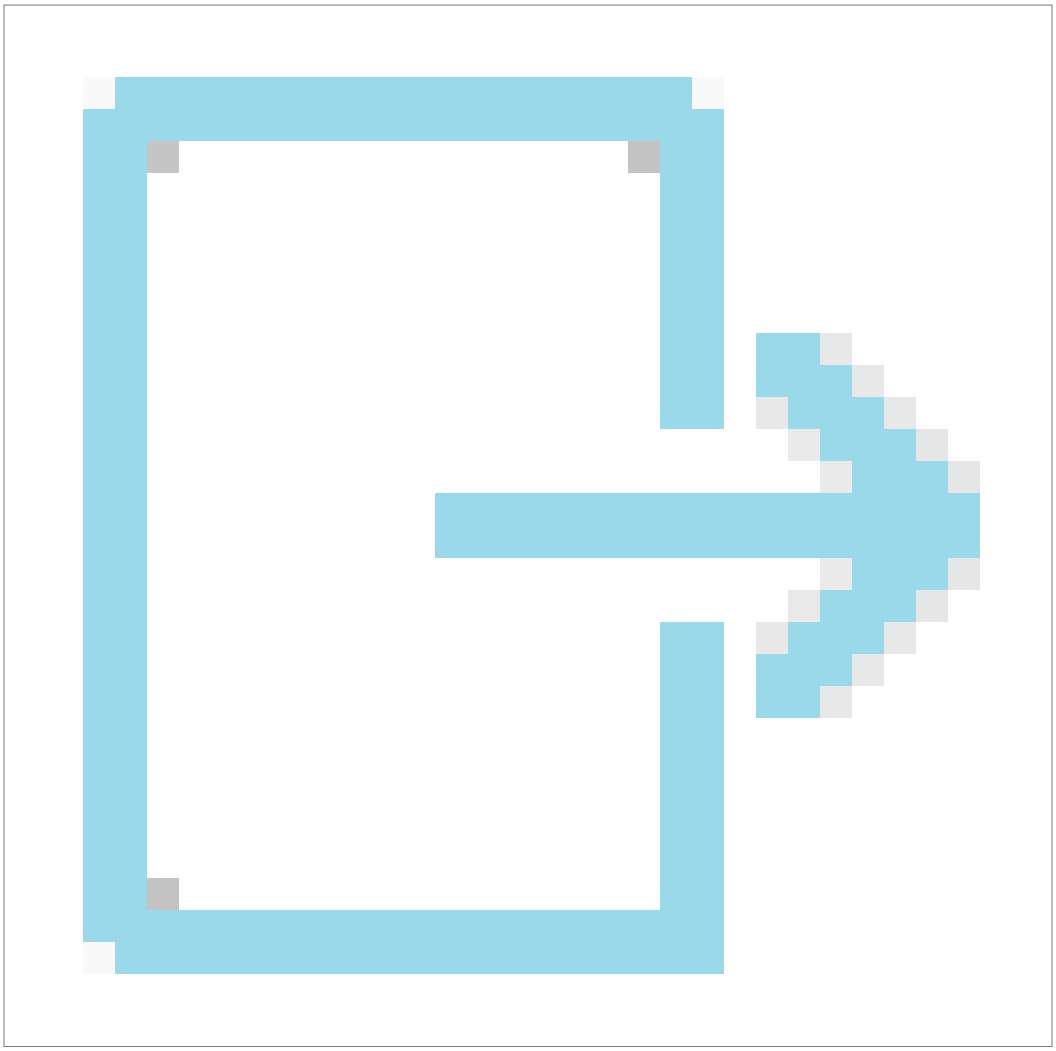
39.7 Absatz 1

g) übermittelt sie der ENISA nach Anonymisierung und Entfernung von Geschäftsgeheimnissen einen zusammenfassenden Bericht mit den Informationen zu dem Cyberangriff.



Input

- Bewertete Informationen zu Cyberangriffen



Output

- Informationsaustausch zu Cyberangriffen

A

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: NCA

Zu informieren: ENISA

39.8 Absatz 2

Erhält ein CSIRT Kenntnis von einer aktiv ausgenutzten Schwachstelle ohne Patch, so

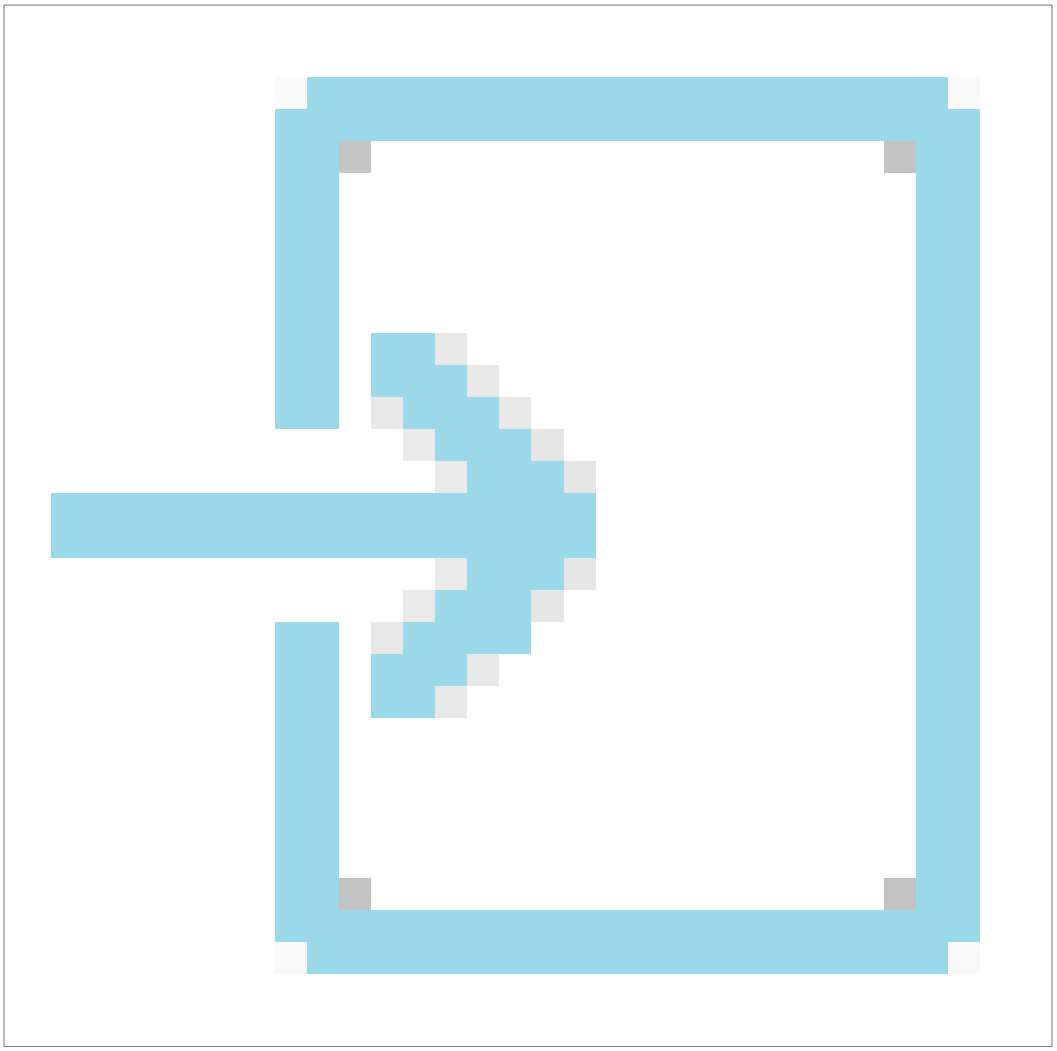
a. teilt es diese der ENISA unverzüglich über einen geeigneten Kanal für den sicheren Informationsaustausch mit, sofern in anderen Rechtsvorschriften der Union nichts anderes bestimmt ist;

b. unterstützt es die betroffene Einrichtung dabei, vom Hersteller oder Anbieter eine wirksame, koordinierte und rasche Behandlung der aktiv ausgenutzten Schwachstelle ohne Patch oder wirksame und effiziente Abhilfemaßnahmen zu erhalten;

c. tauscht es die verfügbaren Informationen mit dem Verkäufer aus und fordert den Hersteller oder Anbieter auf, möglichst eine Liste der CSIRTs in den Mitgliedstaaten vorzulegen, die von der aktiv ausgenutzten Schwachstelle ohne Patch betroffen sind und informiert werden müssen;

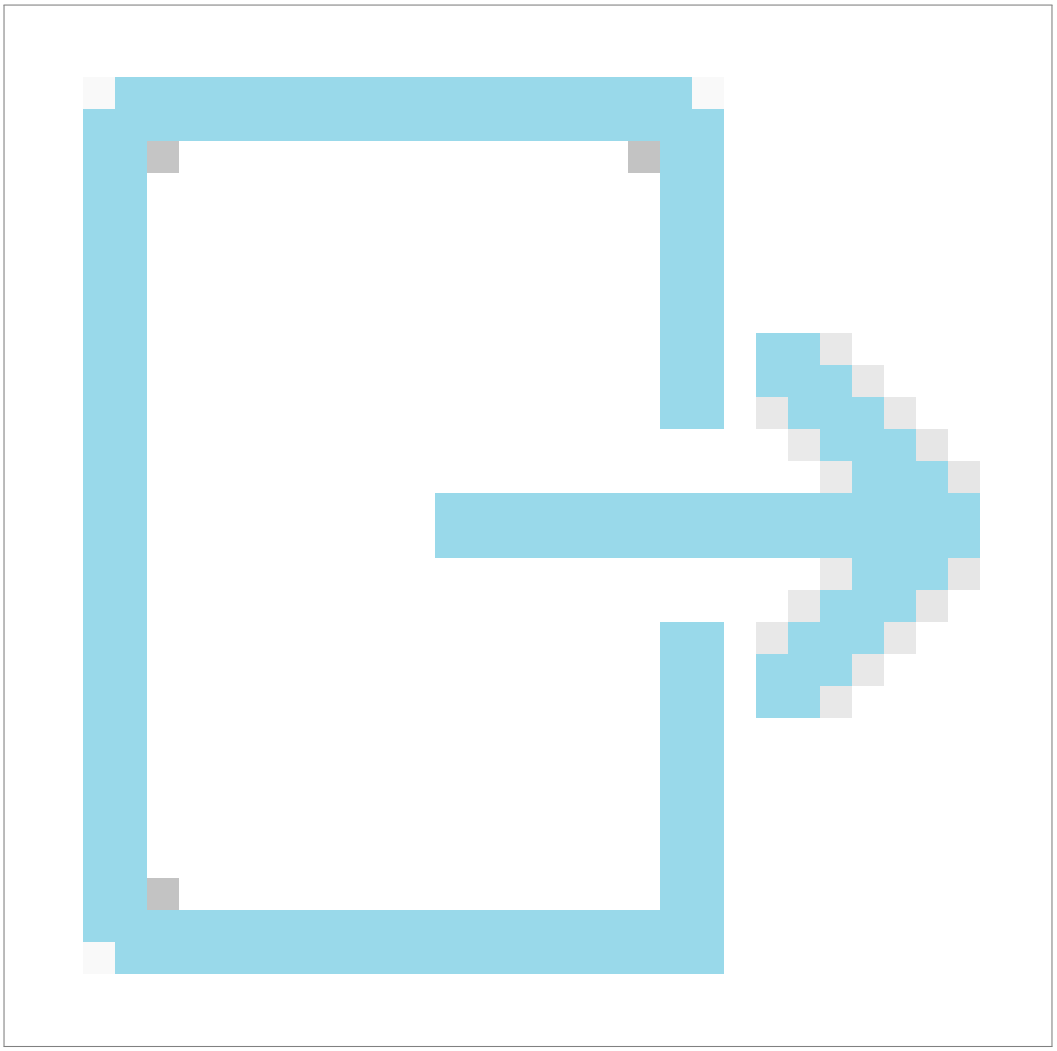
d. tauscht es verfügbare Informationen nach dem Grundsatz „Kenntnis nur, wenn nötig“ mit den unter obigem Buchstaben genannten CSIRTs aus;

e. stellt es Informationen über etwaige vorhandene Abhilfestrategien und -maßnahmen in Bezug auf die aktiv ausgenutzte Schwachstelle ohne Patch bereit.



Input

- Erkannte, ungepatchte und aktiv ausgenutzte Schwachstelle



Output

- Austausch von Informationen zu ungepatchten und derzeit aktiv ausgenutzten Schwachstellen

GOOD TO KNOW

Zeitpunkt

Sofort

Verantwortlich für die Aktivität: CSIRT

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CSIRT

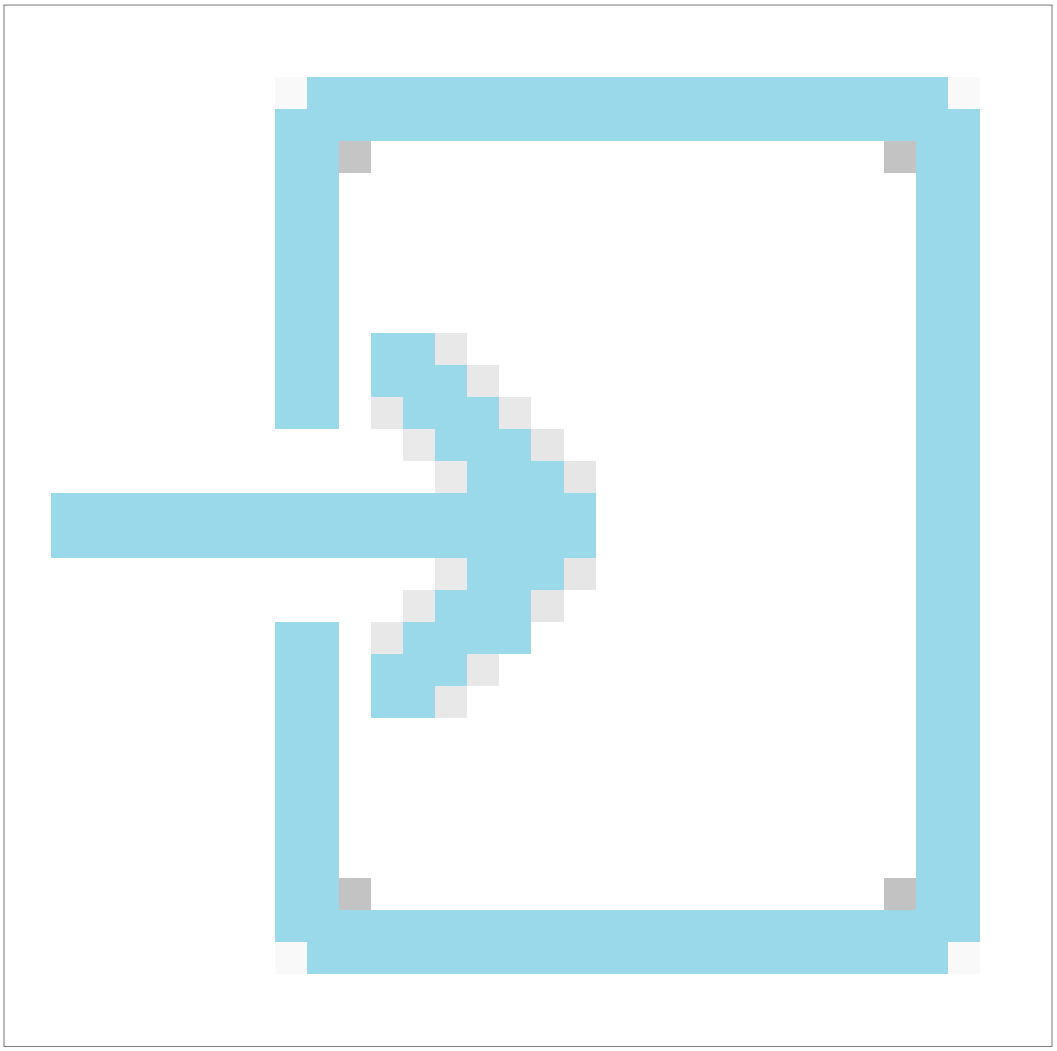
Zu informieren: HIE, CIE, ENISA, Critical ICT

39.9 Absatz 3

Erhält eine zuständige Behörde Kenntnis von einer aktiv ausgenutzten Schwachstelle ohne Patch, so

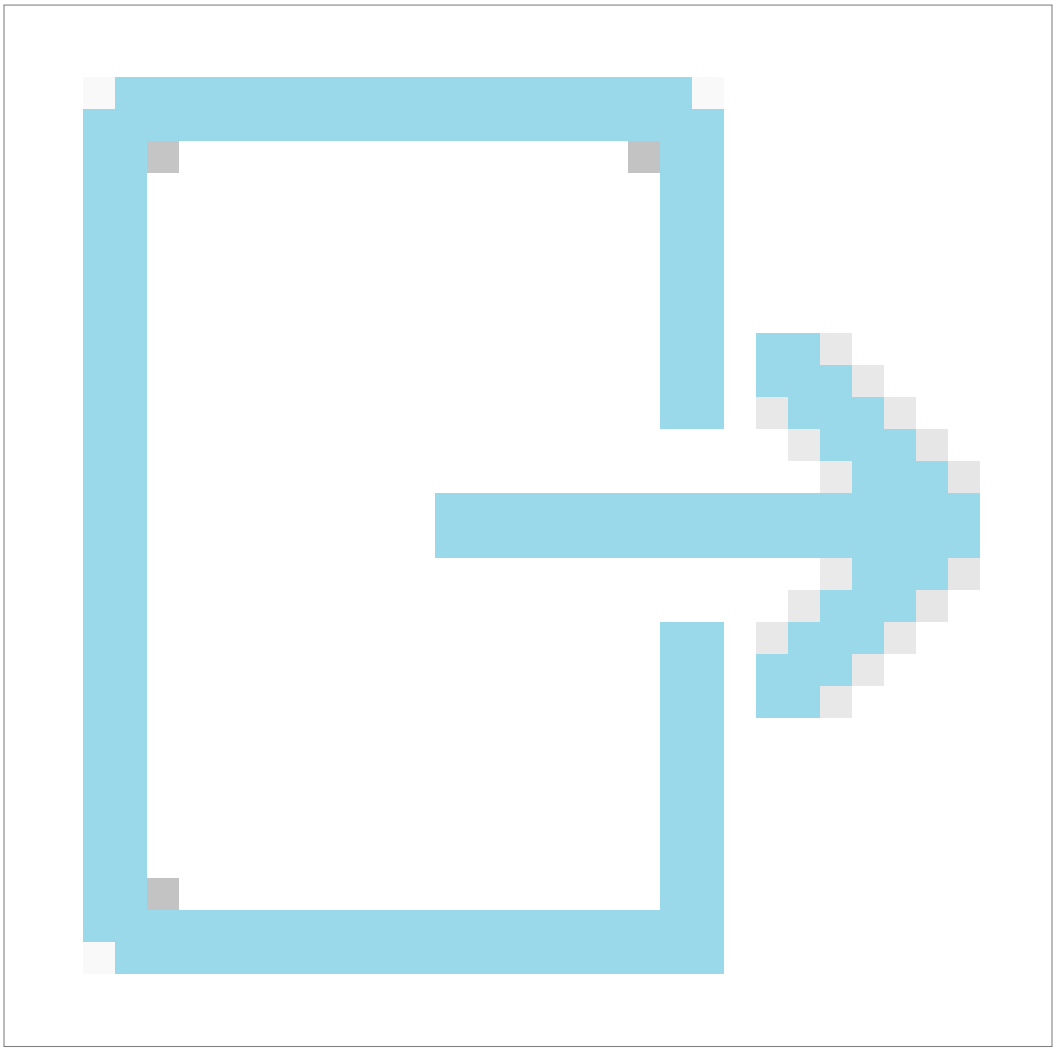
a. informiert sie in Abstimmung mit den CSIRTs in ihrem Mitgliedstaat über etwaige vorhandene Abhilfestrategien und -maßnahmen in Bezug auf die aktiv ausgenutzte Schwachstelle ohne Patch;

b. übermittelt sie die Informationen an ein CSIRT in dem Mitgliedstaat, in dem die aktiv ausgenutzte Schwachstelle ohne Patch gemeldet wurde.



Input

- Erkannte, ungepatchte und aktiv ausgenutzte Schwachstelle



Output

- Austausch von Informationen zu ungepatchten und derzeit aktiv ausgenutzten Schwachstellen

GOOD TO KNOW

Zeitpunkt

Sofort

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

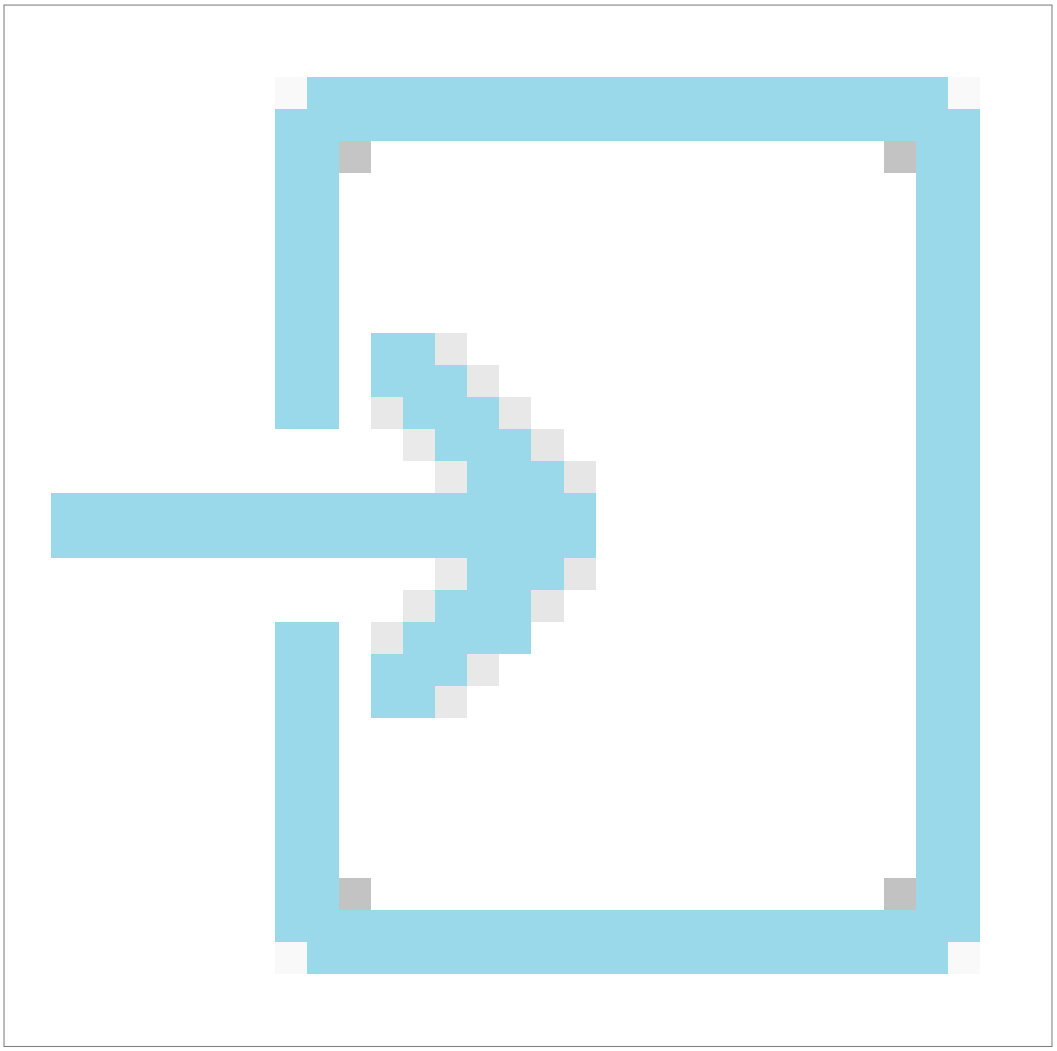
Beteiligt an der Aufgabenausführung: NCA

Zu informieren: CSIRT

39.10 Absatz 4

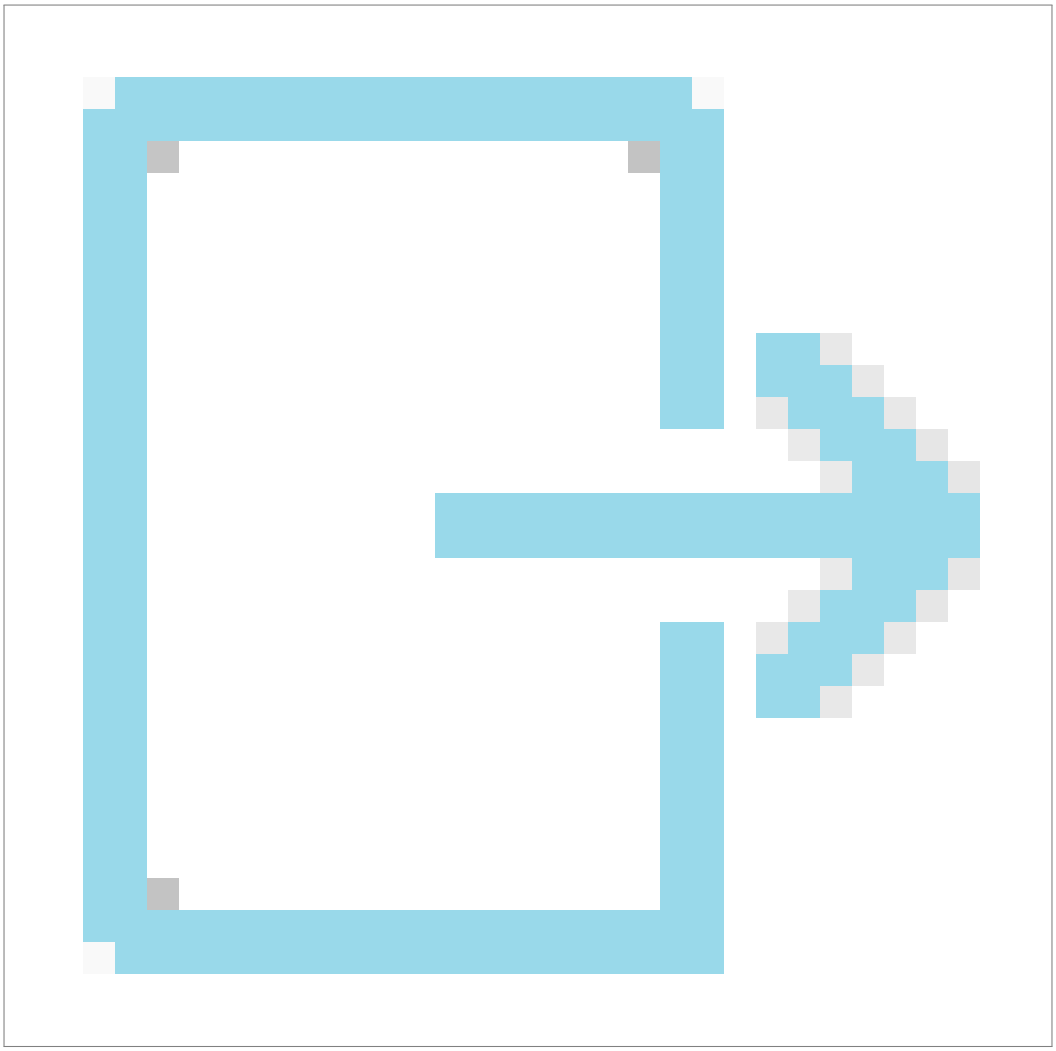
Erhält die zuständige Behörde Kenntnis von einer Schwachstelle ohne Patch, in Bezug auf die keine Beweise für eine aktive Ausnutzung vorliegen, stimmt sie sich unverzüglich mit dem CSIRT im Hinblick auf eine koordinierte Offenlegung von Schwachstellen gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 [a] ab.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_12



Input

- Erkannte, ungepatchte und aktiv ausgenutzte Schwachstelle



Output

- Austausch von Informationen zu ungepatchten und derzeit aktiv ausgenutzten Schwachstellen

GOOD TO KNOW

Zeitpunkt

sofort

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

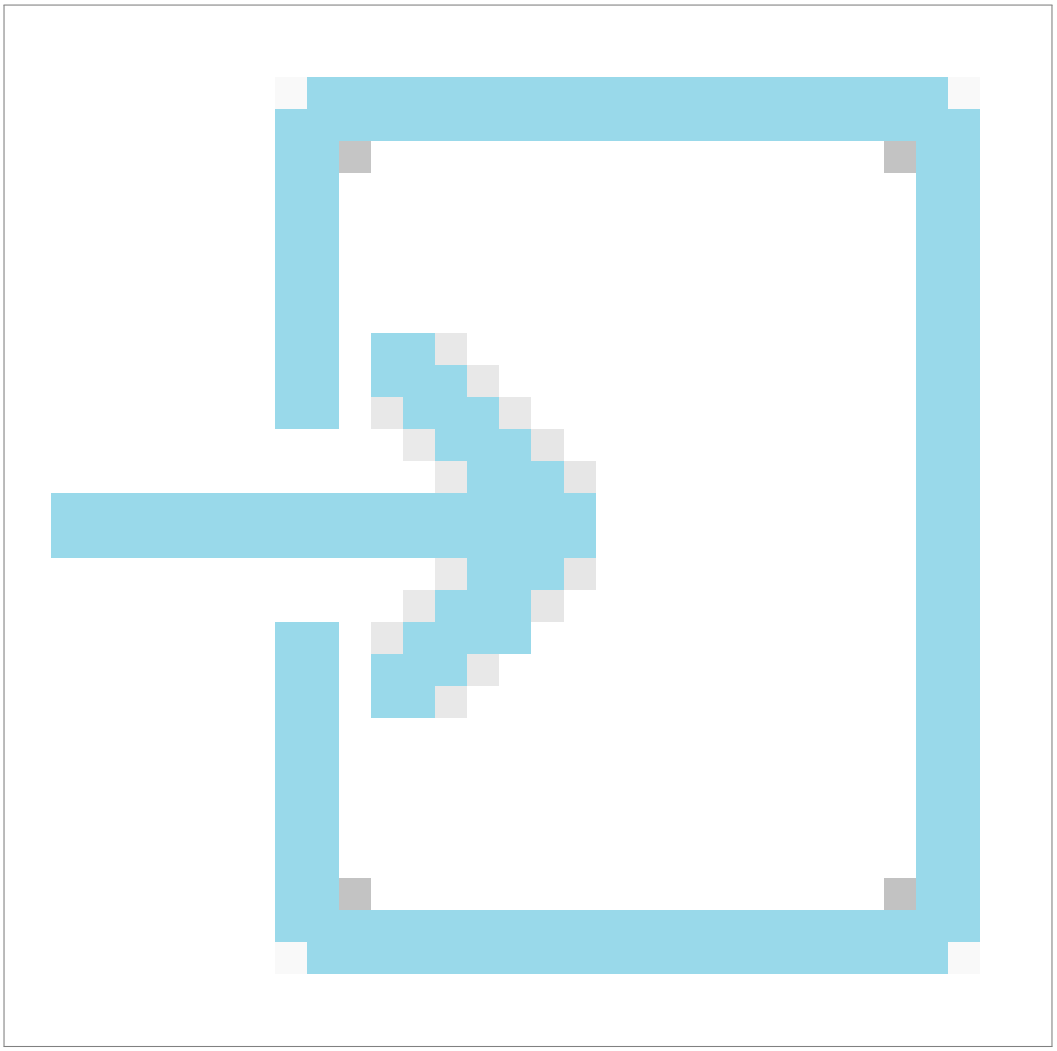
Zu informieren: CSIRT

39.11 Absatz 5

Erhält ein CSIRT gemäß Artikel 38 Absatz 6 von einer oder mehreren Einrichtungen mit erheblichen oder kritischen Auswirkungen Informationen in Bezug auf Cyberbedrohungen, so leitet es diese oder andere Informationen, die für die Verhütung, Erkennung, Behandlung oder Minderung des damit verbundenen Risikos von Bedeutung sind, an die Einrichtungen mit kritischen oder erheblichen Auswirkungen in seinem Mitgliedstaat und gegebenenfalls an alle betroffenen CSIRTs und seine nationale zentralen Anlaufstelle unverzüglich, spätestens jedoch vier Stunden nach Eingang der Informationen, weiter.

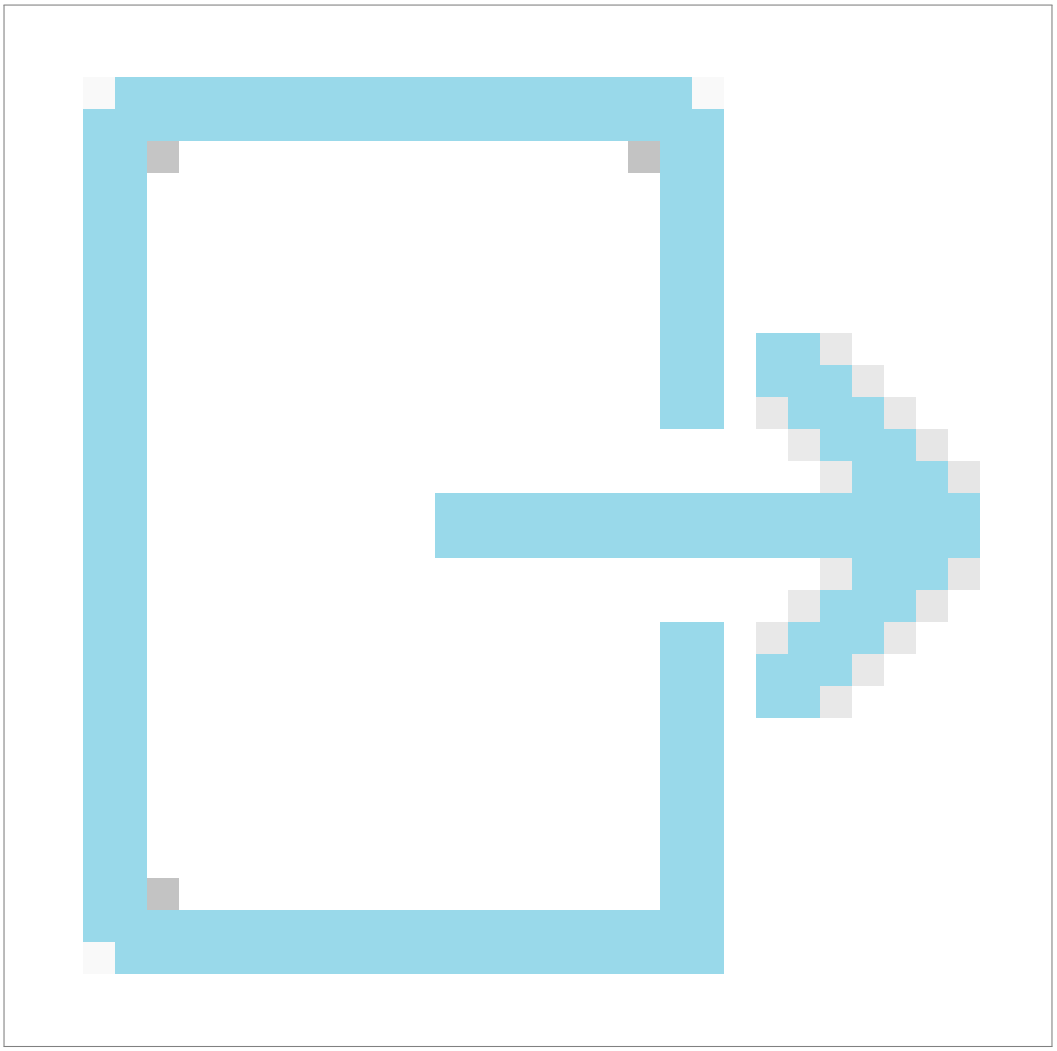
Relevante NCCS-Artikel

- Artikel 38 (6)



Input

- Klassifizierungsskala für Cyberangriffe
- Erkannter Cyberangriff



Output

- Informationsaustausch zu Cyberangriffen

> GOOD TO KNOW
>
> **Zeitpunkt**
>
> Innerhalb von 4 Stunden nach einem Cyberangriff

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

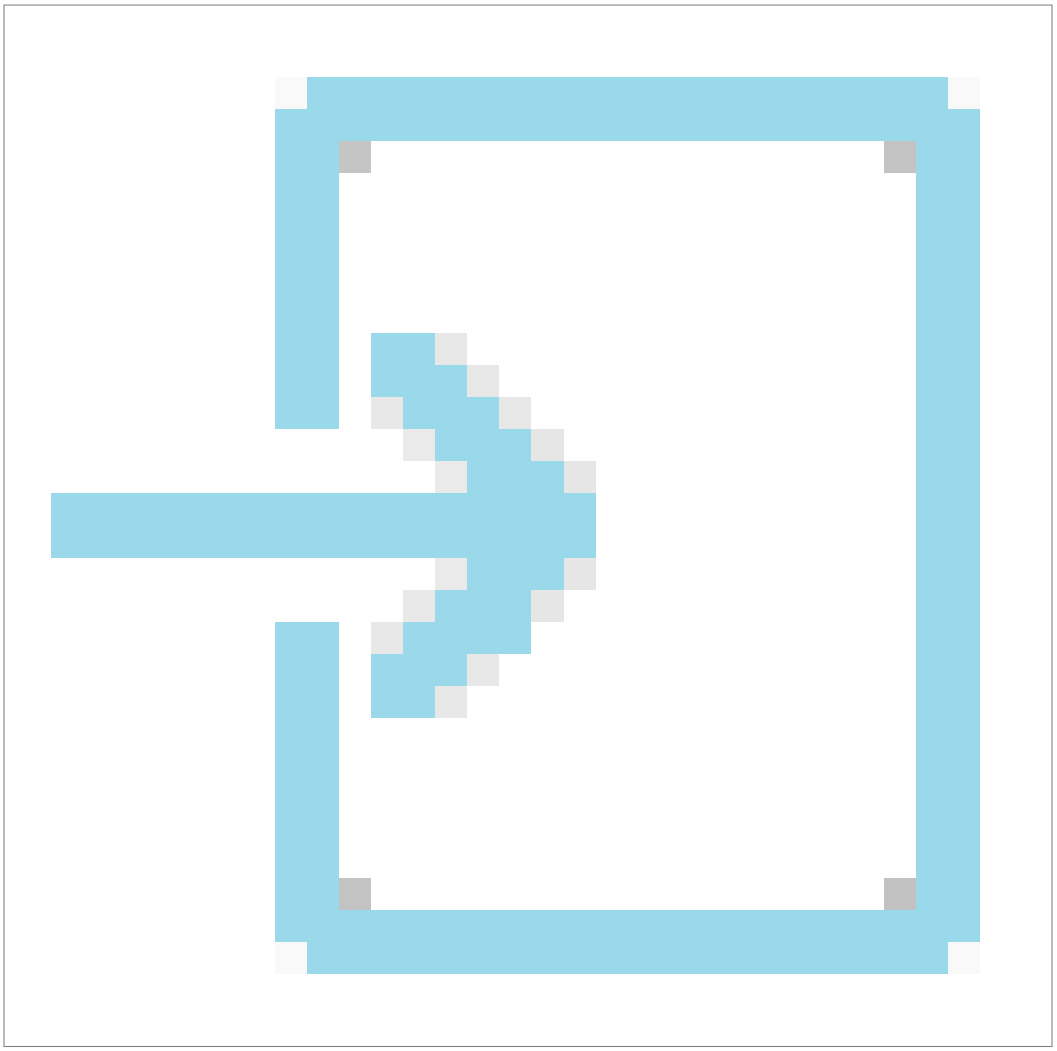
Zu konsultieren: CSIRT

39.12 Absatz 6

Erhält eine zuständige Behörde von einer oder mehreren Einrichtungen mit erheblichen oder kritischen Auswirkungen Informationen über Cyberbedrohungen, so leitet sie diese Informationen für die Zwecke des Absatzes 5 an das CSIRT weiter.

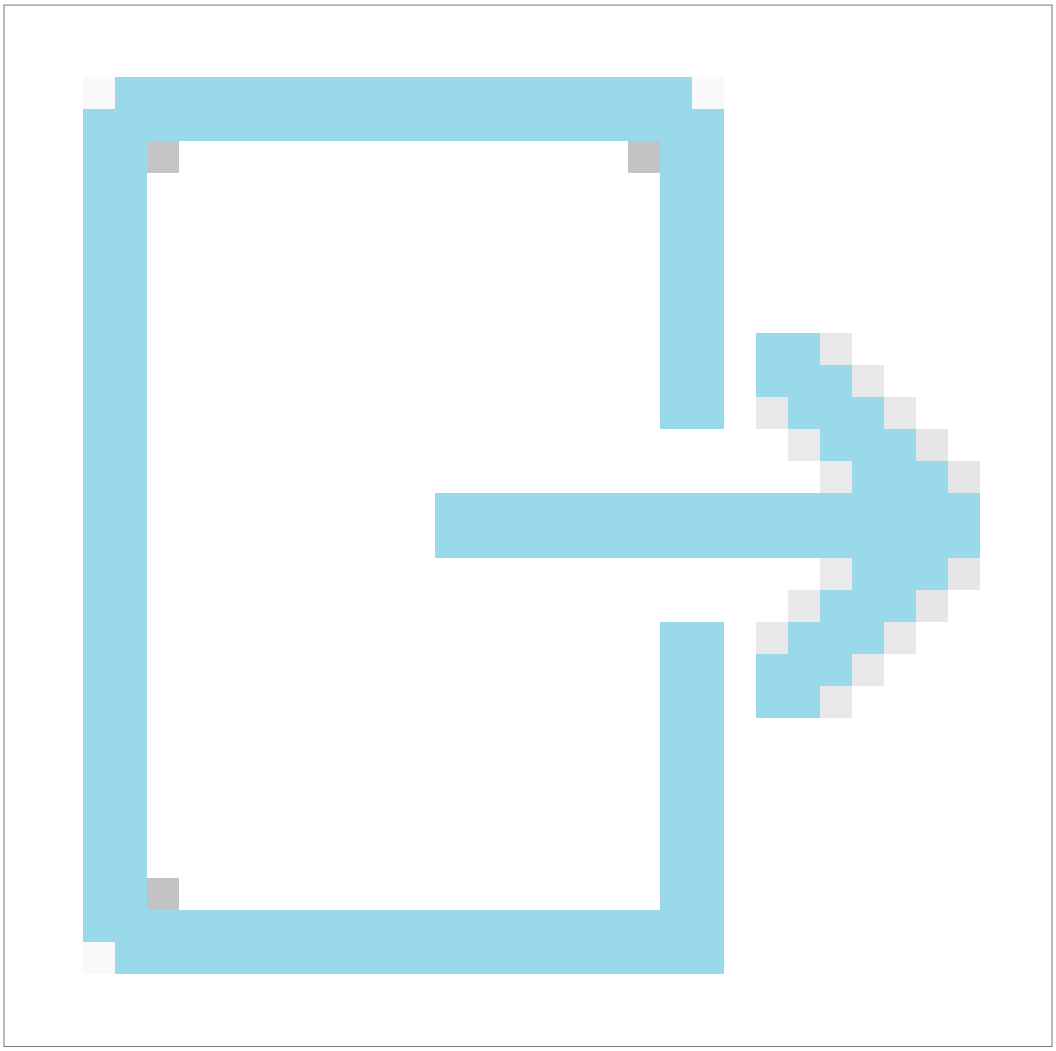
Relevante NCCS-Artikel

- Artikel 37 (5)



Input

- Klassifizierungsskala für Cyberangriffe
- Erkannter Cyberangriff



Output

- Informationsaustausch zu Cyberangriffen

A

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: NCA

Zu informieren: CSIRT

39.13 Absatz 7

Die zuständigen Behörden können die Zuständigkeiten nach den Absätzen 3 und 4 in Bezug auf eine oder mehrere Einrichtungen mit erheblichen oder kritischen Auswirkungen, die in mehr als einem Mitgliedstaat tätig sind, ganz oder teilweise an eine andere zuständige Behörde in einem dieser Mitgliedstaaten delegieren, sofern sich die betroffenen zuständigen Behörden darauf geeinigt haben.

Relevante NCCS-Artikel

- Artikel 37 (3)
- Artikel 37 (4)

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

39.14 Absatz 8

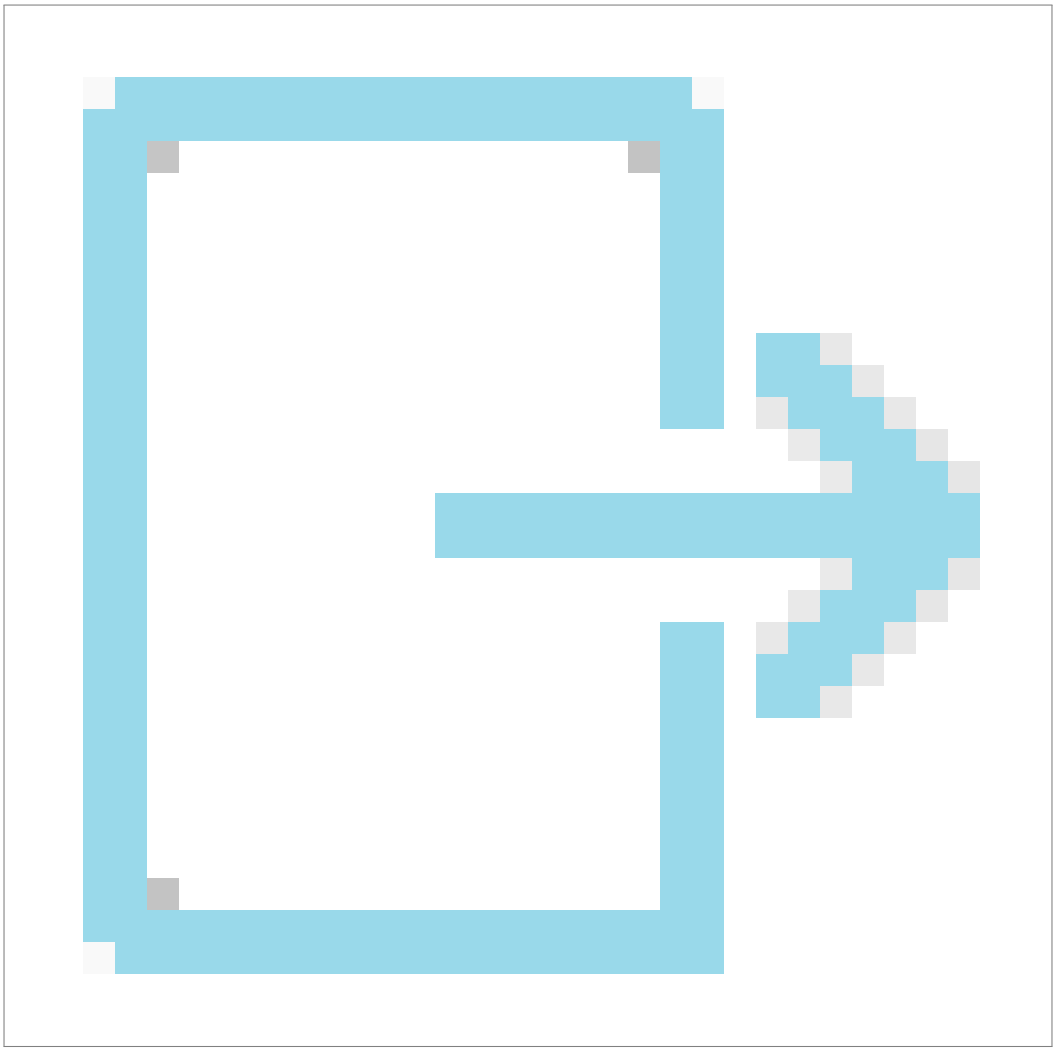
Die ÜNB entwickeln mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO bis zum 13 Juni 2025 eine Klassifizierungsmethode für Cyberangriffe. Die ÜNB können mit Unterstützung von ENTSO-E und der EU-VNBO die zuständigen Behörden ersuchen, die ENISA und ihre für Cybersicherheit zuständigen Behörden zur Unterstützung bei der Entwicklung einer solchen Klassifizierungsskala zu konsultieren. Die Methode muss fünf Stufen für die Schwere eines Cyberangriffs enthalten, wobei „erheblich“ und „kritisch“ die höchsten Stufen darstellen. Die Klassifizierung muss sich auf die Bewertung der folgenden Parameter stützen:

a. die potenziellen Auswirkungen unter Berücksichtigung der gemäß Artikel 26 Absatz 4 Buchstabe c ermittelten exponierten Vermögenswerte und Perimeter und

b. die Schwere des Cyberangriffs.

Relevante NCCS-Artikel

- Artikel 26 (4)



Output

- Klassifizierungsskala für Cyberangriffe

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Juni 2025

Verantwortlich für die Aktivität: TSO

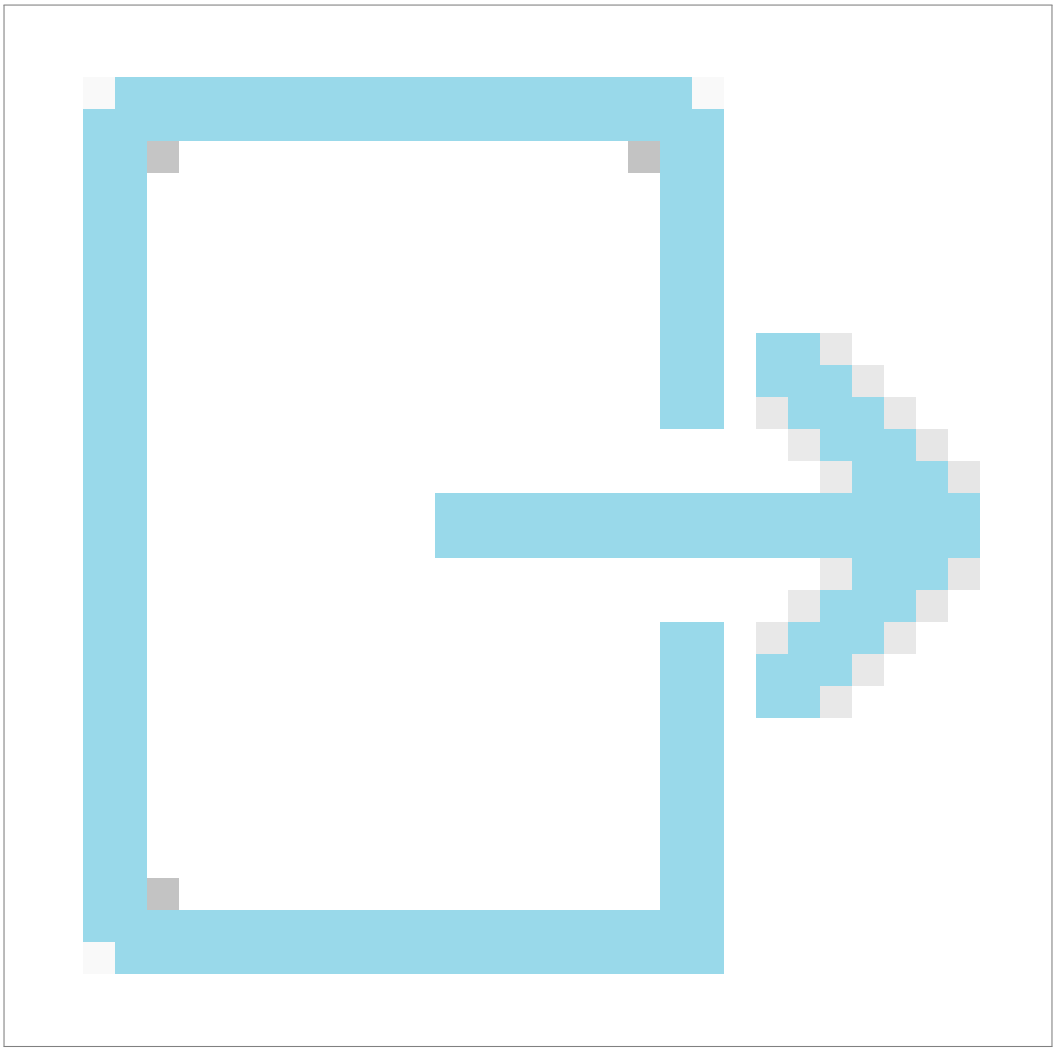
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, TSO, EU DSO

Zu konsultieren: ENISA

39.15 Absatz 9

Bis zum 13 Juni 2026 führt ENTSO-E in Zusammenarbeit mit der EU-VNBO eine Machbarkeitsstudie hinsichtlich der Möglichkeit durch, ein gemeinsames Instrument zu entwickeln, das es allen Einrichtungen ermöglicht, Informationen mit den zuständigen nationalen Behörden auszutauschen, und prüft die damit verbundenen finanziellen Kosten.



Output

- Machbarkeitsstudie zu einem Tool für den Informationsaustausch

GOOD TO KNOW

Zeitpunkt

Bis zum Juni 2026

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

39.16 Absatz 10

In der Machbarkeitsstudie wird die Möglichkeit geprüft, ein solches gemeinsames Instrument

a. zu nutzen, um Einrichtungen mit kritischen oder erheblichen Auswirkungen durch einschlägige sicherheitsrelevante Informationen für den Betrieb grenzüberschreitender Stromflüsse zu unterstützen, z. B. durch echtzeitnahe Berichterstattung über Cyberangriffe, Frühwarnungen im Zusammenhang mit Cybersicherheitsfragen und nicht offengelegten Schwachstellen von Geräten, die im Elektrizitätssystem eingesetzt werden;

b. in einem geeigneten und äußerst vertrauenswürdigen Umfeld zu pflegen;

c. zu nutzen, um Daten bei Einrichtungen mit kritischen oder erheblichen Auswirkungen zu erheben und die Entfernung vertraulicher Informationen und die Anonymisierung der Daten zu unterstützen und diese unverzüglich an Einrichtungen mit kritischen oder erheblichen Auswirkungen weiterzuleiten.

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

39.17 Absatz 11

In Zusammenarbeit mit der EU-VNBO

a. konsultiert ENTSO-E bei der Machbarkeitsstudie die ENISA und die NIS-Kooperationsgruppe, die nationalen zentralen Anlaufstellen und die Vertreter der wichtigsten Interessenträger;

b. legt ENTSO-E die Ergebnisse der Machbarkeitsstudie der ACER und der NIS-Kooperationsgruppe vor.

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu konsultieren: ENISA, NCA, NIS CG

Zu informieren: ACER

39.18 Absatz 12

ENTSO-E kann in Zusammenarbeit mit der EU-VNBO Initiativen analysieren und unterstützen, die von Einrichtungen mit kritischen oder erheblichen Auswirkungen vorgeschlagen werden, um solche Instrumente für den Informationsaustausch zu bewerten und zu testen.

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Chapter 40

Artikel 38. : Aufgaben von Einrichtungen mit erheblichen oder kritischen Auswirkungen beim Informationsaustausch

40.1 Absatz 1

Jede Einrichtung mit erheblichen oder kritischen Auswirkungen

a. richtet für alle Vermögenswerte innerhalb ihres gemäß Artikel 26 Absatz 4 Buchstabe c bestimmten Cybersicherheitsperimeters mindestens die CSOC-Kapazitäten ein, um

   i. sicherzustellen, dass die einschlägigen Netz- und Informationssysteme und -anwendungen Sicherheitsprotokolle für die Sicherheitsüberwachung umfassen, damit Anomalien erkannt und Informationen über Cyberangriffe erhoben werden können;

   ii. die Sicherheitsüberwachung durchzuführen, einschließlich der Erkennung eines Eindringens und der Bewertung von Schwachstellen von Netz- und Informationssystemen;

   iii. zu analysieren und erforderlichenfalls im Rahmen ihrer Zuständigkeit und Kapazitäten alle für den Schutz der Einrichtung erforderlichen Maßnahmen zu ergreifen;

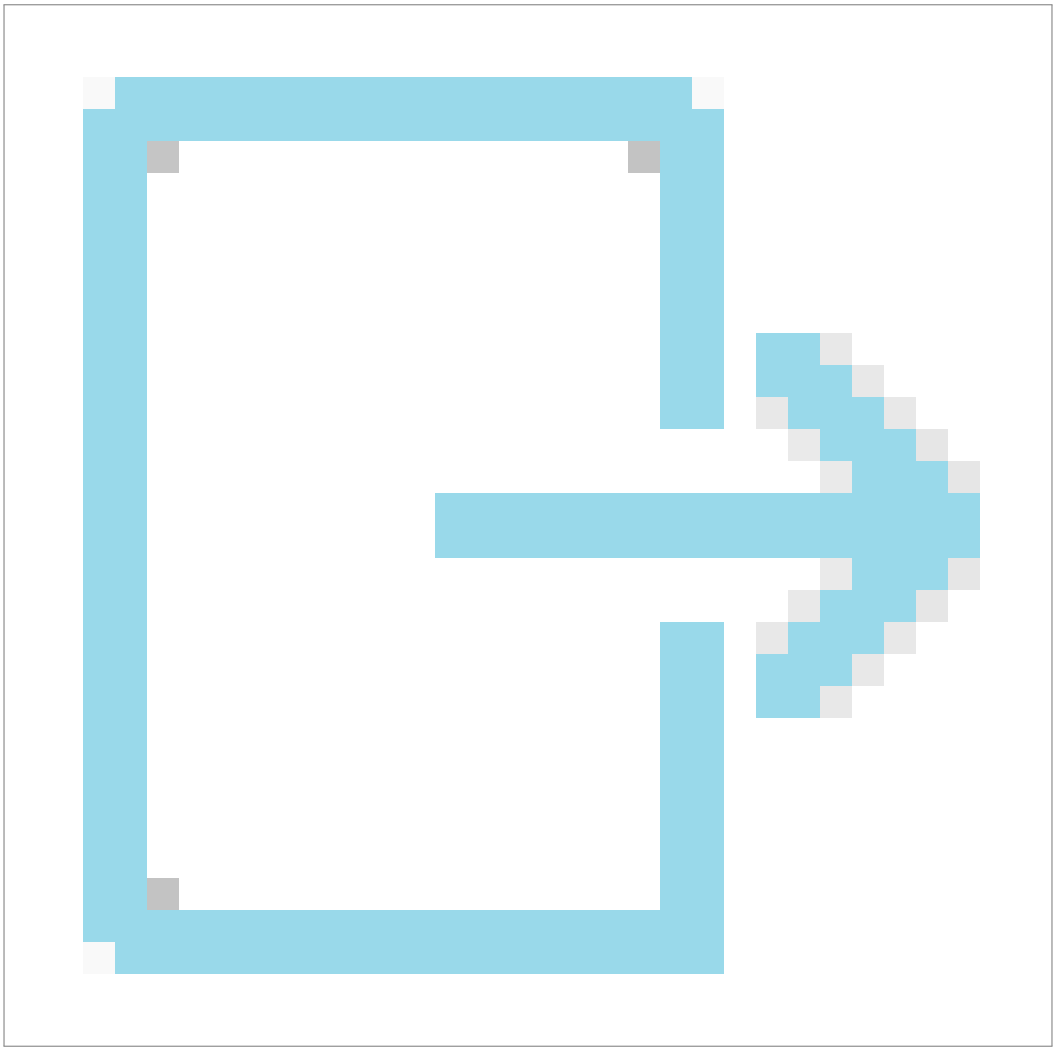
   iv. sich an der in diesem Artikel beschriebenen Erhebung und Weitergabe von Informationen zu beteiligen;

b. ist berechtigt, sich diese Kapazitäten gemäß Buchstabe a ganz oder teilweise über MSSP zu beschaffen. Einrichtungen mit kritischen oder erheblichen Auswirkungen bleiben für die MSSP verantwortlich und überwachen deren Bemühungen;

c. benennt für den Informationsaustausch eine zentrale Anlaufstelle auf Ebene der Einrichtung.

Relevante NCCS-Artikel

- Artikel 26 (4)



Output

- Etablierte CSOC-Fähigkeit

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

40.2 Absatz 2

Die ENISA kann im Rahmen der in Artikel 6 Absatz 2 der Verordnung (EU) 2019/881 [a] festgelegten Aufgabe unverbindliche Leitlinien für die Einrichtung solcher Kapazitäten oder die Vergabe von Unteraufträgen an MSSP für die Erbringung des Dienstes herausgeben.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

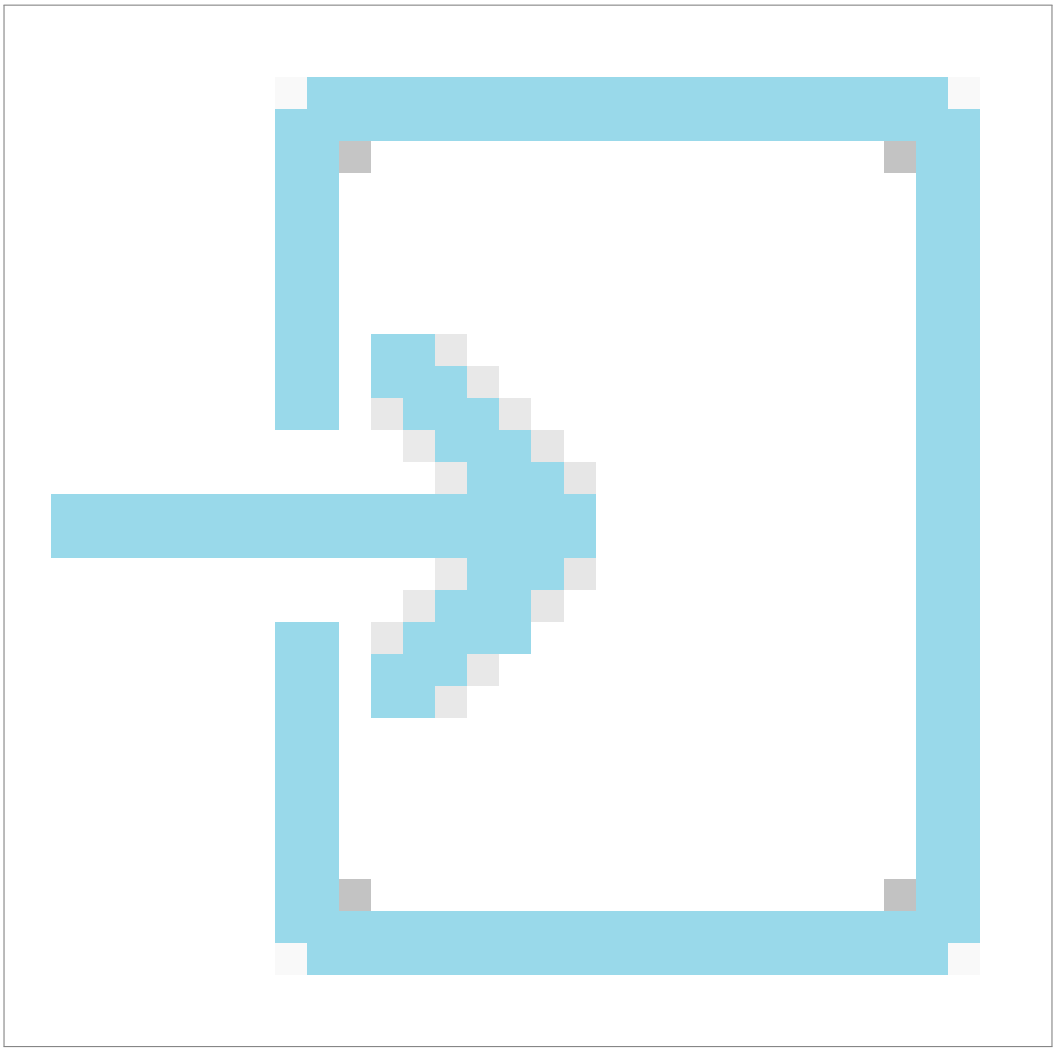
Verantwortlich für die Aktivität: ENISA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENISA

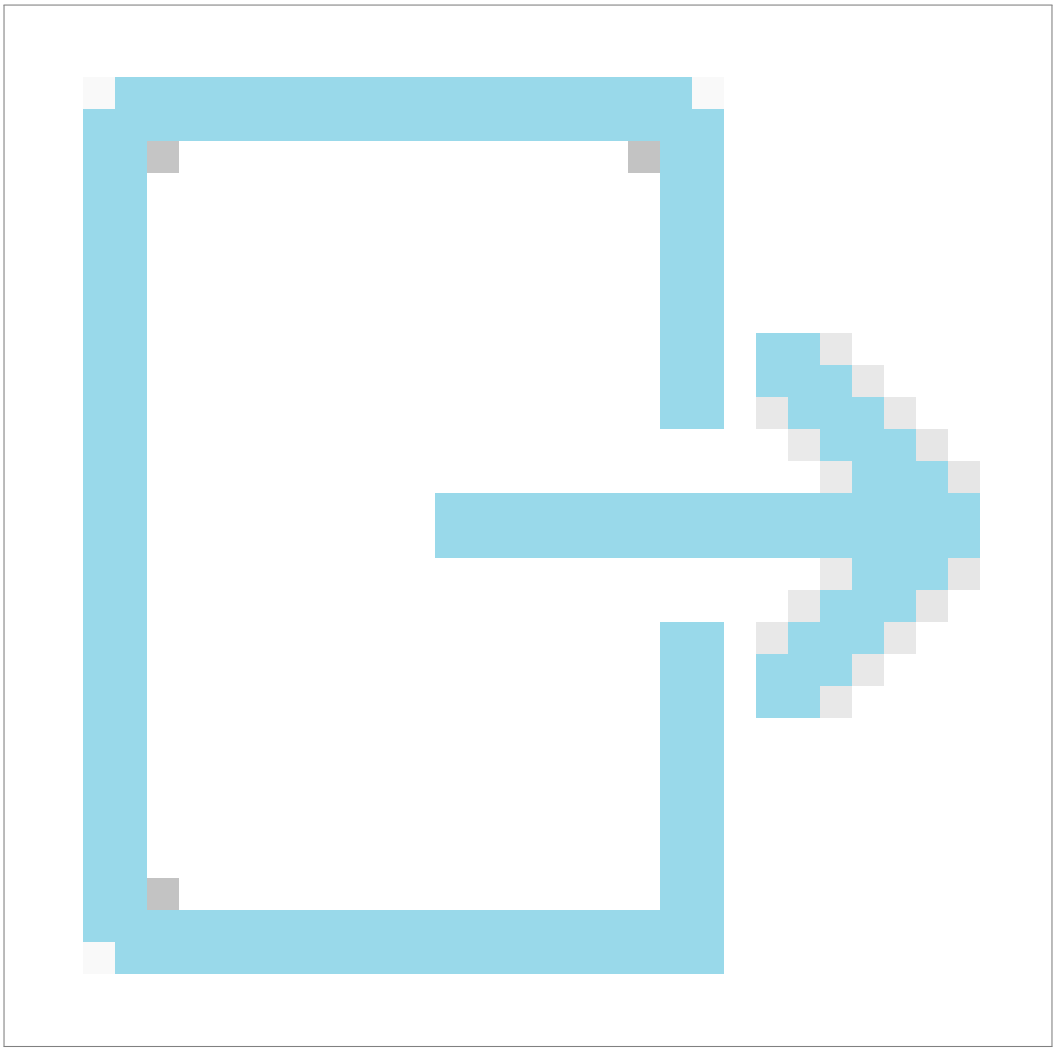
40.3 Absatz 3

Jede Einrichtung mit kritischen oder erheblichen Auswirkungen teilt ihren CSIRTs und der für sie zuständigen Behörde relevante Informationen im Zusammenhang mit einem meldepflichtigen Cyberangriff unverzüglich, spätestens jedoch vier Stunden, nachdem ihr bekannt wurde, dass der Sicherheitsvorfall meldepflichtig ist, mit.



Input

- Klassifizierungsskala für Cyberangriffe
- Erkannter Cyberangriff



Output

- Informationsaustausch zu Cyberangriffen

GOOD TO KNOW

Zeitpunkt

Innerhalb von 4 Stunden nach einem Cyberangriff

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Zu informieren: NCA

40.4 Absatz 4

Informationen im Zusammenhang mit einem Cyberangriff gelten als meldepflichtig, wenn der Cyberangriff bei der Bewertung durch die betroffene Einrichtung nach der Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8 als „erheblich“ bis „kritisch“ eingestuft wird. Die gemäß Absatz 1 Buchstabe c benannte zentrale Anlaufstelle auf Ebene der Einrichtung teilt die Einstufung des Sicherheitsvorfalls mit.

Relevante NCCS-Artikel

- Artikel 37
- Artikel 38

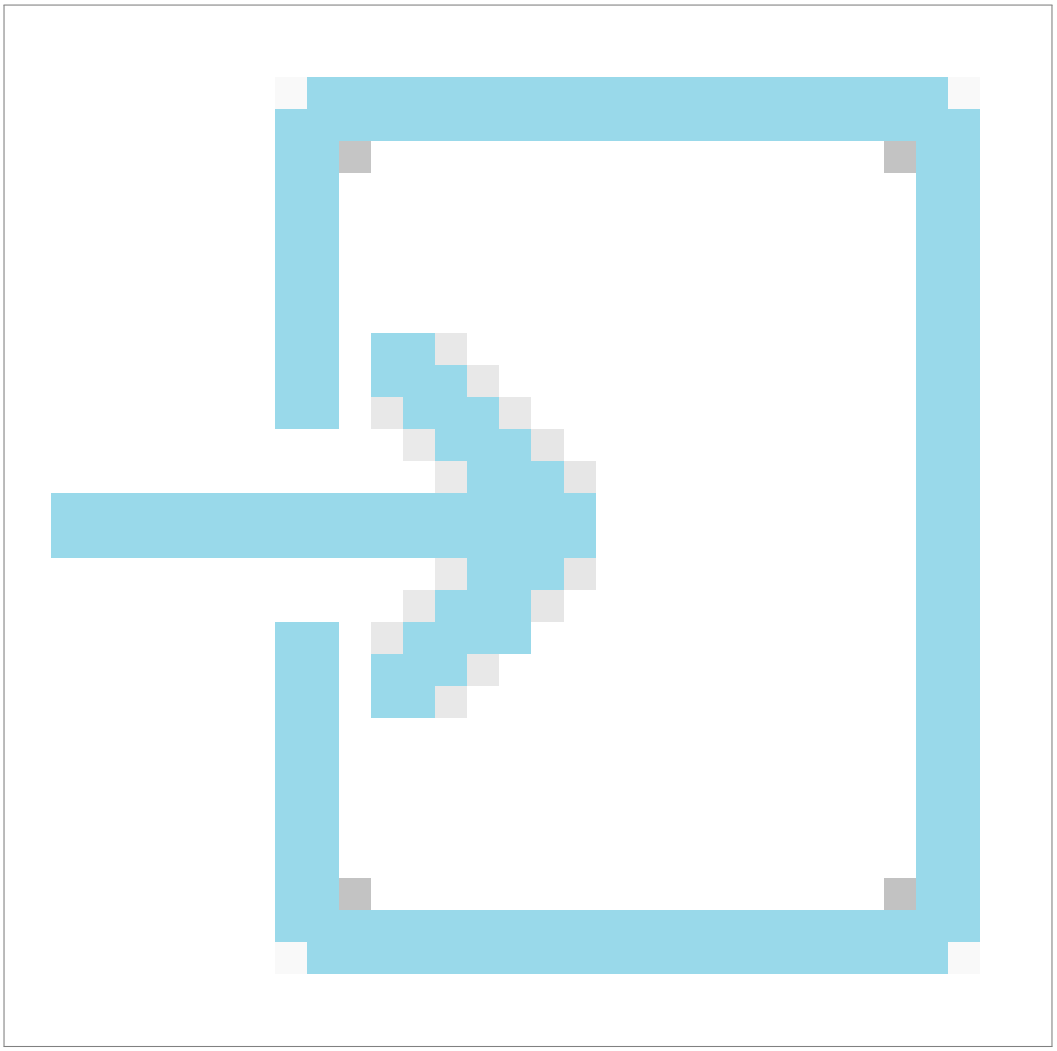
Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

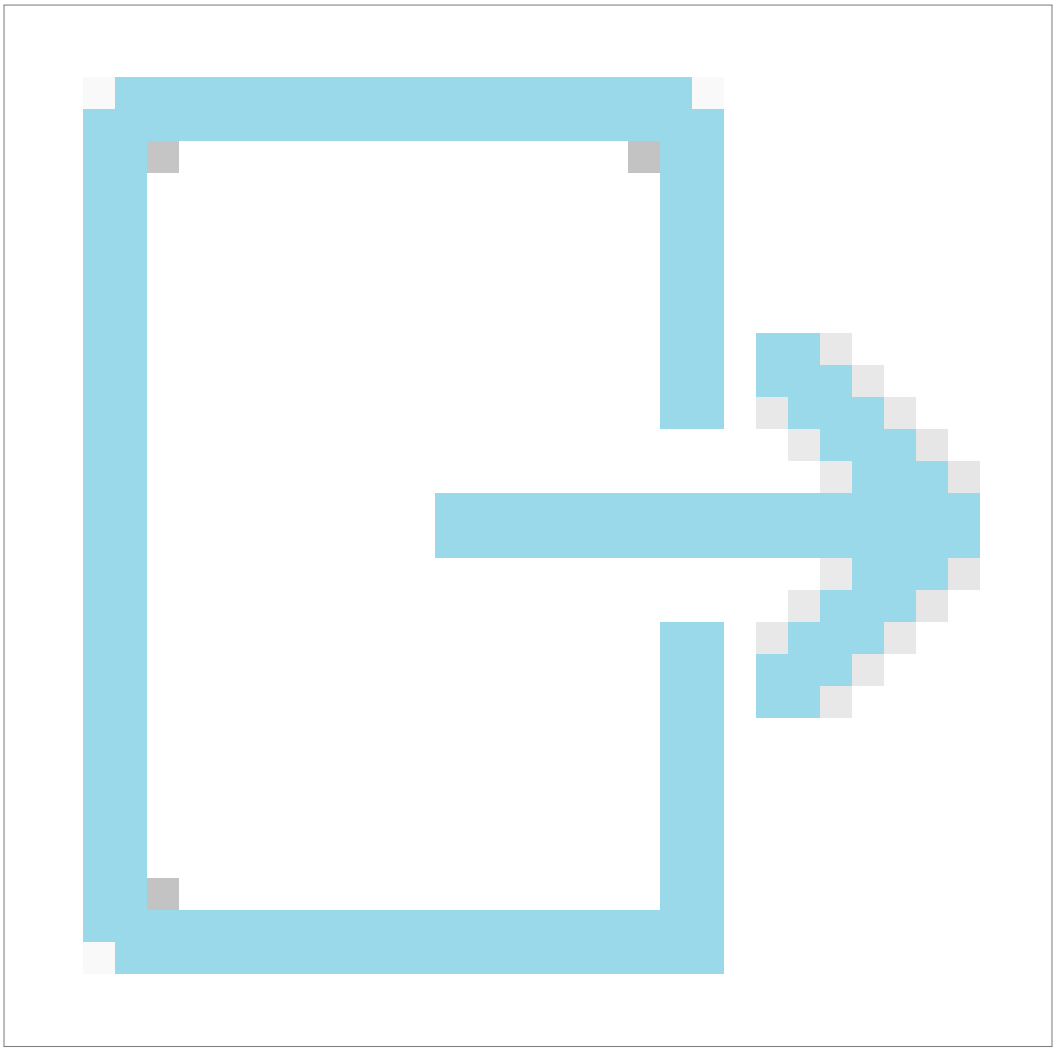
40.5 Absatz 5

Übermitteln Einrichtungen mit kritischen oder erheblichen Auswirkungen relevante Informationen zu aktiv ausgenutzten Schwachstellen ohne Patch an ein CSIRT, so kann dieses diese Informationen an die für das CSIRT zuständige Behörde weiterleiten. Je nach Sensibilität der gemeldeten Informationen kann das CSIRT die Informationen aus triftigen cybersicherheitsbezogenen Gründen zurückhalten oder zeitverzögert übermitteln.



Input

- Erkannte, ungepatchte und aktiv ausgenutzte Schwachstelle



Output

- Erkannte, ungepatchte und aktiv ausgenutzte Schwachstelle

GOOD TO KNOW

Zeitpunkt

NIS 2

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Zu informieren: NCA

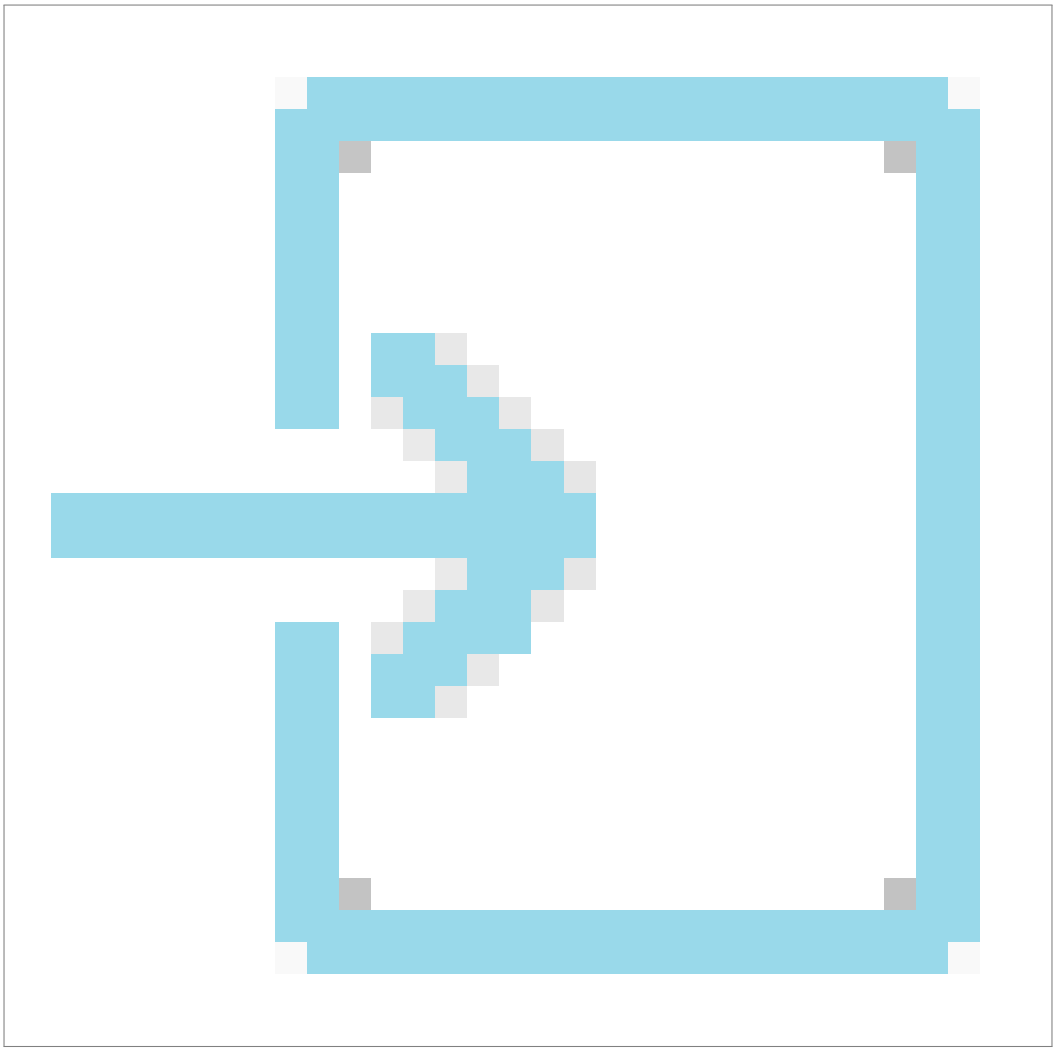
40.6 Absatz 6

Jede Einrichtung mit kritischen oder erheblichen Auswirkungen stellt ihren CSIRTs unverzüglich alle Informationen im Zusammenhang mit einer meldepflichtigen Cyberbedrohung bereit, die grenzüberschreitende Auswirkungen haben könnte. Informationen im Zusammenhang mit einer Cyberbedrohung gelten als meldepflichtig, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

a. Sie umfassen relevante Informationen für die Verhütung, Erkennung, Behandlung oder Minderung der Auswirkungen des Risikos durch andere Einrichtungen mit kritischen oder erheblichen Auswirkungen;

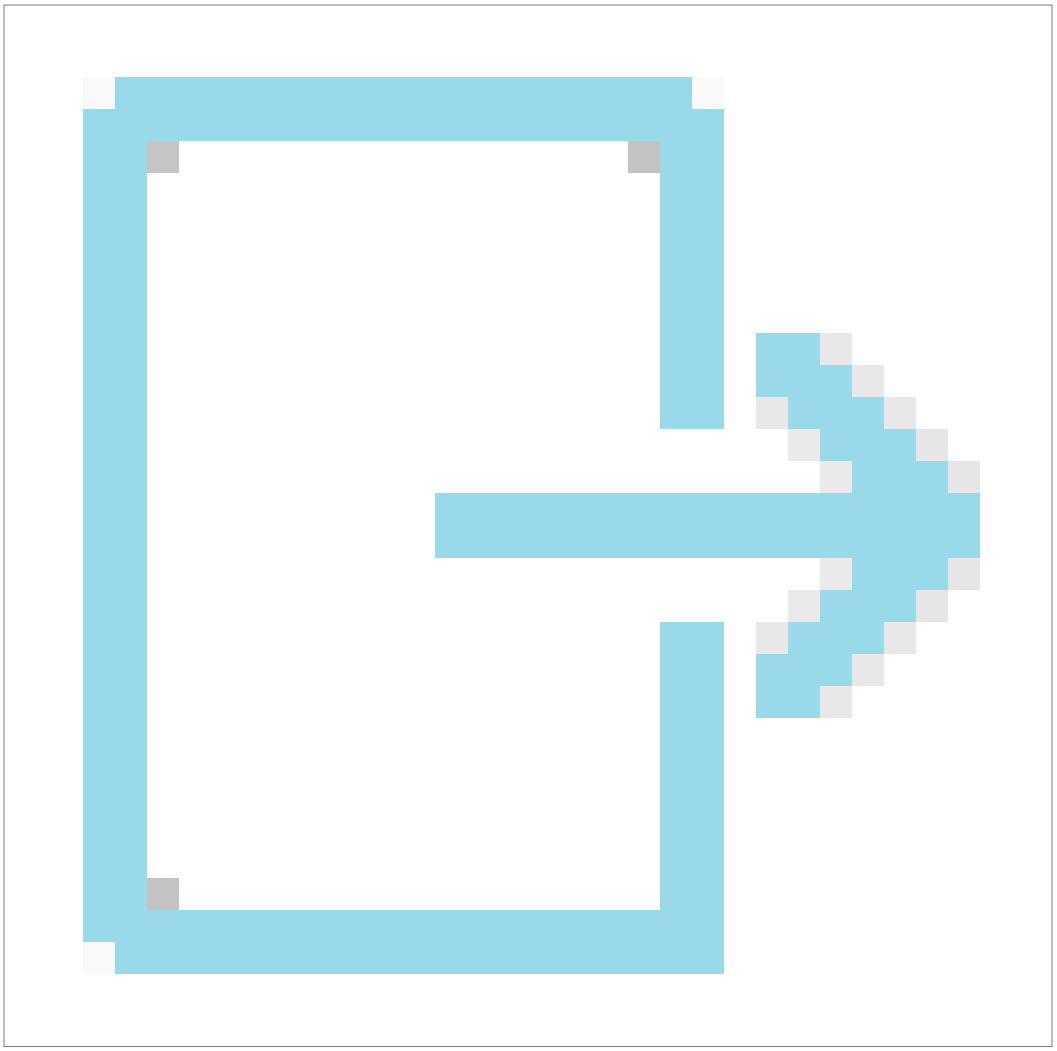
b. die ermittelten, im Zusammenhang mit einem Angriff genutzten Vorgehensweisen, Taktiken und Verfahren sind mit Informationen wie kompromittierten URL-Adressen oder IP-Adressen, Hashs oder anderen Attributen verbunden, die für die Kontextualisierung und Zuordnung des Angriffs nützlich sind;

c. eine Cyberbedrohung kann weiter bewertet und mit zusätzlichen Informationen verknüpft werden, die von Dienstanbietern oder Dritten, die nicht dieser Verordnung unterliegen, bereitgestellt werden.



Input

- Erkannte Cyberbedrohung



Output

- Informationsaustausch über Cyberbedrohungen

GOOD TO KNOW

Zeitpunkt

sofort

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

40.7 Absatz 7

Jede Einrichtung mit kritischen oder erheblichen Auswirkungen gibt beim Austausch von Informationen gemäß diesem Artikel an,

a. dass die Informationen gemäß dieser Verordnung übermittelt werden;

b. ob die Informationen Folgendes betreffen:

   i. einen meldepflichtigen Cyberangriff gemäß Absatz 3;

   ii. nicht öffentlich bekannte aktiv ausgenutzte Schwachstellen ohne Patch gemäß Absatz 4;

   iii. eine meldepflichtige Cyberbedrohung gemäß Absatz 5;

c. im Falle eines meldepflichtigen Cyberangriffs, welchen Grad der Cyberangriff nach der in Artikel 37 Absatz 8 genannten Klassifizierungsmethode für Cyberangriffe aufweist und welche Informationen zu dieser Einstufung geführt haben, einschließlich mindestens der Kritikalität des Cyberangriffs.

Relevante NCCS-Artikel

- Artikel 38 (3)
- Artikel 38 (4)

- Artikel 38 (5)
- Artikel 37 (8)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

40.8 Absatz 8

Meldet eine Einrichtung mit kritischen oder erheblichen Auswirkungen einen erheblichen Sicherheitsvorfall gemäß Artikel 23 der Richtlinie (EU) 2022/2555 [a] und enthält die Meldung des Sicherheitsvorfalls nach dem genannten Artikel einschlägige Informationen gemäß Absatz 3 des vorliegenden Artikels, so gilt die Meldung der Einrichtung nach Artikel 23 Absatz 1 der genannten Richtlinie auch als Meldung von Informationen gemäß Absatz 3 des vorliegenden Artikels.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#tit_1

Relevante NCCS-Artikel

- Artikel 38 (3)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

40.9 Absatz 9

Jede Einrichtung mit kritischen oder erheblichen Auswirkungen erstattet der für sie zuständigen Behörde oder dem CSIRT Bericht, wobei sie klar angibt, welche Informationen nur an die zuständige Behörde oder das CSIRT übermittelt werden dürfen, wenn der Informationsaustausch die Quelle eines Cyberangriffs sein könnte. Jede Einrichtung mit kritischen oder erheblichen Auswirkungen hat das Recht, dem zuständigen CSIRT eine nichtvertrauliche Fassung der Informationen zur Verfügung zu stellen.

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Zu informieren: NCA

Chapter 41

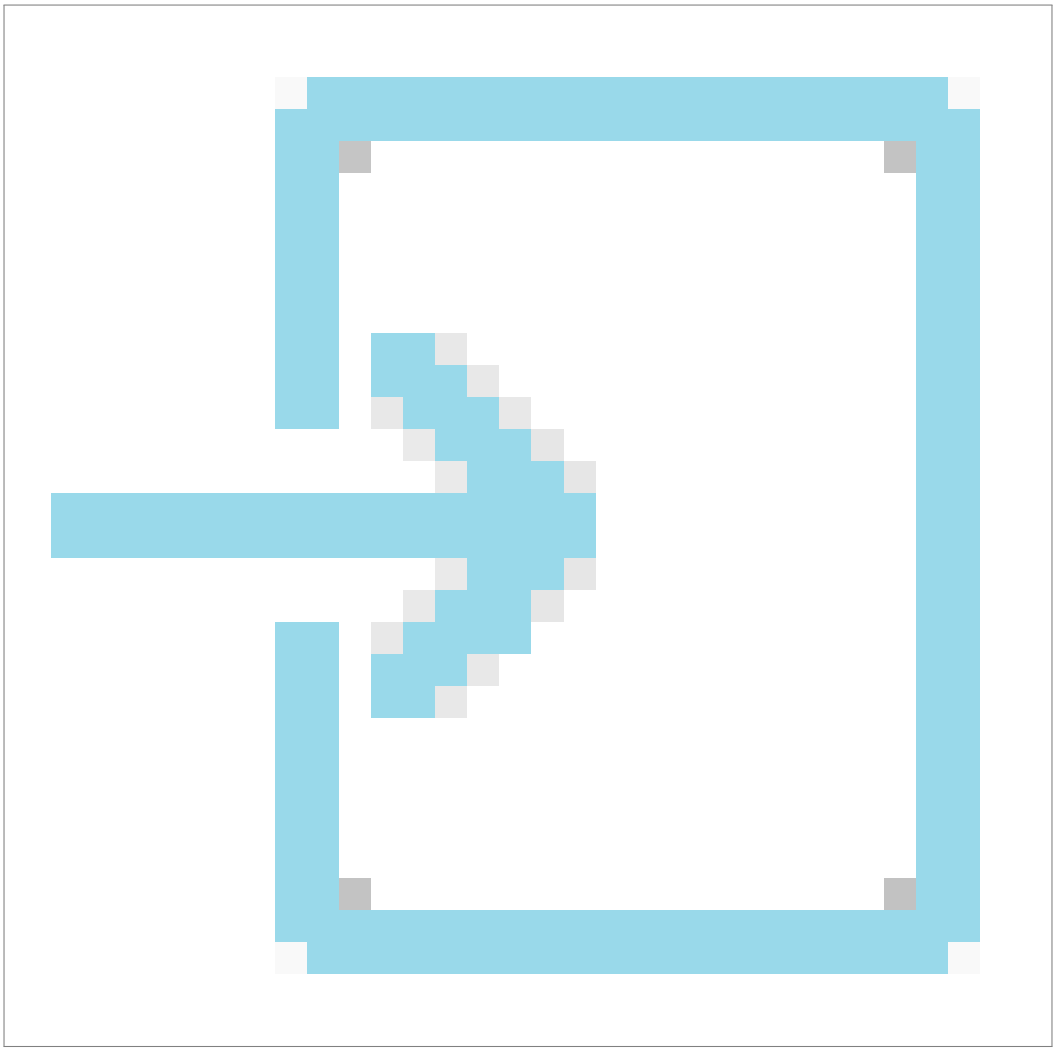
Artikel 39. : Erkennung von Cyberangriffen und Umgang mit den damit zusammenhängenden Informationen

41.1 Absatz 1

Einrichtungen mit erheblichen oder kritischen Auswirkungen entwickeln mit der erforderlichen Unterstützung der jeweils zuständigen Behörde, von ENTSO-E und der EU-VNBO die erforderlichen Kapazitäten für den Umgang mit entdeckten Cyberangriffen. Einrichtungen mit kritischen oder erheblichen Auswirkungen können von dem CSIRT unterstützt werden, das in ihrem jeweiligen Mitgliedstaat im Rahmen der den CSIRTs gemäß Artikel 11 Absatz 5 Buchstabe a der Richtlinie (EU) 2022/2555 [a] übertragenen Aufgabe benannt wurde.

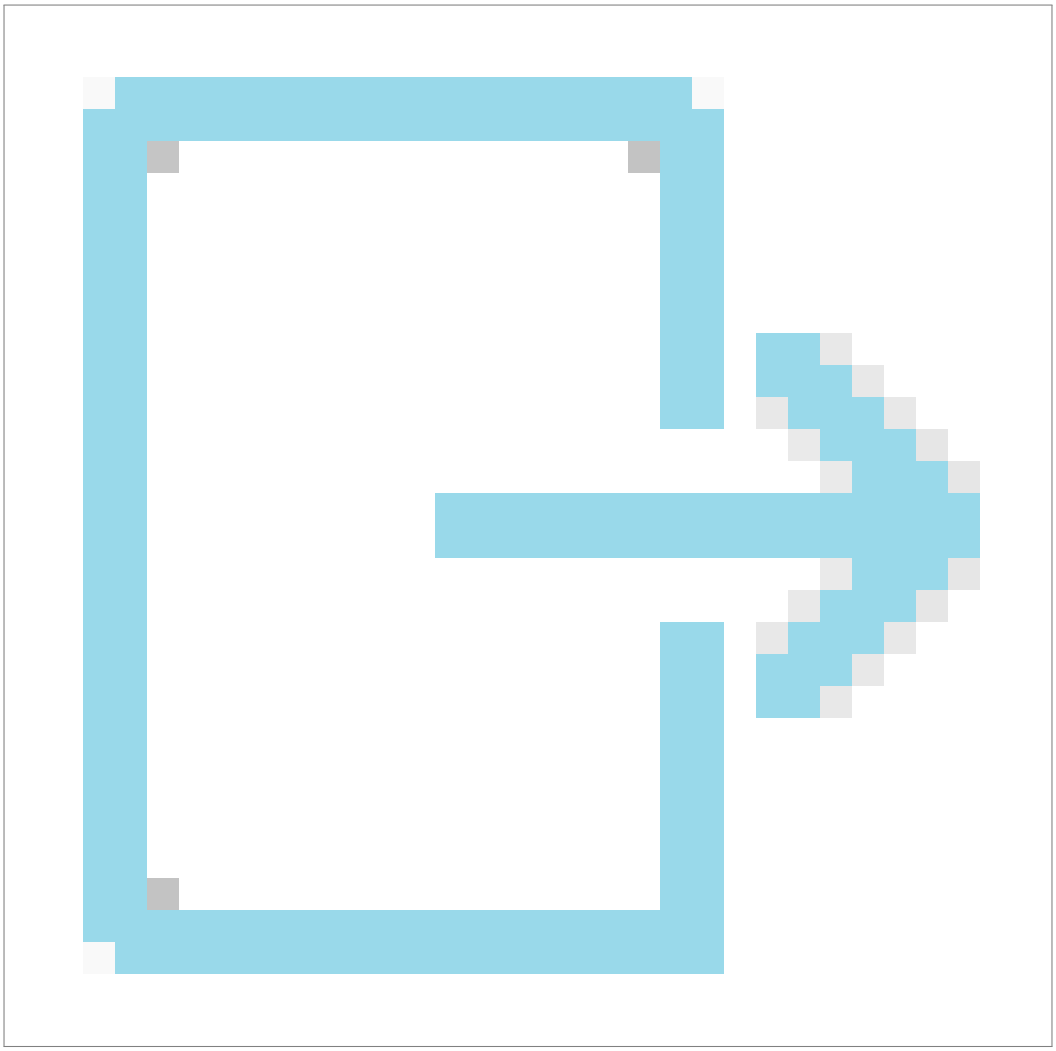
Einrichtungen mit kritischen oder erheblichen Auswirkungen setzen wirksame Verfahren zur Ermittlung, Klassifizierung und Bewältigung von Cyberangriffen ein, die sich auf grenzüberschreitende Stromflüsse auswirken oder auswirken könnten, um deren Auswirkungen möglichst gering zu halten.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_11



Input

- Klassifizierungsskala für Cyberangriffe



Output

- Verfahren auf Unternehmensebene zum Umgang mit Cyberangriffen

A

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: HIE, CIE, ENTSO-E, TSO, EU DSO, NCA

41.2 Absatz 2

Hat ein Cyberangriff Auswirkungen auf grenzüberschreitende Stromflüsse, so arbeiten die zentralen Anlaufstellen auf Ebene der betroffenen Einrichtungen mit kritischen oder erheblichen Auswirkungen zusammen, um Informationen untereinander auszutauschen,

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

41.3 Absatz 2

wobei sie von der zuständigen Behörde des Mitgliedstaats, in dem der Cyberangriff zuerst gemeldet wurde, koordiniert werden.

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA

41.4 Absatz 3

Einrichtungen mit kritischen oder erheblichen Auswirkungen

a. stellen sicher, dass ihre eigene zentrale Anlaufstelle auf Ebene der Einrichtung nach dem Grundsatz „Kenntnis nur, wenn nötig“ Zugang zu den Informationen hat, die sie von der nationalen zentralen Anlaufstelle über ihre zuständige Behörde erhalten hat;

b. übermitteln, sofern dies nicht bereits gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2022/2555 geschehen ist, der zuständigen Behörde des Mitgliedstaats, in dem sie niedergelassen sind, und der nationalen zentralen Anlaufstelle eine Liste ihrer für die Cybersicherheit zuständigen zentralen Anlaufstellen,

   i. von denen die zuständige Behörde und die nationale zentrale Anlaufstelle Informationen über meldepflichtige Cyberangriffe erhalten könnte;

   ii. an die die zuständigen Behörden und die nationalen zentralen Anlaufstellen gegebenenfalls Informationen übermitteln müssen;

c. richten auf der Grundlage der beobachtbaren Entwicklung des Cyberangriffs innerhalb der Perimeter mit kritischen oder erheblichen Auswirkungen Verfahren zur Bewältigung von Cyberangriffen ein, einschließlich Rollen und Zuständigkeiten, Aufgaben und Reaktionen;

d. testen mindestens einmal jährlich alle Verfahren zur Bewältigung von Cyberangriffen, wobei sie mindestens ein Szenario testen, das sich direkt oder indirekt auf grenzüberschreitende Stromflüsse auswirkt. Dieser jährliche Test kann von Einrichtungen mit kritischen oder erheblichen Auswirkungen während der regelmäßigen Übungen gemäß Artikel 43 durchgeführt werden. Jede Live-Reaktionsmaßnahme auf einen Cyberangriff mit einer Folge, die gemäß der in Artikel 37 Absatz 8 genannten Klassifizierungsmethode für Cyberangriffe mindestens in die Stufe 2 eingestuft wird und der eine Cybersicherheitsursache zugrunde liegt, kann als jährlicher Test des Plans für die Reaktion auf Cyberangriffe betrachtet werden.

Relevante NCCS-Artikel

- Artikel 43
- Artikel 37 (8)

GOOD TO KNOW

Rekurrenz

1 Jahr

Verantwortlich für die Aktivität: HIE, CIE

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE

Zu informieren: NCA

41.5 Absatz 4

Die in Absatz 1 aufgeführten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 der Verordnung (EU) 2019/943 [a] auch an die regionalen Koordinierungszentren delegiert werden.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1

Relevante NCCS-Artikel

- Artikel 39 (1)

Verantwortlich für die Aktivität: MS

Beteiligte Stakeholder:

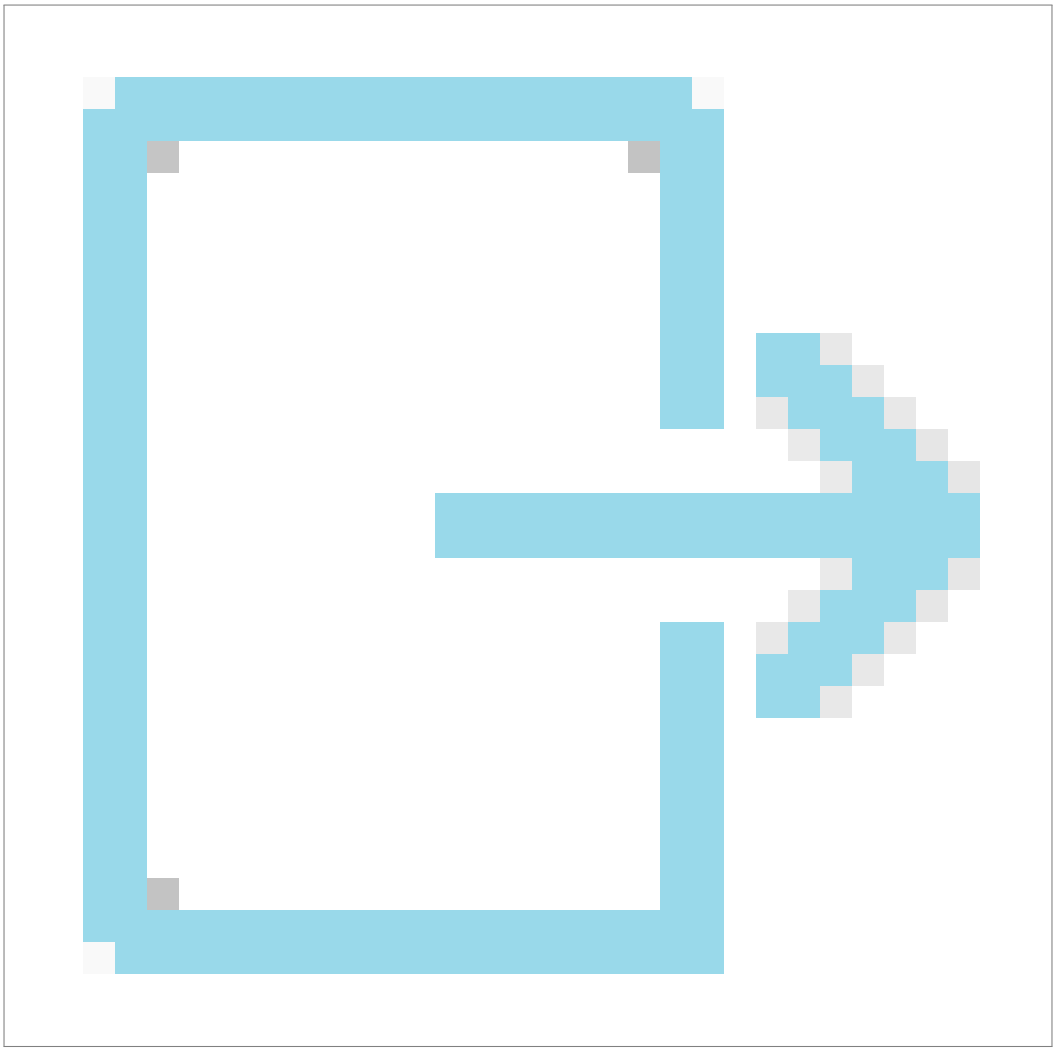
Beteiligt an der Aufgabenausführung: MS, RCC

Chapter 42

Artikel 40. : Krisenmanagement

42.1 Absatz 1

Stellt die zuständige Behörde fest, dass eine Stromversorgungskrise im Zusammenhang mit einem Cyberangriff steht, der Auswirkungen auf mehr als einen Mitgliedstaat hat, setzen die zuständigen Behörden der betroffenen Mitgliedstaaten, die CS-NCA, die RP-NCA und die NIS-Behörden für das Cyberkrisenmanagement der betroffenen Mitgliedstaaten gemeinsam eine Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen ein.



Output

- Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen

A

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: NCA, RP NCA, CS NCA

42.2 Absatz 2

Die Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen

a. koordiniert eine effiziente Einholung aller relevanten Cybersicherheitsinformationen und deren weitere Übermittlung an die am Krisenmanagementprozess beteiligten Einrichtungen;

b. organisiert die Kommunikation zwischen allen von der Krise betroffenen Einrichtungen und den zuständigen Behörden, um Überschneidungen zu verringern und die Effizienz der Analysen und technischen Reaktionen zur Bewältigung zeitgleich auftretender Stromversorgungskrisen, denen eine Cybersicherheitsursache zugrunde liegt, zu erhöhen;

c. stellt in Zusammenarbeit mit den zuständigen CSIRTs das erforderliche Fachwissen bereit, einschließlich operativer Beratung bei der Umsetzung möglicher Abhilfemaßnahmen für die von dem Sicherheitsvorfall betroffenen Einrichtungen;

d. unterrichtet die Kommission und die Koordinierungsgruppe „Strom“ im Einklang mit den in Artikel 46 festgelegten Schutzprinzipien über den Stand des Sicherheitsvorfalls und aktualisiert diese Informationen regelmäßig;

e. holt Rat bei den zuständigen Behörden, Agenturen oder Einrichtungen ein, die zur Bewältigung der Stromversorgungskrise beitragen könnten.

Relevante NCCS-Artikel

- Artikel 46

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA, RP NCA, CS NCA

Zu informieren: EC, ECG

42.3 Absatz 3

Gilt der Cyberangriff als Cybersicherheitsvorfall großen Ausmaßes oder wird dies erwartet, unterrichtet die Ad-hocKoordinierungsgruppe für grenzüberschreitende Krisen unverzüglich die nationalen Behörden für das Cyberkrisenmanagement gemäß Artikel 9 Absatz 1 [a] der Richtlinie (EU) 2022/2555 in den von dem Sicherheitsvorfall betroffenen Mitgliedstaaten sowie die Kommission und das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe). In einer solchen Situation unterstützt die Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen das EU-CyCLONe in Bezug auf sektorale Besonderheiten.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9

Beteiligte Stakeholder:

Zu informieren: EC, CS NCA

42.4 Absatz 4

Einrichtungen mit kritischen oder erheblichen Auswirkungen müssen Kapazitäten, interne Leitlinien, Vorsorgepläne und Personal, das an der Aufdeckung und Eindämmung grenzüberschreitender Krisen mitwirkt, vorsehen und darüber verfügen. Die von einer zeitgleich auftretenden Stromversorgungskrise betroffene Einrichtung mit kritischen oder erheblichen Auswirkungen untersucht die zugrunde liegende Ursache dieser Krise in Zusammenarbeit mit der für sie zuständigen Behörde, um festzustellen, inwieweit die Krise mit einem Cyberangriff in Verbindung steht.

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA

42.5 Absatz 5

Die in Absatz 4 genannten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 [a] der Verordnung (EU) 2019/943 auch an die regionalen Koordinierungszentren delegiert werden.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1

Relevante NCCS-Artikel

- Artikel 40 (4)

Verantwortlich für die Aktivität: MS

Beteiligte Stakeholder:

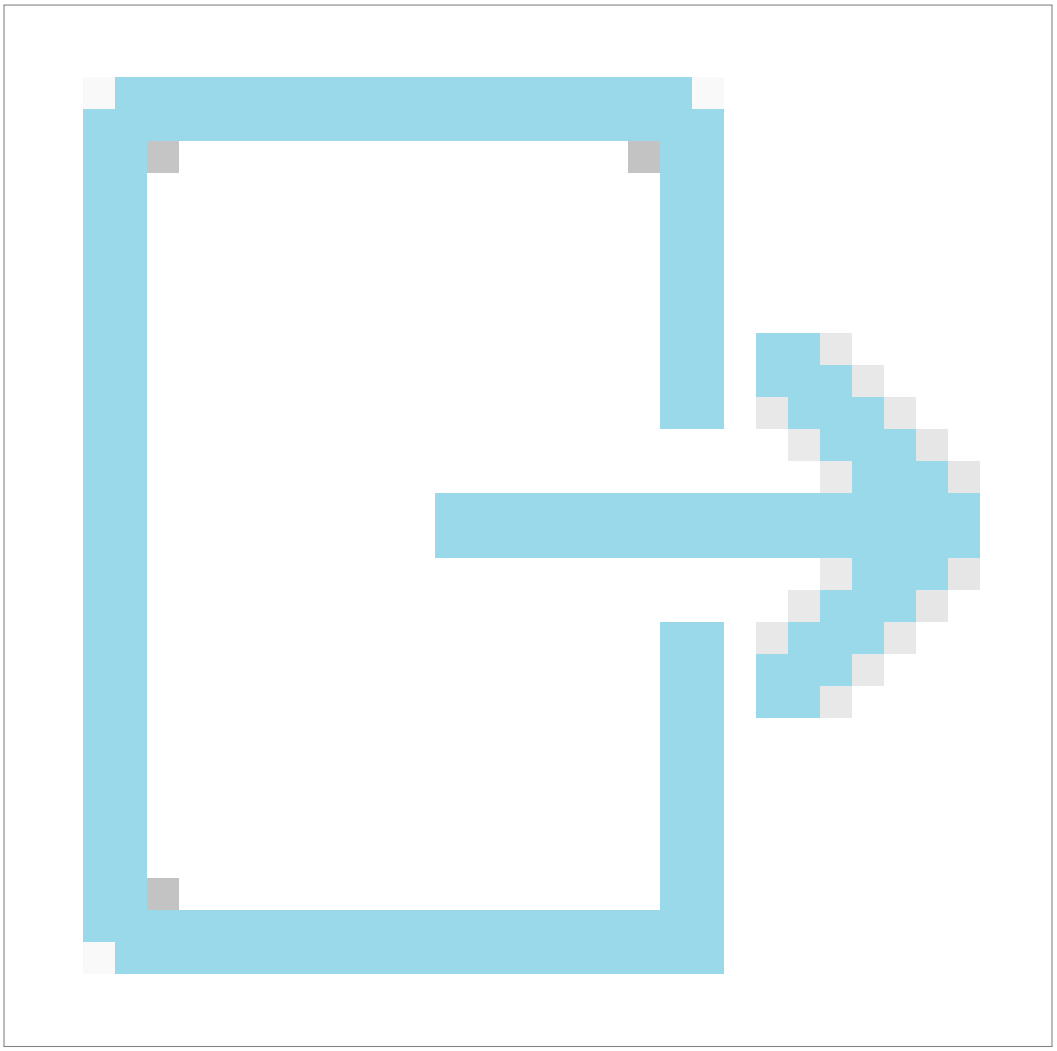
Beteiligt an der Aufgabenausführung: MS

Chapter 43

Artikel 41. : Cybersicherheitskrisenmanagement- und -reaktionspläne

43.1 Absatz 1

Innerhalb von 24 Monaten nach der Übermittlung des Berichts über die unionsweite Risikobewertung an die ACER entwickelt diese in enger Zusammenarbeit mit der ENISA, ENTSO-E, der EU-VNBO, den CS-NCA, den zuständigen Behörden, den RP-NCA, den NRB und den nationalen NIS-Behörden für das Cyberkrisenmanagement einen unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplan für den Elektrizitätssektor.



Output

- Krisenmanagement- und Reaktionsplan auf Ebene der Mitgliedstaaten (modifiziert)

GOOD TO KNOW

Zeitpunkt

Innerhalb von 24 Monaten nach Einreichung des EU-weiten Risikobewertungsberichts

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, NIS CG, CS NCA

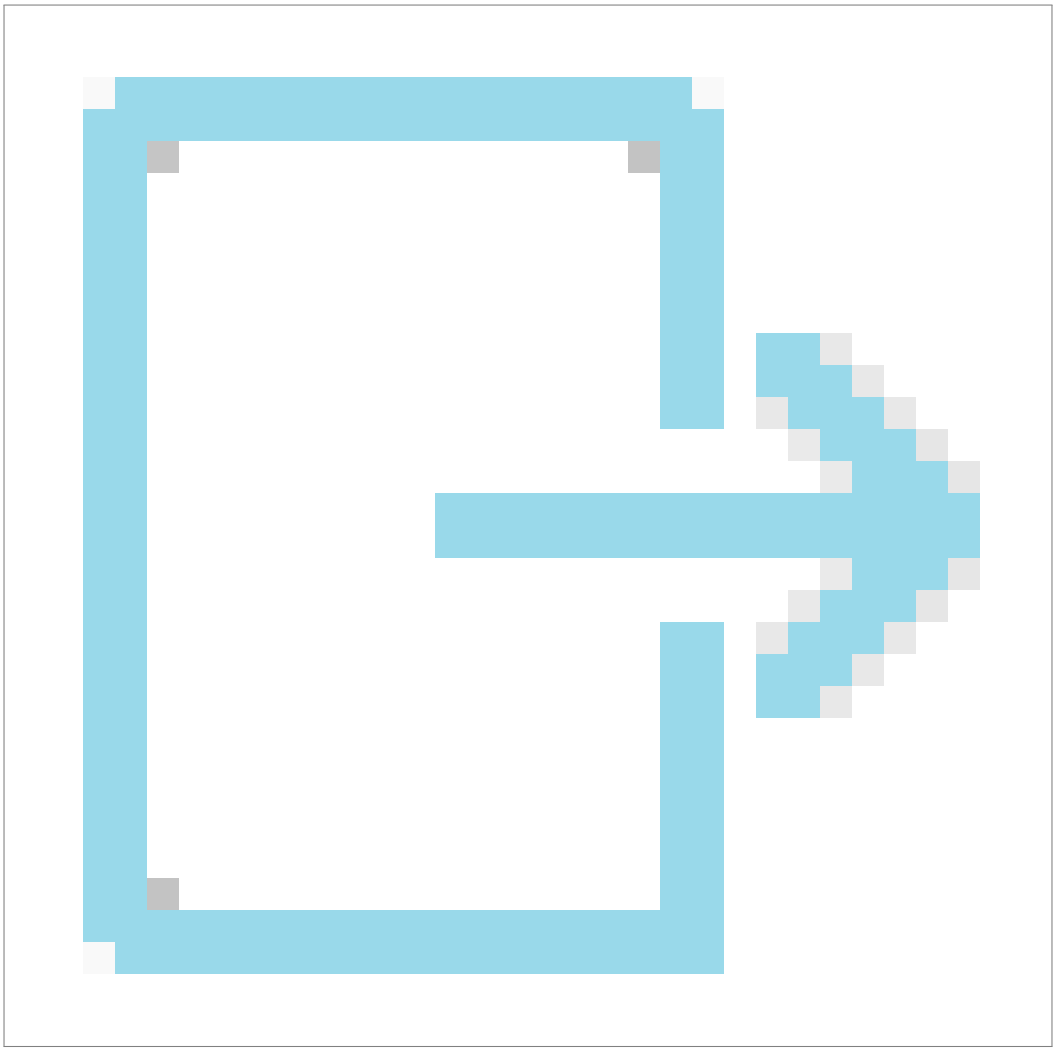
43.2 Absatz 2

Innerhalb von 12 Monaten nach der Ausarbeitung des unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplans für den Elektrizitätssektor gemäß Absatz 1 durch die ACER erstellt jede zuständige Behörde einen nationalen Cybersicherheitskrisenmanagement- und -reaktionsplan für grenzüberschreitende Stromflüsse unter Berücksichtigung des unionsweiten Cybersicherheitskrisenmanageme und -reaktionsplans für den Elektrizitätssektor und des gemäß Artikel 10 der Verordnung (EU) 2019/941 [a] erstellten nationalen Risikovorsorgeplans. Dieser Plan muss mit dem Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gemäß Artikel 9 Absatz 4 der Richtlinie (EU) 2022/2555 [b] im Einklang stehen. Die zuständige Behörde stimmt sich mit den Einrichtungen mit kritischen oder erheblichen Auswirkungen sowie mit der RP-NCA in ihrem Mitgliedstaat ab.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e928-1-1
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9

Relevante NCCS-Artikel

- Artikel 41 (1)



Output

- Krisenmanagement- und Reaktionsplan auf Unionsebene (modifiziert)

GOOD TO KNOW

Zeitpunkt

Innerhalb von 12 Monaten nach der Entwicklung des Plans für das Krisenmanagement und die Reaktion auf Cybersicherheitskrisen auf EU-Ebene

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO, NCA, CS NCA

43.3 Absatz 3

Der gemäß Artikel 9 Absatz 4 der Richtlinie (EU) 2022/2555 [a] erforderliche nationale Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gilt als nationaler Plan für das Cybersicherheitskrisenmanagement im Sinne dieses Artikels, wenn er Bestimmungen für das Krisenmanagement und die Krisenreaktion in Bezug auf grenzüberschreitende Stromflüsse enthält.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

43.4 Absatz 4

Die in den Absätzen 1 und 2 aufgeführten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 [a] der Verordnung (EU) 2019/943 auch an die regionalen Koordinierungszen-

tren delegiert werden.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1

Relevante NCCS-Artikel

- Artikel 41 (1)
- Artikel 41 (2)

Verantwortlich für die Aktivität: MS

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: MS, RCC

43.5 Absatz 5

Einrichtungen mit kritischen oder erheblichen Auswirkungen stellen sicher, dass ihre Krisenmanagementprozesse im Bereich der Cybersicherheit

a. kompatible Verfahren für die grenzüberschreitende Bewältigung von Cybersicherheitsvorfällen gemäß Artikel 6 Nummer 8 der Richtlinie (EU) 2022/2555 [a] umfassen, die förmlich in ihren Krisenmanagementpläne enthalten sind;

b. Teil der allgemeinen Krisenmanagementmaßnahmen sind.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_6

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

43.6 Absatz 6

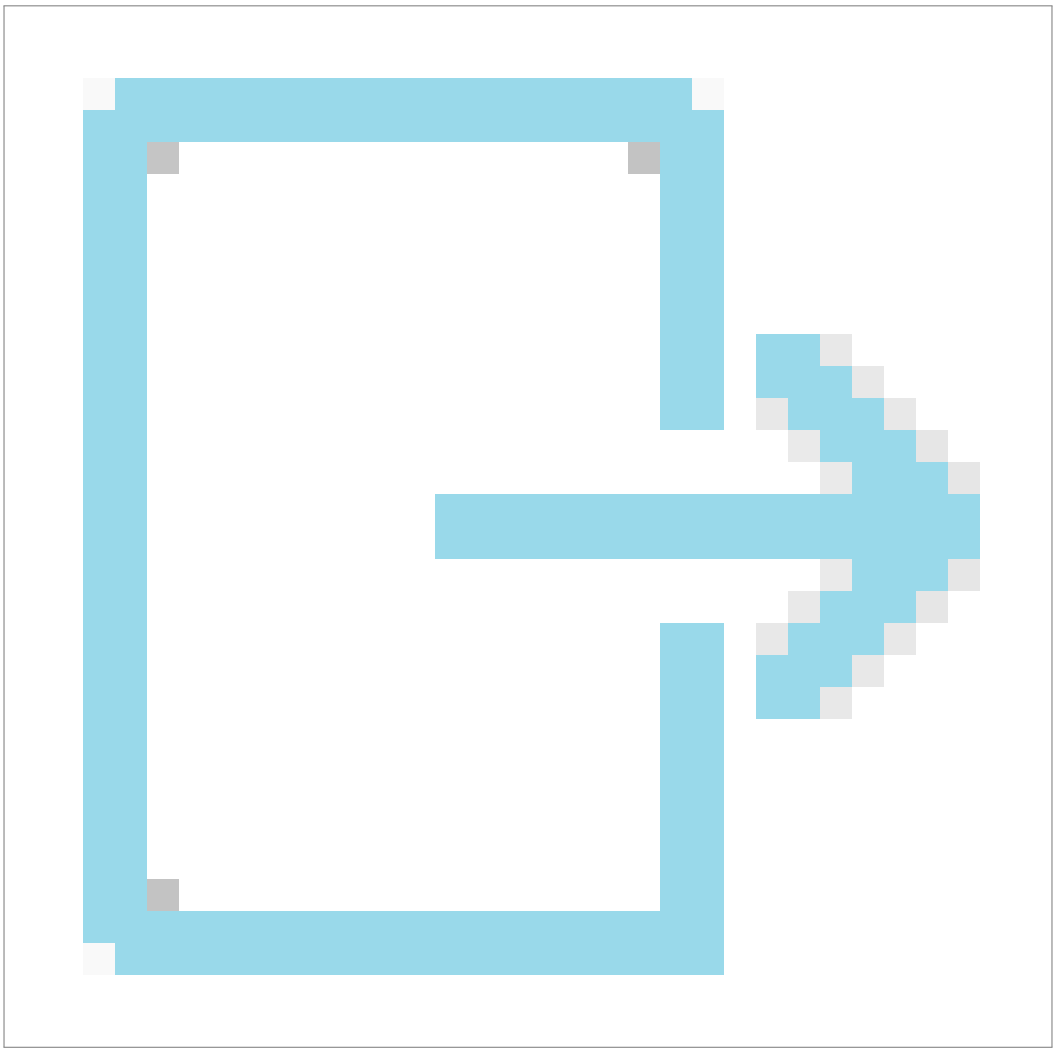
Innerhalb von 12 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre erstellen Einrichtungen mit kritischen oder erheblichen Auswirkungen auf Ebene der Einrichtung einen Krisenmanagementplan für Cybersicherheitskrisen, der in ihre allgemeinen Krisenmanagementpläne aufgenommen wird. Dieser Plan muss mindestens Folgendes umfassen:

a. Regeln für die Erklärung einer Krise gemäß Artikel 14 Absätze 2 und 3 der Verordnung (EU) 2019/941; [a]
b. klare Aufgaben und Zuständigkeiten für das Krisenmanagement, einschließlich der Rolle anderer relevanter Einrichtungen mit kritischen oder erheblichen Auswirkungen;
c. aktuelle Kontaktinformationen sowie Regeln für die Kommunikation und den Informationsaustausch während einer Krisensituation, einschließlich der Verbindung zu den CSIRTs.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e1185-1-1

Relevante NCCS-Artikel

- Artikel 24 (6)



Output

- Krisenmanagement- und Reaktionsplan auf Unternehmensebene (einschließlich Business Continuity Plan)

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

12 Monate nach Identifizierung

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

43.7 Absatz 7

Die Maßnahmen für das Krisenmanagement gemäß Artikel 21 Absatz 2 [a] Buchstabe c der Richtlinie (EU) 2022/2555 gelten als Krisenmanagementplan auf Ebene der Einrichtung für den Elektrizitätssektor im Sinne dieses Artikels, wenn sie alle in Absatz 6 aufgeführten Anforderungen erfüllen.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_21

Relevante NCCS-Artikel

- Artikel 41 (6)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

43.8 Absatz 8

Die Krisenmanagementpläne werden in den Cybersicherheitsübungen gemäß den Artikeln 43, 44 und 45 getestet.

Relevante NCCS-Artikel

- Artikel 43
- Artikel 44
- Artikel 45

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

43.9 Absatz 9

In Bezug auf Prozesse mit kritischen oder erheblichen Auswirkungen nehmen Einrichtungen mit kritischen oder erheblichen Auswirkungen ihre Krisenmanagementpläne auf Ebene der Einrichtung in ihre Pläne zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity) auf. Die Krisenmanagementpläne auf Ebene der Einrichtung müssen Folgendes umfassen:

a. Prozesse, die von der Verfügbarkeit, Integrität und Zuverlässigkeit von IT-Diensten abhängen;

b. alle Standorte für die Aufrechterhaltung des Geschäftsbetriebs, einschließlich der Standorte für Hardware und Software;

c. alle internen Aufgaben und Zuständigkeiten im Zusammenhang mit den Verfahren zur Aufrechterhaltung des Geschäftsbetriebs.

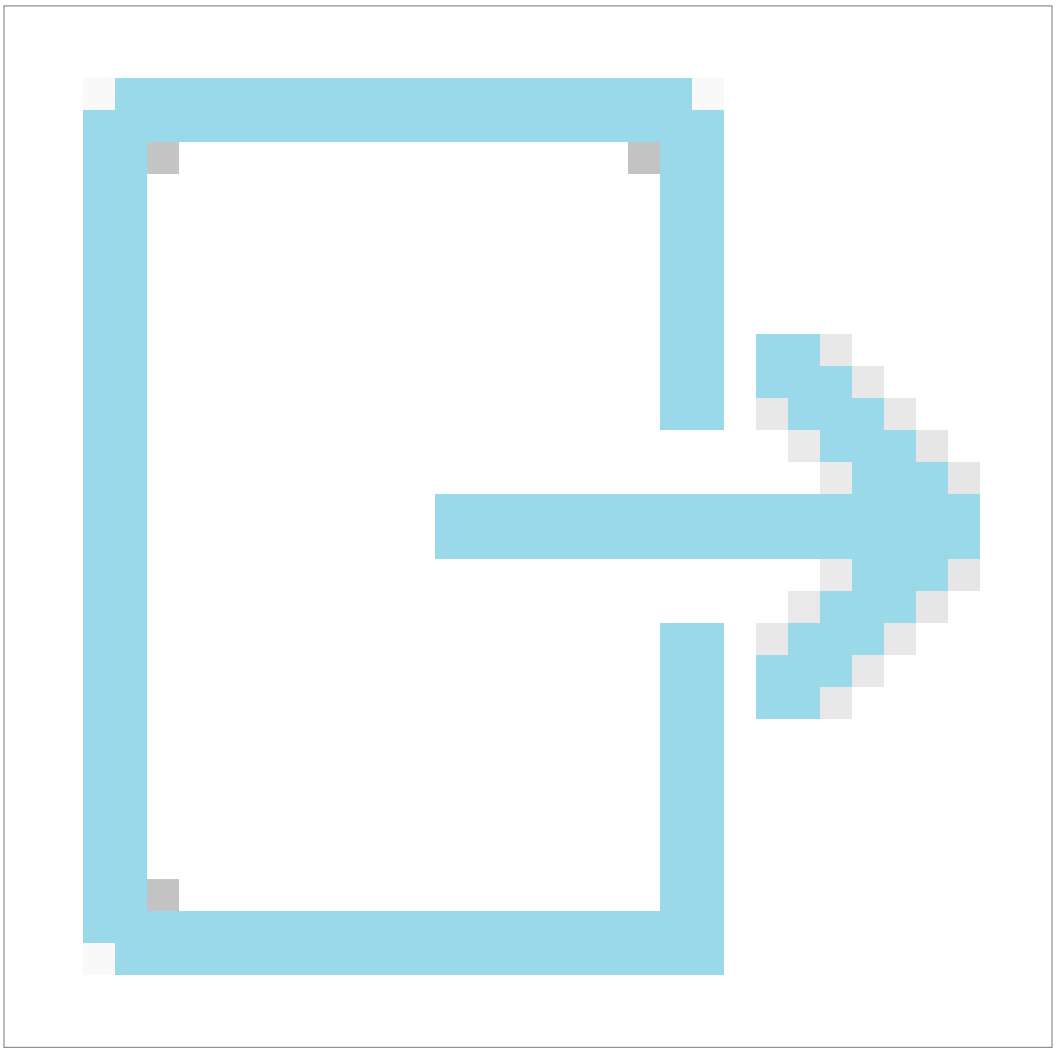
Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

43.10 Absatz 10

Einrichtungen mit kritischen oder erheblichen Auswirkungen aktualisieren ihre Krisenmanagementpläne auf Ebene der Einrichtung mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.



Output

- Krisenmanagement- und Reaktionsplan auf Unternehmensebene (modifiziert)

GOOD TO KNOW

Rekurrenz

3 Jahre

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

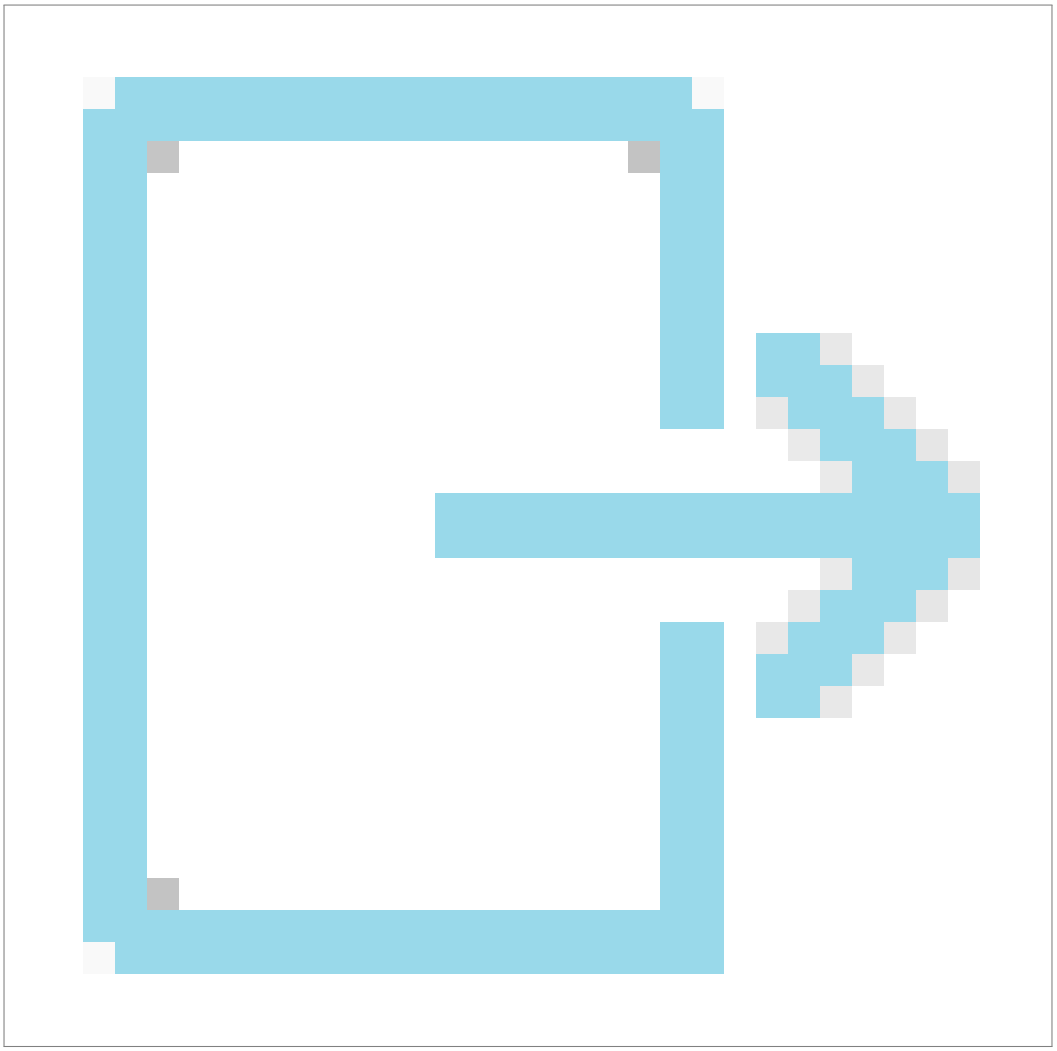
Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

43.11 Absatz 11

Die ACER aktualisiert den gemäß Absatz 1 erstellten unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplan für den Elektrizitätssektor mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.

Relevante NCCS-Artikel

- Artikel 4 (1)



Output

- Krisenmanagement- und Reaktionsplan auf Unionsebene (modofiziert)

GOOD TO KNOW

Rekurrenz

3 Jahre

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

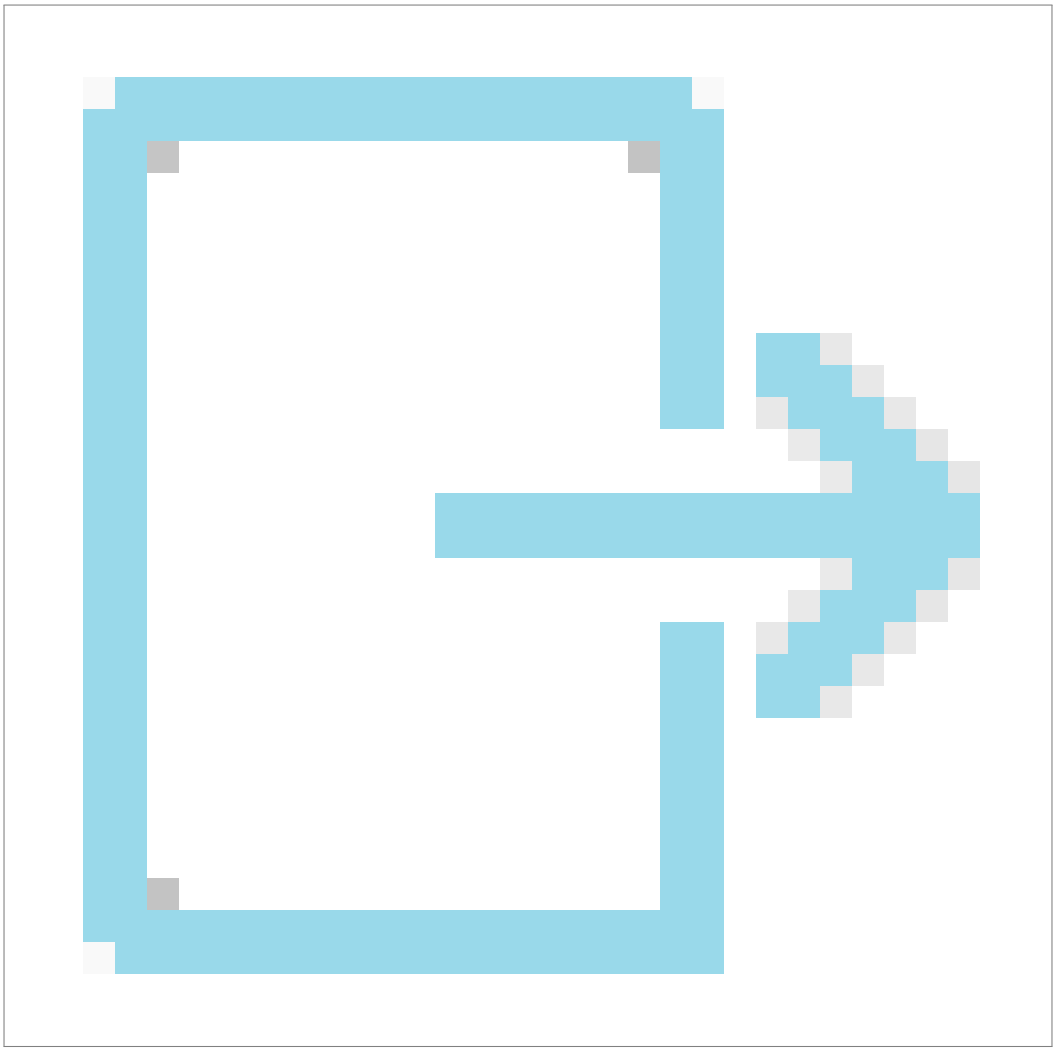
Beteiligt an der Aufgabenausführung: ACER

43.12 Absatz 12

Jede zuständige Behörde aktualisiert den gemäß Absatz 2 erstellten nationalen Cybersicherheitskrisenmanagementund -reaktionsplan für grenzüberschreitende Stromflüsse mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.

Relevante NCCS-Artikel

- Artikel 4 (2)



Output

- Nationaler Krisenmanagement- und Reaktionsplan für Cybersicherheit (modifiziert)

GOOD TO KNOW

Rekurrenz

3 Jahre

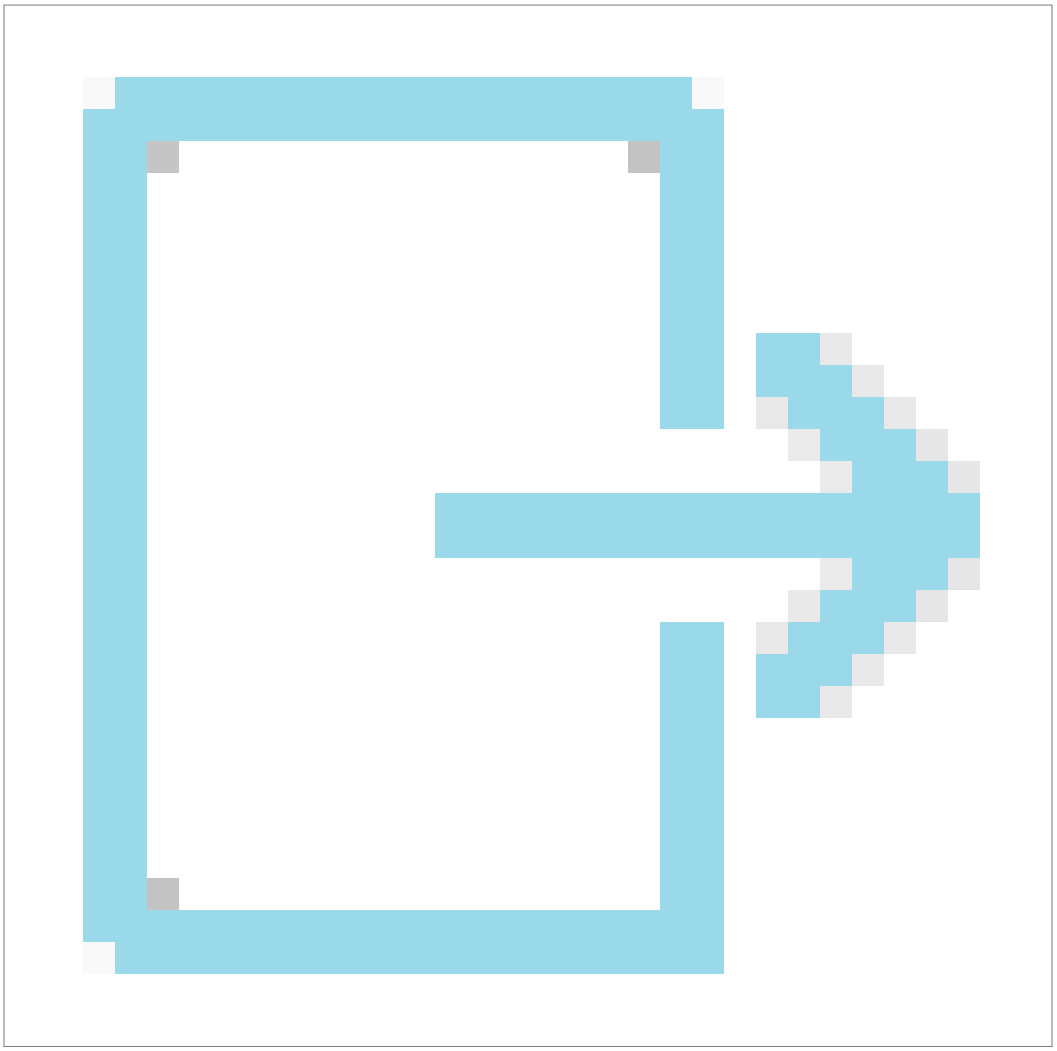
Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

43.13 Absatz 13

Einrichtungen mit kritischen oder erheblichen Auswirkungen testen ihre Pläne zur Aufrechterhaltung des Geschäftsbetriebs mindestens einmal alle drei Jahre oder nach größeren Änderungen in einem Prozess mit kritischen Auswirkungen. Die Ergebnisse der Tests der Pläne zur Aufrechterhaltung des Geschäftsbetriebs werden dokumentiert. Einrichtungen mit kritischen oder erheblichen Auswirkungen können den Test ihres Plans zur Aufrechterhaltung des Geschäftsbetriebs in die Cybersicherheitsübungen einbeziehen.



Output

- Business Continuity Plan (Modifizierung)

GOOD TO KNOW

Rekurrenz

3 Jahre

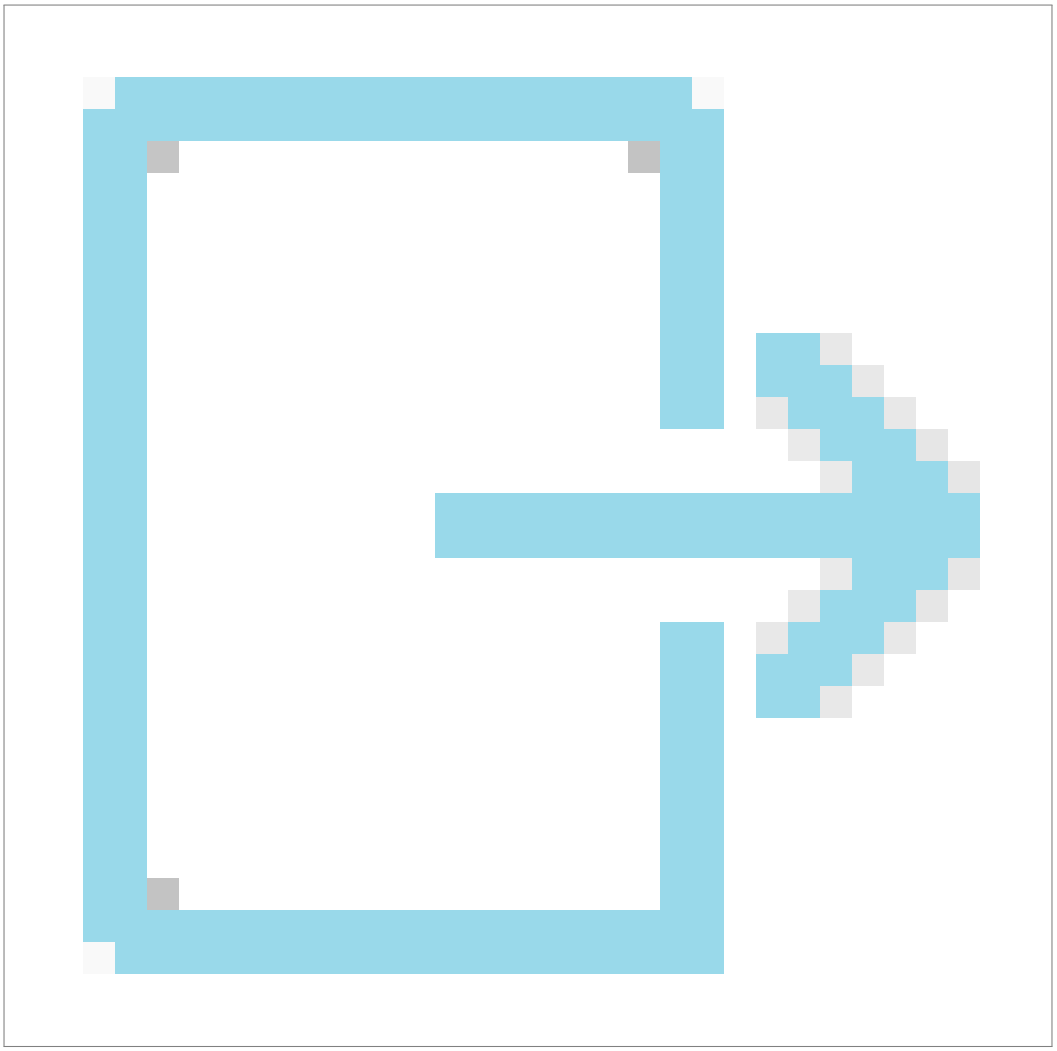
Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

43.14 Absatz 14

Einrichtungen mit kritischen oder erheblichen Auswirkungen aktualisieren ihren Plan zur Aufrechterhaltung des Geschäftsbetriebs immer bei Bedarf und mindestens einmal alle drei Jahre unter Berücksichtigung der Ergebnisse des Tests.



Output

- Test des Business-Continuity-Plans

GOOD TO KNOW

Rekurrenz

3 Jahre

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

43.15 Absatz 15

Werden bei einem Test Mängel im Plan zur Aufrechterhaltung des Geschäftsbetriebs festgestellt, behebt die Einrichtung mit kritischen oder erheblichen Auswirkungen diese Mängel innerhalb von 180 Kalendertagen nach dem Test und führt einen neuen Test durch, um nachzuweisen, dass die Korrekturmaßnahmen wirksam sind.

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

Cybersicherheitsübung auf Unternehmensebene + 180 Tage

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

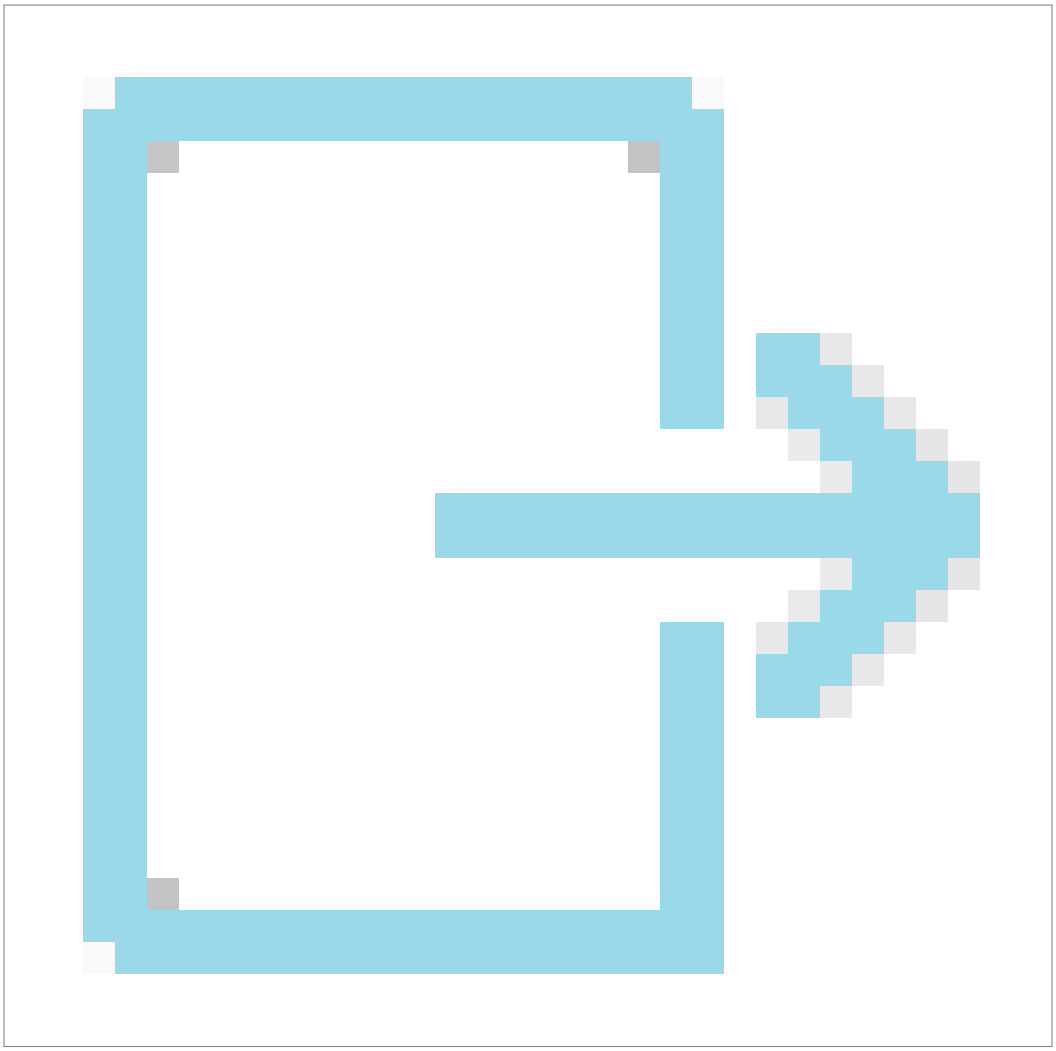
Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

43.16 Absatz 16

Kann eine Einrichtung mit kritischen oder erheblichen Auswirkungen die Mängel nicht innerhalb von 180 Kalendertagen beheben, nimmt sie die Gründe in den Bericht auf, der der für sie zuständigen Behörde gemäß Artikel 27 vorzulegen ist.

Relevante NCCS-Artikel

- Artikel 27



Output

- Risikobewertungsbericht auf Unternehmensebene

A

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Zu informieren: NCA

Chapter 44

Artikel 42. : Cybersicherheits-Frühwarnkapazitäten für den Elektrizitätssektor

44.1 Absatz 1

Die zuständigen Behörden arbeiten mit der ENISA zusammen, um im Rahmen der Unterstützung für die Mitgliedstaaten gemäß Artikel 6 Absätze 2 und 7 der Verordnung (EU) 2019/881 [a] Frühwarnkapazitäten für die Cybersicherheit im Elektrizitätsbereich (Electricity Cybersecurity Early Alert Capabilities, ECEAC) zu entwickeln.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Verantwortlich für die Aktivität: ENISA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENISA, NCA

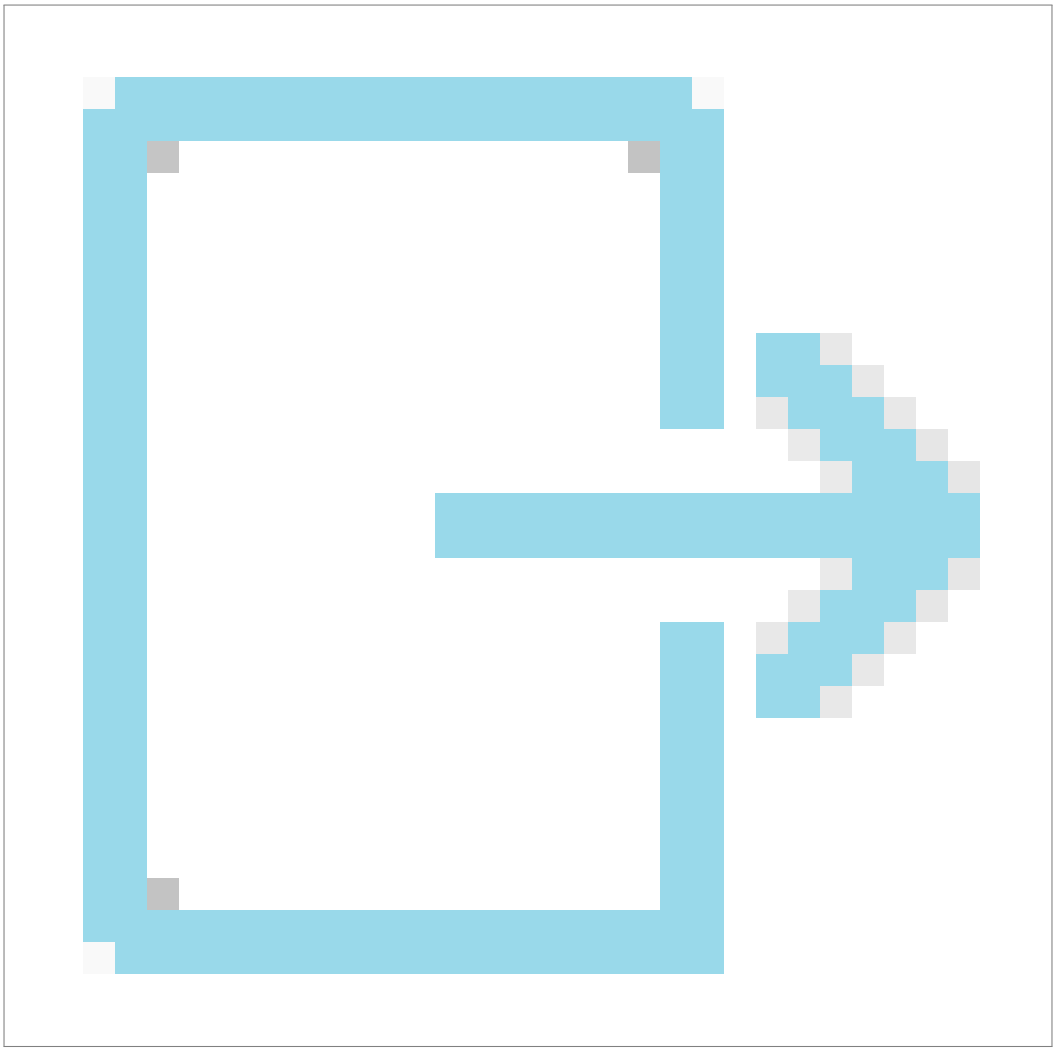
44.2 Absatz 2

Die ECEAC müssen es der ENISA bei der Wahrnehmung der in Artikel 7 Absatz 7 der Verordnung (EU) 2019/881aufgeführten Aufgaben ermöglichen,

a. freiwillig ausgetauschte Informationen einzuholen bei:
    i. CSIRTs, zuständigen Behörden;
    ii. den in Artikel 2 der vorliegenden Verordnung aufgeführten Einrichtungen;
    iii. jeder anderen Einrichtung, die relevante Informationen auf freiwilliger Basis weitergeben möchte;

Relevante NCCS-Artikel

- Artikel 2



Output

- ECEAC

A

Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

44.3 Absatz 2

b) die eingeholten Informationen zu bewerten und zu klassifizieren;

c) die Informationen zu bewerten, zu denen die ENISA Zugang hat, um Risikobedingungen für die Cybersicherheit und relevante Indikatoren für Aspekte grenzüberschreitender Stromflüsse zu ermitteln;

d) Bedingungen und Indikatoren zu ermitteln, die häufig mit Cyberangriffen im Elektrizitätssektor korrelieren;

e) anhand der Bewertung und Ermittlung von Risikofaktoren festzulegen, ob weitere Analysen vorzunehmen und Präventivmaßnahmen zu ergreifen sind;

Verantwortlich für die Aktivität: ENISA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENISA

44.4 Absatz 2

f) die zuständigen Behörden über die ermittelten Risiken und empfohlene Präventionsmaßnahmen für die betreffenden Einrichtungen zu unterrichten;

g) alle in Artikel 2 aufgeführten relevanten Einrichtungen über die Ergebnisse der gemäß den Buchstaben b, c und d dieses Absatzes bewerteten Informationen zu unterrichten;

Relevante NCCS-Artikel

- Artikel 2

Verantwortlich für die Aktivität: ENISA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENISA

Zu informieren: HIE, CIE, ENTSO-E, TSO, ACER, NCA, NRA, RP NCA, CS NCA

44.5 Absatz 2

h) die einschlägigen Informationen regelmäßig in den gemäß Artikel 7 Absatz 6 der Verordnung (EU) 2019/881 [a] erstellten EU-Cybersicherheitslagebericht aufnehmen;

i. soweit möglich, aus den erhobenen Informationen anwendbare Daten abzuleiten, die darauf hindeuten, dass ein potenzieller Sicherheitsverstoß oder Cyberangriff („Kompromittierungsindikatoren“) vorliegt.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Verantwortlich für die Aktivität: ENISA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENISA, EU DSO, CS NCA

44.6 Absatz 3

Die CSIRTs leiten die von der ENISA bereitgestellten Informationen im Rahmen ihrer in Artikel 11 Absatz 3 Buchstabe b der Richtlinie (EU) 2022/2555 [a] festgelegten Aufgaben unverzüglich an die betreffenden Einrichtungen weiter.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_11

Verantwortlich für die Aktivität: CSIRT

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENISA, RP NCA, CSIRT, CS NCA

Zu informieren: HIE, CIE, ENTSO-E, TSO, ACER, EU DSO, NCA, NRA

44.7 Absatz 4

Die ACER überwacht die Wirksamkeit der ECEAC. Die ENISA unterstützt die ACER durch Bereitstellung aller erforderlichen Informationen gemäß Artikel 6 Absatz 2 und Artikel 7 Absatz 1 der Verordnung (EU) 2019/881.

Verantwortlich für die Aktivität: ENISA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENISA

44.8 Absatz 4

Die Analyse dieser Überwachungstätigkeit ist Teil der Überwachung gemäß Artikel 12 [a] der vorliegenden Verordnung.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Relevante NCCS-Artikel

- Artikel 12

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ACER

Zu informieren: ENISA

Chapter 45

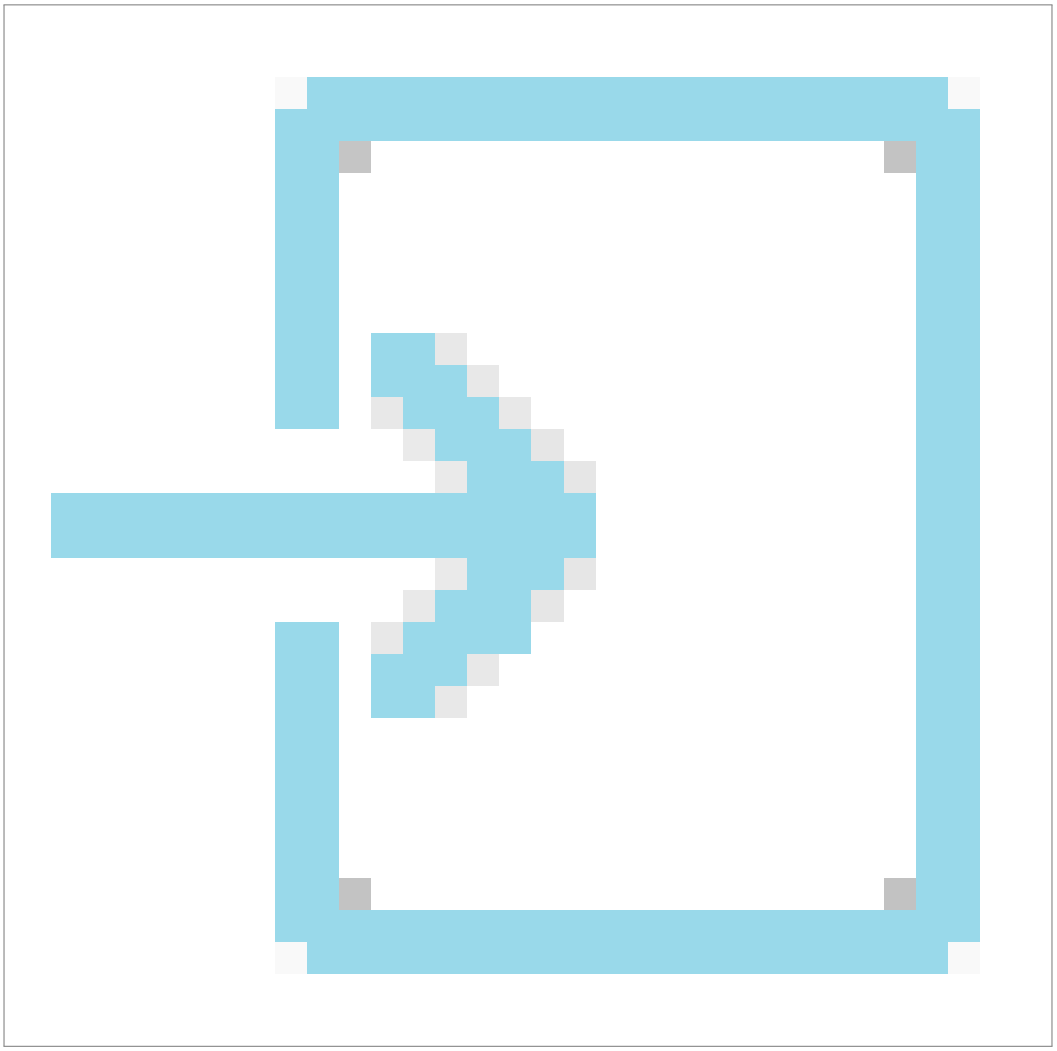
Artikel 43. : Cybersicherheitsübungen auf Ebene der Einrichtungen und der Mitgliedstaaten

45.1 Absatz 1

Bis zum 31. Dezember des Jahres nach der Unterrichtung der Einrichtungen mit kritischen Auswirkungen und danach alle drei Jahre führt jede Einrichtung mit kritischen Auswirkungen eine Cybersicherheitsübung durch, die ein oder mehrere Szenarien mit Cyberangriffen umfasst, die sich direkt oder indirekt auf grenzüberschreitende Stromflüsse auswirken und mit den gemäß den Artikeln 20 und 27 bei den Cybersicherheitsrisikobewertungen auf Ebene der Mitgliedstaaten und Einrichtungen ermittelten Risiken im Zusammenhang stehen.

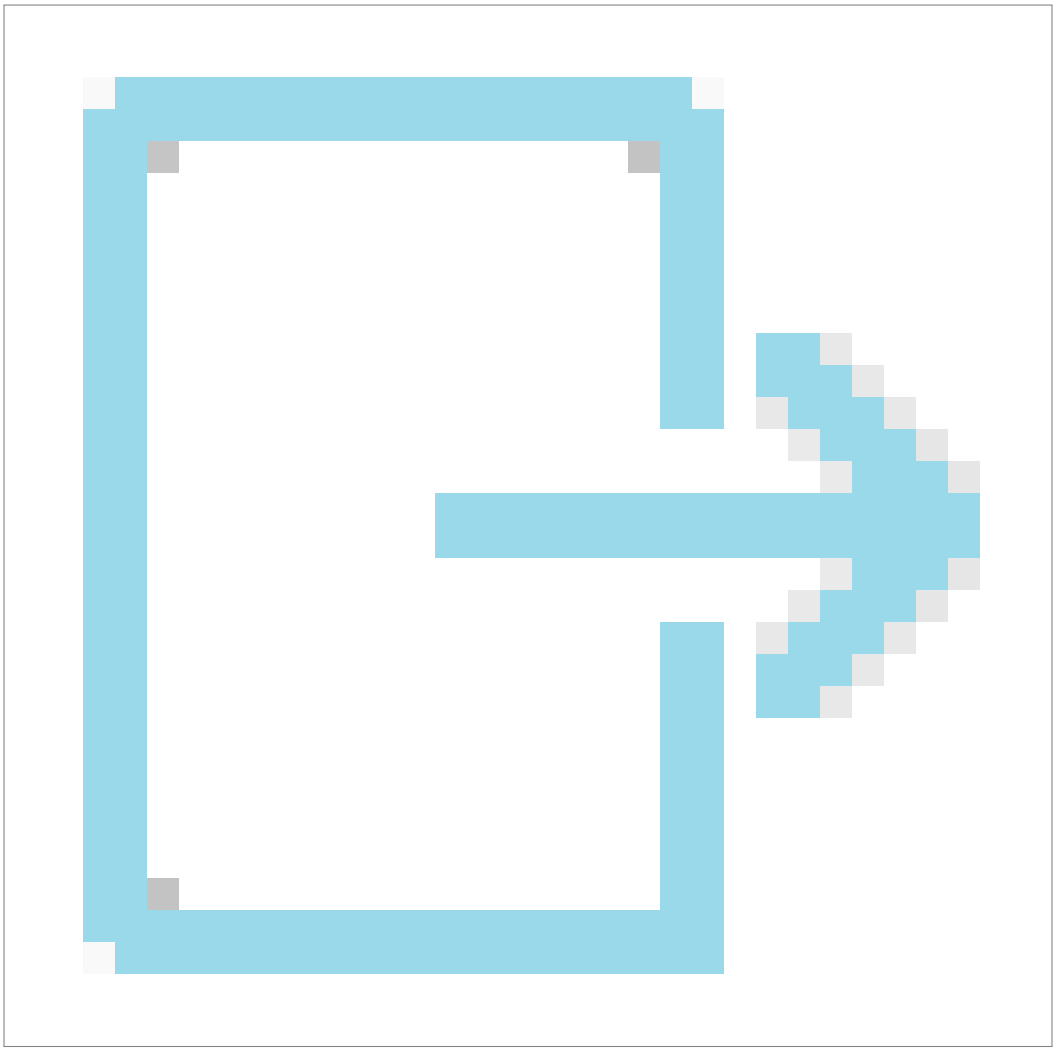
Relevante NCCS-Artikel

- Artikel 20
- Artikel 27



Input

- Risikobewertung auf Ebene der Mitgliedstaaten
- Risikobewertung auf Unternehmensebene



Output

- Übung auf Unternehmensebene

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

Bis zum 31. Dezember 2029

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, TSO

45.2 Absatz 2

Abweichend von Absatz 1 kann die RP-NCA nach Konsultation der zuständigen Behörde und der gemäß Artikel 9 der Richtlinie (EU) 2022/2555 [a] benannten oder eingerichteten zuständigen Behörde für das Cyberkrisenmanagement beschließen, anstelle der Cybersicherheitsübung auf Ebene der Einrichtung eine Cybersicherheitsübung gemäß Absatz 1 auf Ebene des Mitgliedstaats durchzuführen. In diesem Zusammenhang unterrichtet die zuständige Behörde

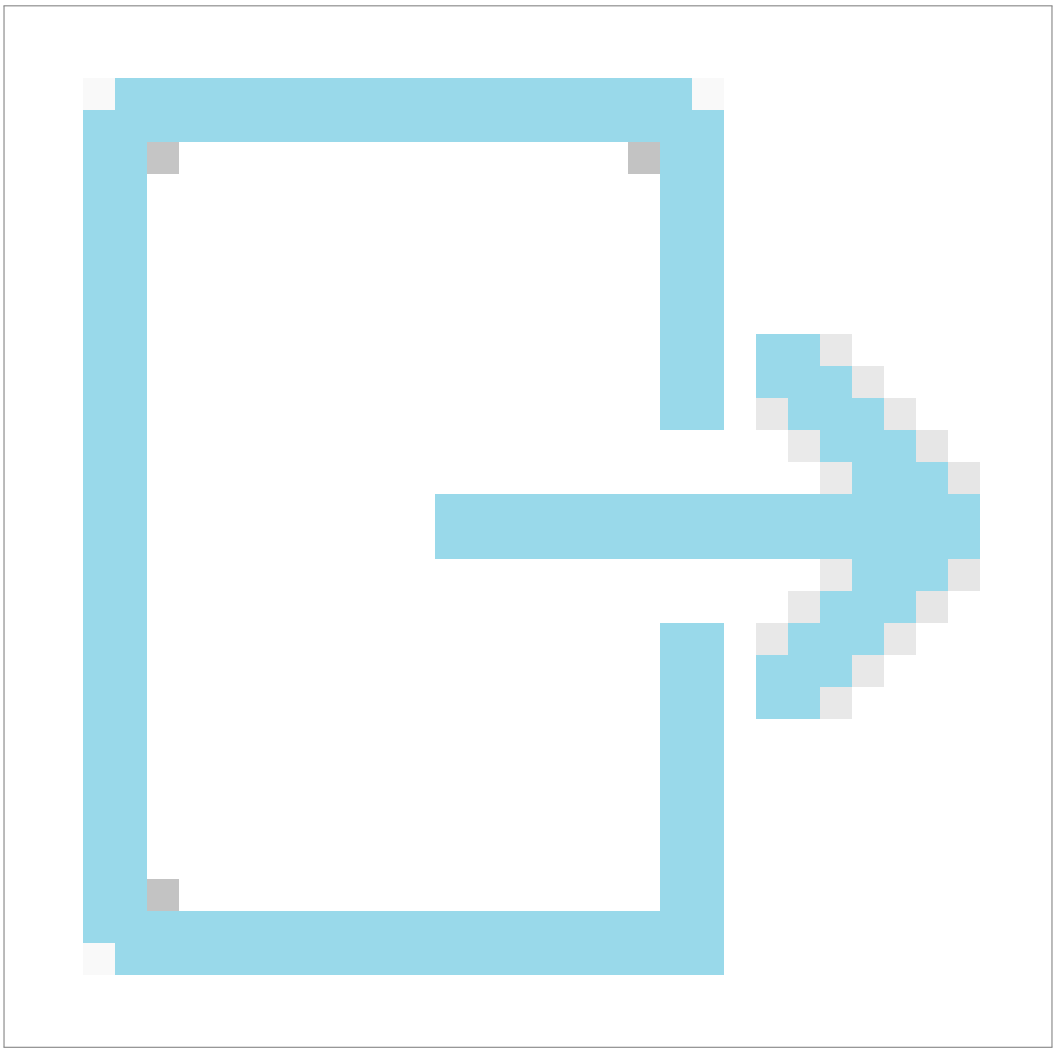
a. alle Einrichtungen mit kritischen Auswirkungen ihres Mitgliedstaats, die NRB, die CSIRTs und die CS-NCA bis spätestens 30. Juni des Jahres, das der Cybersicherheitsübung auf Ebene der Einrichtungen vorausgeht;

b. jede Einrichtung, die an der Cybersicherheitsübung auf Ebene des Mitgliedstaats teilnehmen muss, spätestens sechs Monate vor der Übung.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9

Relevante NCCS-Artikel

- Artikel 43 (1)



Output

- Übung auf Ebene der Mitgliedstaaten

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

6 Monate vor der Übung auf nationaler Ebene

Verantwortlich für die Aktivität: RP NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA, RP NCA

Zu konsultieren: CS NCA

Zu informieren: CIE

45.3 Absatz 3

Die RP-NCA organisiert mit technischer Unterstützung ihrer CSIRTs die in Absatz 2 beschriebene Cybersicherheitsübung auf Ebene des Mitgliedstaats getrennt oder zusammen mit einer anderen Cybersicherheitsübung in diesem Mitgliedstaat. Um diese Übungen zusammenfassen zu können, kann die RP-NCA die in Absatz 1 genannte Cybersicherheitsübung auf Ebene des Mitgliedstaats um ein Jahr verschieben

Relevante NCCS-Artikel

- Artikel 43 (2)
- Artikel 43 (1)

Verantwortlich für die Aktivität: RP NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, TSO, RP NCA, CSIRT

45.4 Absatz 4

Die Cybersicherheitsübungen auf Ebene der Einrichtungen und der Mitgliedstaaten müssen mit den nationalen Rahmen für das Cybersicherheitskrisenmanagement gemäß Artikel 9 Absatz 4 Buchstabe d der Richtlinie (EU) 2022/2555 [a] im Einklang stehen.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9

Verantwortlich für die Aktivität: CIE, TSO, RP NCA

Beteiligte Stakeholder:

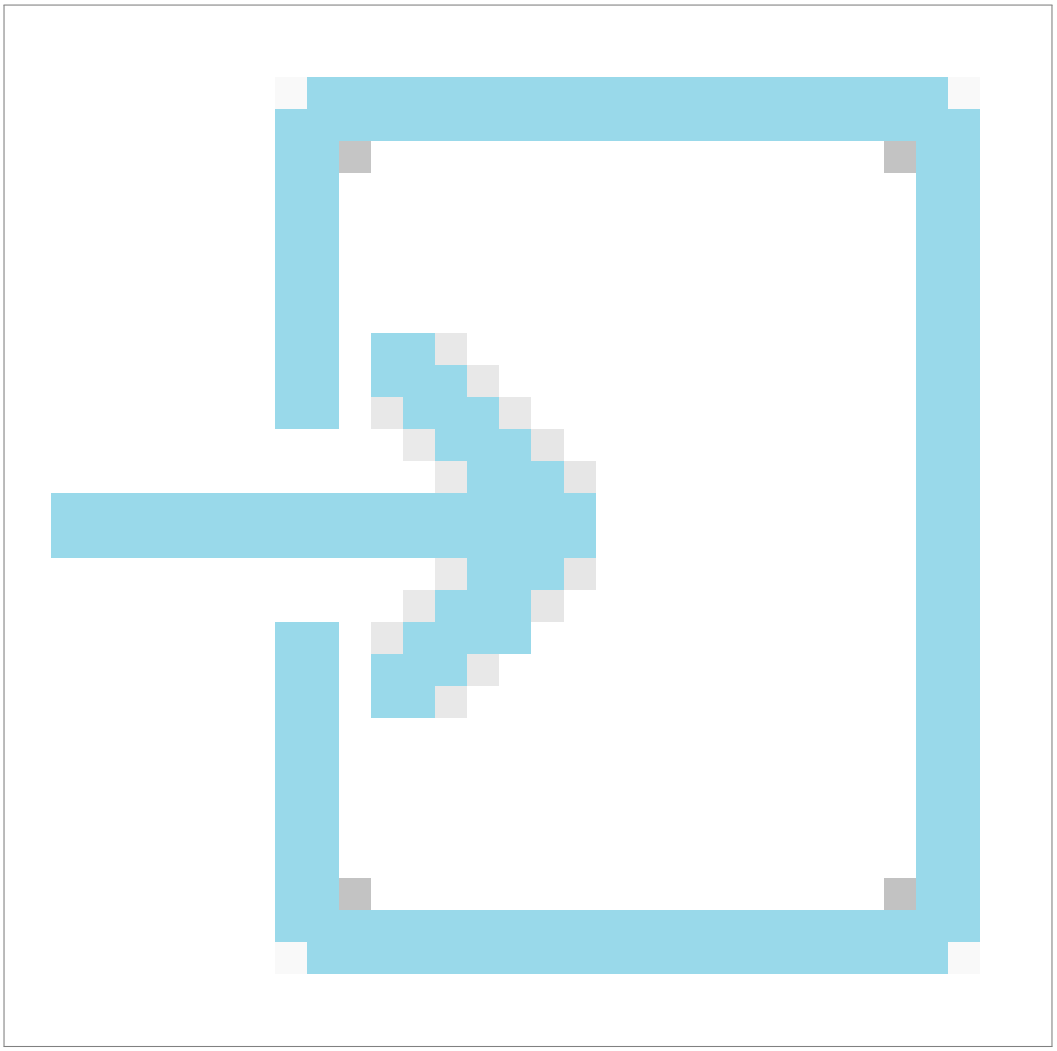
Beteiligt an der Aufgabenausführung: CIE, TSO, RP NCA

45.5 Absatz 5

Bis zum 31 Dezember 2026 und danach alle drei Jahre stellt ENTSO-E in Zusammenarbeit mit der EU-VNBO ein Muster für das Übungsszenario für die Durchführung der in Absatz 1 genannten Cybersicherheitsübungen auf Ebene der Einrichtungen und der Mitgliedstaaten bereit. Das Muster muss den Ergebnissen der jüngsten Bewertung des Cybersicherheit-srisikos auf Ebene der Einrichtungen und der Mitgliedstaaten Rechnung tragen und zentrale Leistungskriterien enthalten. ENTSO-E und die EU-VNBO beziehen die ACER und die ENISA bei der Entwicklung dieses Musters ein.

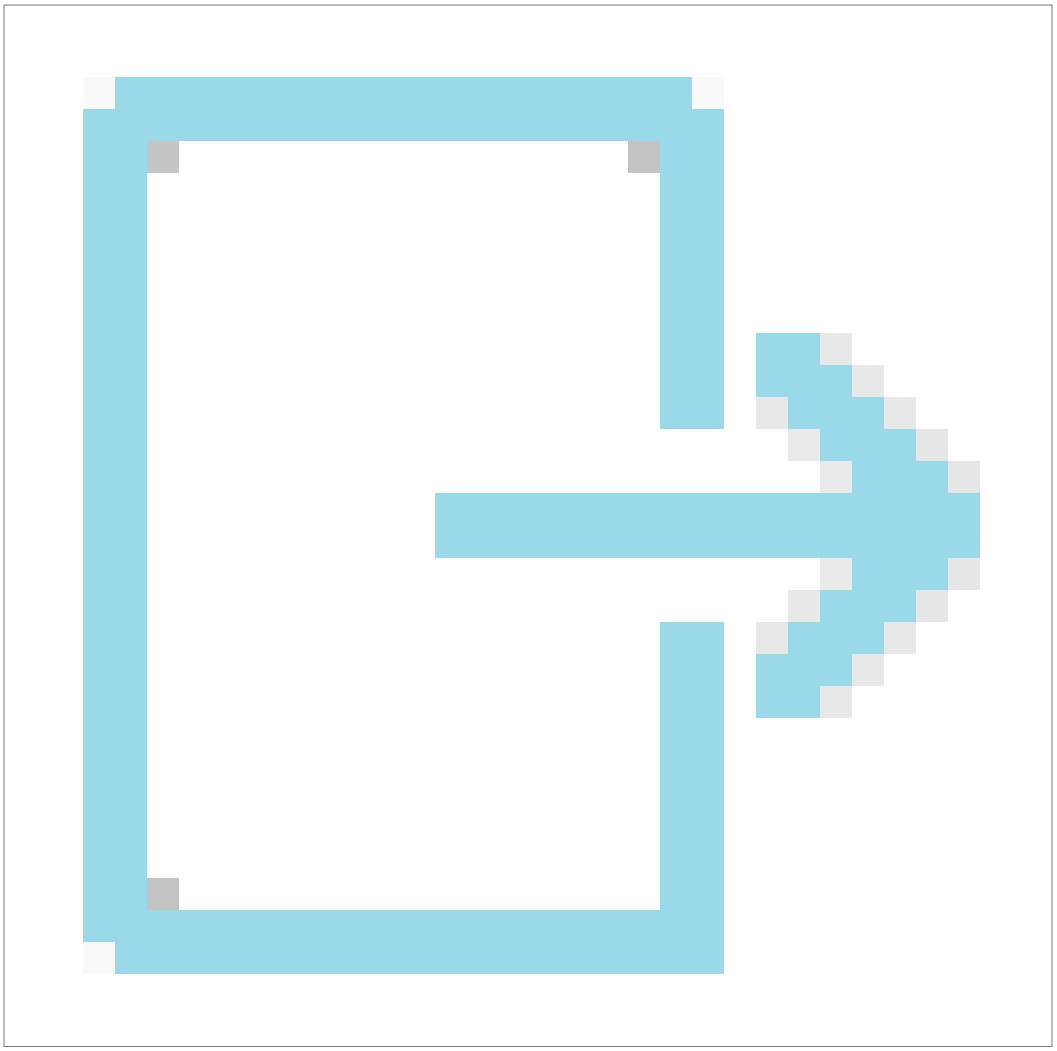
Relevante NCCS-Artikel

- Artikel 43 (1)



Input

- Risikobewertungsbericht auf Ebene der Mitgliedstaaten
- Erfolgskriterien



Output

- Vorlage für Übungen auf Mitgliedstaatenebene
- Vorlage für Übungen auf Unternehmensebene

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

Bis zum 31. Dezember 2026

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, ACER, ENISA, EU DSO

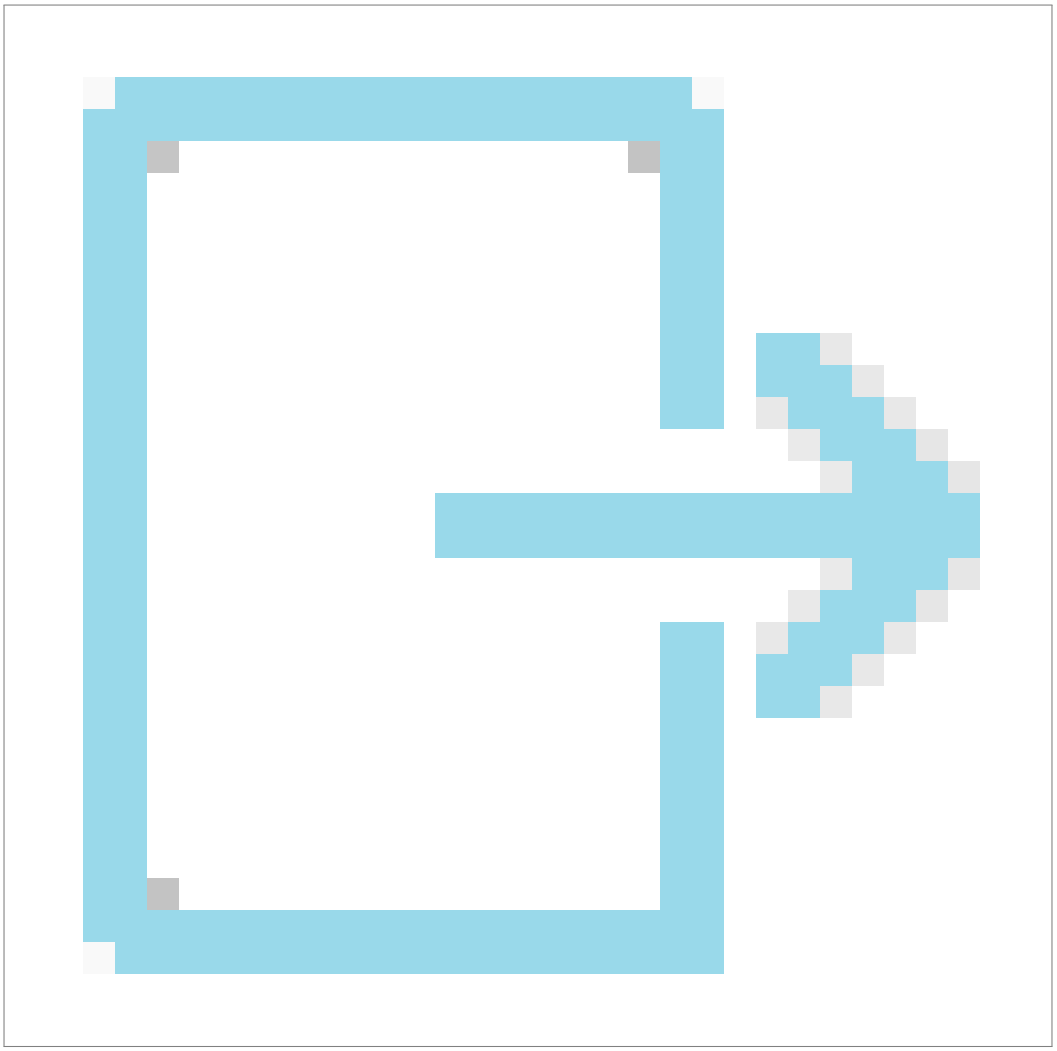
Zu informieren: CIE

Chapter 46

Artikel 44. : Regionale oder überregionale Cybersicherheitsübungen

46.1 Absatz 1

Bis zum 31 Dezember 2029 und danach alle drei Jahre organisiert ENTSO-E in Zusammenarbeit mit der EU-VNBO in jeder Netzbetriebsregion eine regionale Cybersicherheitsübung. An der regionalen Cybersicherheitsübung nehmen die Einrichtungen mit kritischen Auswirkungen teil. ENTSO-E kann in Zusammenarbeit mit der EU-VNBO innerhalb desselben Zeitrahmens anstelle einer regionalen Cybersicherheitsübung eine überregionale Cybersicherheitsübung in mehr als einer Netzbetriebsregion organisieren. Bei der Übung sollten andere vorhandene Risikobewertungen und Szenarien für die Cybersicherheit, die auf Unionsebene entwickelt wurden, berücksichtigt werden.



Output

- Regionale Cybersicherheitsübung

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

Bis zum 31. Dezember 2029

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, ENTSO-E, TSO, EU DSO

46.2 Absatz 2

Die ENISA unterstützt ENTSO-E und die EU-VNBO bei der Vorbereitung und Organisation der Cybersicherheitsübung auf regionaler oder überregionaler Ebene.

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, ENISA, EU DSO

46.3 Absatz 3

ENTSO-E unterrichtet in Abstimmung mit der EU-VNBO die Einrichtungen mit kritischen Auswirkungen, die an der regionalen oder überregionalen Cybersicherheitsübung teilnehmen müssen, sechs Monate vor der Übung.

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

6 Monate vor der Übung auf regionaler Ebene

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu informieren: CIE

46.4 Absatz 4

Der Organisator einer regelmäßigen Cybersicherheitsübung auf Unionsebene gemäß Artikel 7 Absatz 5 der Verordnung (EU) 2019/881 [a] oder einer obligatorischen Cybersicherheitsübung in Bezug auf den Elektrizitätssektor innerhalb desselben geografischen Perimeters kann ENTSO-E und die EU-VNBO zur Teilnahme einladen. In diesen Fällen gilt die Verpflichtung nach Absatz 1 nicht, sofern alle Einrichtungen mit kritischen Auswirkungen in der Netzbetriebsregion an derselben Übung teilnehmen.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Relevante NCCS-Artikel

- Artikel 44 (1)

Verantwortlich für die Aktivität: ENISA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, ENTSO-E, TSO, ENISA, EU DSO

46.5 Absatz 5

Nehmen ENTSO-E und die EU-VNBO an einer Cybersicherheitsübung gemäß Absatz 4 teil, so können sie die in Absatz 1 genannte regionale oder überregionale Cybersicherheitsübung um ein Jahr verschieben.

Relevante NCCS-Artikel

- Artikel 44 (1)
- Artikel 44 (4)

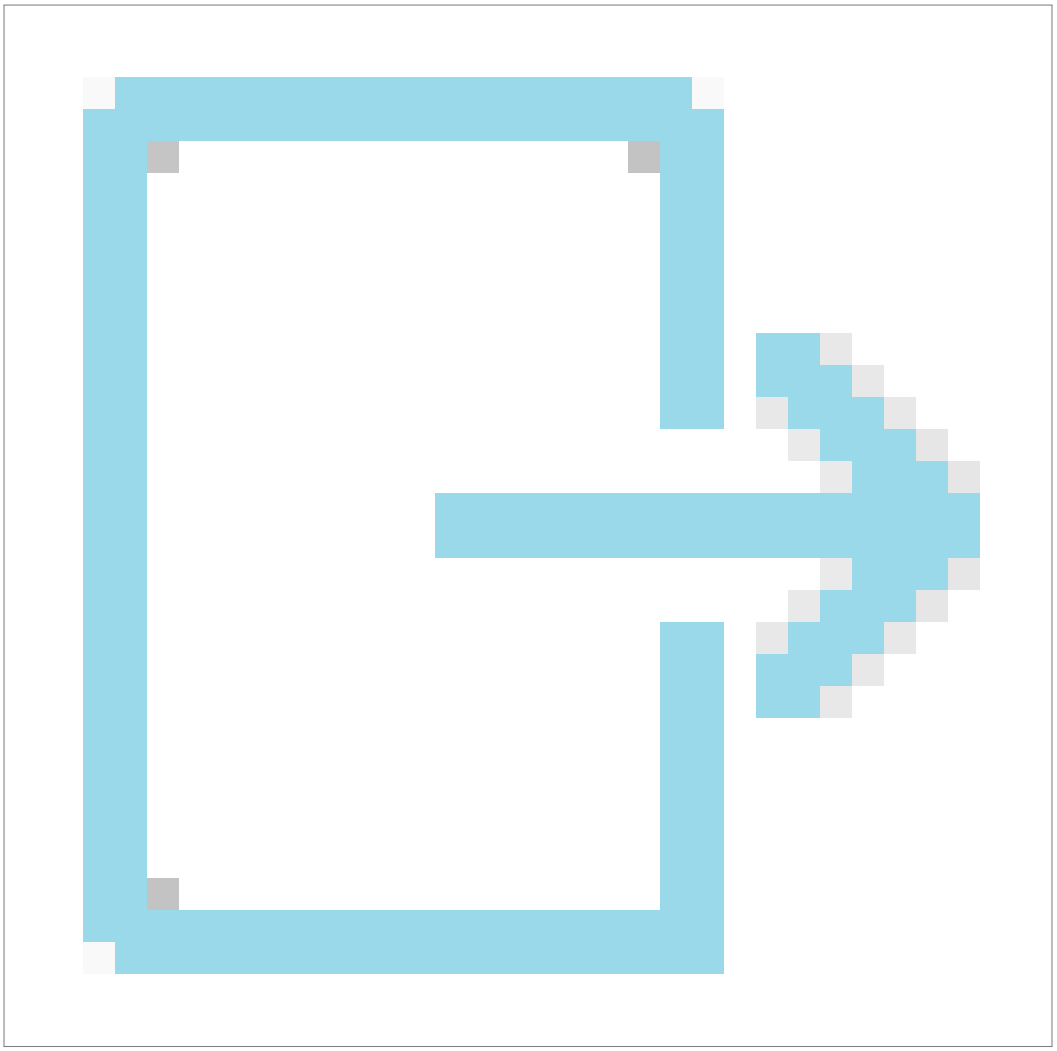
Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, ENTSO-E, TSO, EU DSO

46.6 Absatz 6

Bis zum 31 Dezember 2027 und danach alle drei Jahre stellt ENTSO-E in Abstimmung mit der EU-VNBO ein Muster für die Durchführung der regionalen und überregionalen Cybersicherheitsübungen bereit. Das Muster muss den Ergebnissen der jüngsten Bewertung des Cybersicherheitsrisikos auf regionaler Ebene Rechnung tragen und zentrale Leistungskriterien enthalten. In Bezug auf die Organisation und Durchführung der regionalen und überregionalen Cybersicherheitsübungen konsultiert ENTSO-E die Kommission und kann den Rat der ACER, der ENISA und der Gemeinsamen Forschungsstelle einholen.



Output

- Übungsvorlage für die regionale Ebene

GOOD TO KNOW

Rekurrenz

3 Jahre

GOOD TO KNOW

Zeitpunkt

Bis zum 31. Dezember 2027

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu konsultieren: EC, ACER, ENISA

Chapter 47

Artikel 45. : Ergebnisse von Cybersicherheitsübungen auf regionaler oder überregionaler Ebene oder auf der Ebene von Einrichtungen oder Mitgliedstaaten

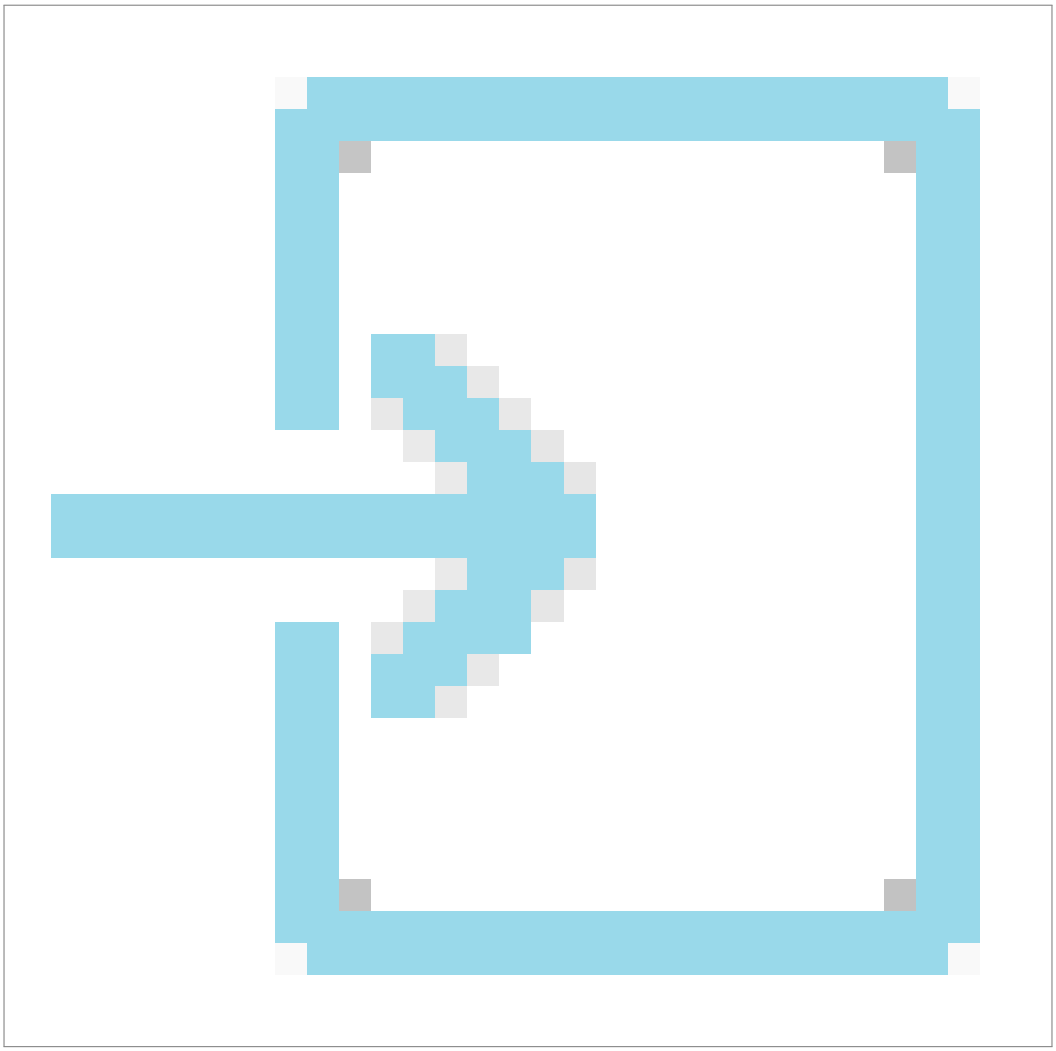
47.1 Absatz 1

Auf Ersuchen einer Einrichtung mit kritischen Auswirkungen nehmen die Anbieter kritischer Dienste an den in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen teil, wenn sie Dienste für die Einrichtung mit kritischen Auswirkungen in dem Bereich erbringen, der dem Anwendungsbereich der betreffenden Cybersicherheitsübung entspricht.

Relevante NCCS-Artikel

- Artikel 43 (1)
- Artikel 43 (2)

- Artikel 44 (1)



Input

- Unionweite Prozesse mit erheblicher und kritischer Auswirkung

A

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, ENTSO-E, TSO, ENISA, Critical ICT

47.2 Absatz 2

Die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen analysieren und beenden die einschlägigen Cybersicherheitsübungen mit einem an alle Teilnehmer gerichteten Bericht, in dem die gewonnenen Erkenntnisse zusammengefasst werden, wobei sie bei der ENISA gemäß Artikel 7 Absatz 5 der Verordnung (EU) 2019/881 [a] Rat einholen können. Der Bericht muss Folgendes enthalten:

a. die Übungsszenarien, Sitzungsberichte, wichtigsten Standpunkte, Erfolge und Erkenntnisse auf allen Ebenen der Elektrizitätswertschöpfungskette;

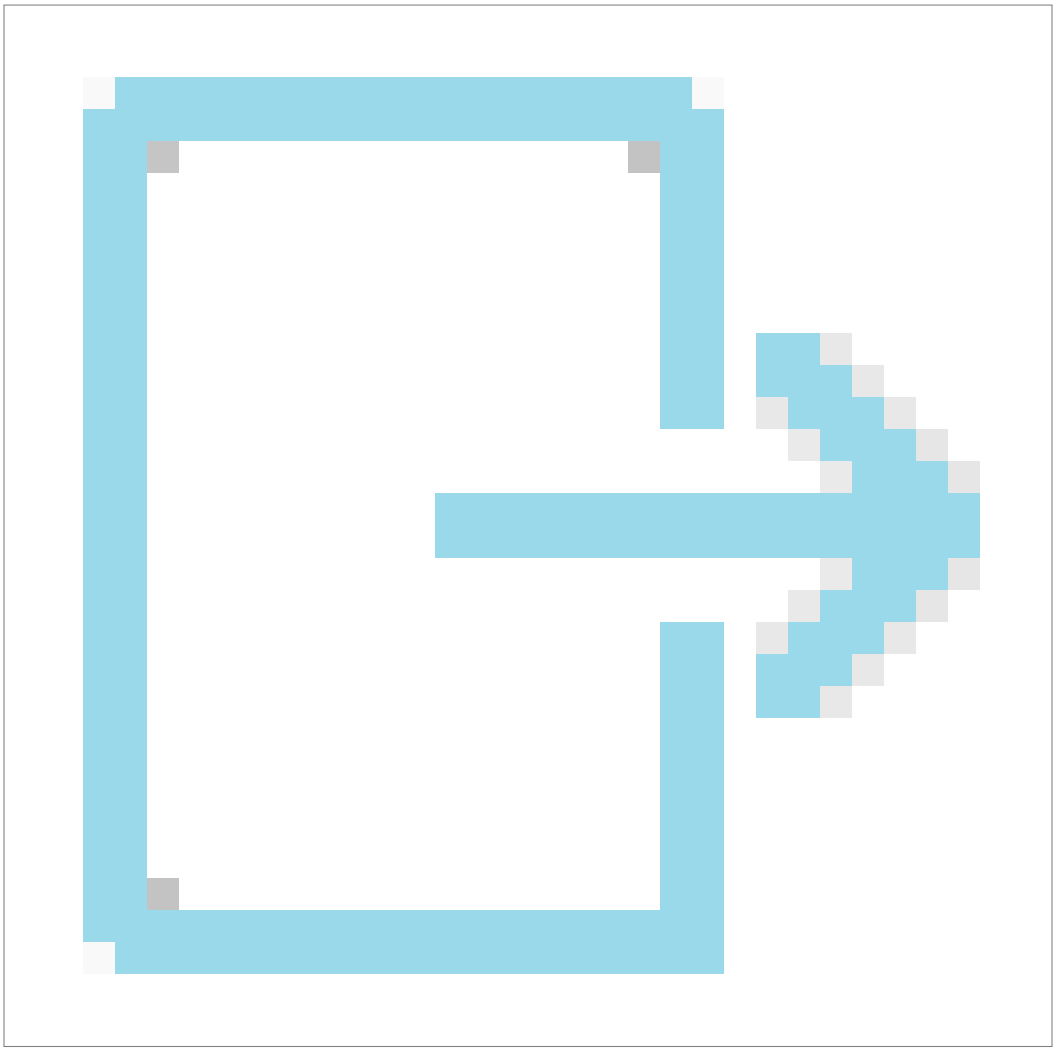
b. die Angabe, ob die wichtigsten Leistungskriterien erfüllt wurden;

c. eine Liste von Empfehlungen für Einrichtungen, die an der einschlägigen Cybersicherheitsübung teilnehmen, in Bezug auf eine Korrektur, Anpassung oder Änderung von cybersicherheitskrisenprozessen, -verfahren, zugehörigen Governance-Modellen und etwaigen bestehenden vertraglichen Verpflichtungen mit Anbietern kritischer Dienste.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Relevante NCCS-Artikel

- Artikel 43 (1)
- Artikel 43 (2)
- Artikel 44 (1)



Output

- Bericht über Cybersicherheitsübung

A

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

R

Beteiligt an der Aufgabenausführung: CIE, ENTSO-E, TSO

Zu konsultieren: ENISA

Zu informieren: NCA

47.3 Absatz 3

Auf Ersuchen des CSIRTs-Netzes, der NIS-Kooperationsgruppe oder des EU-CyCLONe leiten die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen die Ergebnisse der einschlägigen Cybersicherheitsübung weiter. Die Organisatoren teilen jeder an den Übungen teilnehmenden Einrichtung die in Absatz 2 Buchstaben a und b dieses Artikels genannten Informationen mit. Die Organisatoren übermitteln die Liste der in Absatz 2 Buchstabe c genannten Empfehlungen ausschließlich an die Einrichtungen, an die sich die Empfehlungen richten.

Relevante NCCS-Artikel

- Artikel 43 (1)
- Artikel 43 (2)
- Artikel 44 (1)
- Artikel 45 (2)

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, ENTSO-E, TSO, NCA, NIS CG, CSIRT

47.4 Absatz 4

Die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen treffen mit den an den Übungen teilnehmenden Einrichtungen regelmäßig Folgemaßnahmen in Bezug auf die Umsetzung der Empfehlungen gemäß Absatz 2 Buchstabe c des vorliegenden Artikels.

Relevante NCCS-Artikel

- Artikel 43 (1)
- Artikel 43 (2)
- Artikel 44 (1)
- Artikel 45 (2)

Verantwortlich für die Aktivität: CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: CIE, ENTSO-E, TSO

Chapter 48

Artikel 46. : Grundsätze für den Schutz ausgetauschter Informationen

48.1 Absatz 1

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass die im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen nur nach dem Grundsatz „Kenntnis nur, wenn nötig“ und im Einklang mit den einschlägigen Vorschriften der Union und der Mitgliedstaaten über die Informationssicherheit zugänglich sind.

Relevante NCCS-Artikel

- Artikel 2 (1)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

48.2 Absatz 2

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass die im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen während des gesamten Lebenszyklus dieser Informationen entsprechend behandelt und nachverfolgt werden und dass sie am Ende ihres Lebenszyklus erst dann freigegeben werden, wenn sie anonymisiert wurden.

Relevante NCCS-Artikel

- Artikel 2 (1)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

48.3 Absatz 3

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass alle erforderlichen Schutzmaßnahmen organisatorischer und technischer Art getroffen werden, um die Vertraulichkeit, Integrität, Verfügbarkeit und Nichtabstreitbarkeit der im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen, unabhängig von den dabei genutzten Mitteln, zu wahren und zu schützen. Die Schutzmaßnahmen müssen

a. verhältnismäßig sein;

b. Cybersicherheitsrisiken im Zusammenhang mit bekannten früheren und sich abzeichnenden Bedrohungen Rechnung tragen, denen die Informationen im Zusammenhang mit dieser Verordnung ausgesetzt sein könnten;

c. soweit möglich auf nationalen, europäischen oder internationalen Normen und bewährten Verfahren beruhen;

d. dokumentiert werden.

Relevante NCCS-Artikel

- Artikel 2 (1)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

48.4 Absatz 4

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass jede Person, der Zugang zu den im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen gewährt wird, über die auf Ebene der Einrichtungen geltenden Sicherheitsvorschriften sowie über die für den Schutz von Informationen relevanten Maßnahmen und Verfahren unterrichtet wird. Die Einrichtungen stellen sicher, dass die betroffene Person die Zuständigkeit anerkennt, die Informationen nach den in der Unterrichtung erteilten Anweisungen zu schützen.

Relevante NCCS-Artikel

- Artikel 2 (1)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

48.5 Absatz 5

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass der Zugang zu den im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen auf Personen beschränkt wird,

a. die aufgrund ihrer Funktionen, und beschränkt auf die Ausführung der ihnen übertrage-

nen Aufgaben, zum Zugang zu diesen Informationen berechtigt sind;

b. in Bezug auf die die Einrichtung ethische Grundsätze und Integritätsgrundsätze prüfen konnte und für die es keine Hinweise auf ein negatives Ergebnis einer Zuverlässigkeitsüberprüfung gibt, mit der die Zuverlässigkeit der Person im Einklang mit bewährten Verfahren und den Standardsicherheitsanforderungen der Einrichtung und erforderlichenfalls mit den nationalen Gesetzen und Vorschriften bewertet wurde.

Relevante NCCS-Artikel

- Artikel 2 (1)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

48.6 Absatz 6

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen bedürfen der schriftlichen Zustimmung der natürlichen oder juristischen Person, die die Informationen ursprünglich erstellt oder bereitgestellt hat, bevor sie diese Informationen an Dritte weitergeben, die nicht in den Anwendungsbereich dieser Verordnung fallen.

Relevante NCCS-Artikel

- Artikel 2 (1)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

48.7 Absatz 7

Eine in Artikel 2 Absatz 1 aufgeführte Einrichtung kann der Ansicht sein, dass diese Informationen ohne Einhaltung der Absätze 1 und 4 des vorliegenden Artikels weitergegeben werden müssen, um eine zeitgleich auftretende Stromversorgungskrise mit einer zugrunde liegenden Cybersicherheitsursache oder eine grenzüberschreitende Krise innerhalb der Union in einem anderen Sektor zu verhindern. In diesem Fall

a. konsultiert sie die zuständige Behörde und kann von ihr zur Weitergabe dieser Informationen ermächtigt werden;

b. anonymisiert sie diese Informationen, ohne dass die Elemente verloren gehen, die erforderlich sind, um die Öffentlichkeit über ein unmittelbares und ernstes Risiko für grenzüberschreitende Stromflüsse und mögliche Abhilfemaßnahmen zu informieren;

c. schützt sie die Identität des Urhebers und der Einrichtungen, die diese Informationen im Rahmen dieser Verordnung verarbeitet haben.

Relevante NCCS-Artikel

- Artikel 2 (1)
- Artikel 46 (1)
- Artikel 46 (4)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Zu konsultieren: NCA

48.8 Absatz 8

Abweichend von Absatz 6 des vorliegenden Artikels können die zuständigen Behörden Informationen, die im Rahmen dieser Verordnung bereitgestellt, empfangen, ausgetauscht oder übermittelt werden, einem nicht in Artikel 2 Absatz 1 aufgeführten Dritten bereitstellen, ohne dass der Urheber der Informationen schriftlich zugestimmt hat, müssen diesen jedoch so bald wie möglich davon in Kenntnis setzen. Bevor die betreffende zuständige Behörde Informationen, die im Rahmen dieser Verordnung bereitgestellt, empfangen, ausgetauscht oder übermittelt wurden, einem nicht in Artikel 2 Absatz 1 aufgeführten Dritten offenlegt, muss sie in angemessenem Umfang sicherstellen, dass der betreffende Dritte Kenntnis von den geltenden Sicherheitsvorschriften hat, und hinreichende Gewähr dafür er-

halten, dass der betreffende Dritte die empfangenen Informationen gemäß den Absätzen 1 bis 5 des vorliegenden Artikels schützen kann. Die zuständige Behörde anonymisiert diese Informationen, ohne dass die Elemente verloren gehen, die erforderlich sind, um die Öffentlichkeit über ein unmittelbares und ernstes Risiko für grenzüberschreitende Stromflüsse und mögliche Abhilfemaßnahmen zu informieren, und schützt die Identität des Urhebers der Informationen. In diesem Fall schützt der nicht in Artikel 2 Absatz 1 aufgeführte Dritte die empfangenen Informationen gemäß den auf Ebene der Einrichtung bereits geltenden Bestimmungen oder, wenn dies nicht möglich ist, nach den Bestimmungen und Anweisungen der jeweils zuständigen Behörde.

Relevante NCCS-Artikel

- Artikel 46 (6)
- Artikel 2 (1)
- Artikel 46 (1)
- Artikel 46 (2)
- Artikel 46 (3)
- Artikel 46 (4)
- Artikel 46 (5)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

48.9 Absatz 9

Dieser Artikel gilt nicht für Einrichtungen, die nicht in Artikel 2 Absatz 1 aufgeführt sind, wenn sie Informationen gemäß Absatz 6 des vorliegenden Artikels erhalten. In diesem Fall ist Absatz 7 anzuwenden, oder die zuständige Behörde kann dieser Einrichtung schriftliche Bestimmungen bereitstellen, die in Fällen anzuwenden sind, in denen Informationen gemäß dieser Verordnung eingehen.

Relevante NCCS-Artikel

- Artikel 2 (1)
- Artikel 46 (6)
- Artikel 46 (7)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Chapter 49

Artikel 47. : Vertraulichkeit von Informationen

49.1 Absatz 1

Alle gemäß dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen unterliegen dem Berufsgeheimnis gemäß den Absätzen 2 bis 5 dieses Artikels sowie den Anforderungen aus Artikel 65 der Verordnung (EU) 2019/943. [a] Alle von den in Artikel 2 dieser Verordnung aufgeführten Einrichtungen für die Zwecke der Durchführung dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen werden unter Berücksichtigung des vom Urheber angewandten Vertraulichkeitsgrads der Informationen geschützt.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e5115-54-1

Relevante NCCS-Artikel

- Artikel 47 (2)
- Artikel 47 (3)
- Artikel 47 (4)
- Artikel 47 (5)

- Artikel 2

Verantwortlich für die Aktivität: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

49.2 Absatz 2

Die in Artikel 2 aufgeführten Einrichtungen unterliegen der Verpflichtung zur Wahrung des Berufsgeheimnisses.

Relevante NCCS-Artikel

- Artikel 2

Verantwortlich für die Aktivität: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

49.3 Absatz 3

Die CS-NCAs, die NRB, die RP-NCA und die CSIRTs tauschen alle für die Wahrnehmung ihrer Aufgaben erforderlichen Informationen aus.

Verantwortlich für die Aktivität: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

49.4 Absatz 4

Alle von den in Artikel 2 Absatz 1 aufgeführten Einrichtungen für die Zwecke der Durchführung von Artikel 23 empfangenen, ausgetauschten oder übermittelten Informationen werden anonymisiert und aggregiert.

Relevante NCCS-Artikel

- Artikel 2 (1)
- Artikel 23

Verantwortlich für die Aktivität: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, CS NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, CS NCA

49.5 Absatz 5

Informationen, die eine dieser Verordnung unterliegende Einrichtung oder Behörde im Rahmen der Erfüllung ihrer Pflichten erhält, dürfen an keine andere Einrichtung oder Behörde weitergegeben werden; davon unberührt bleiben Fälle, die unter das nationale Recht, andere Bestimmungen dieser Verordnung oder andere einschlägige Unionsvorschriften fallen.

Verantwortlich für die Aktivität: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

49.6 Absatz 6

Unbeschadet des nationalen Rechts und des Unionsrechts dürfen Behörden, Einrichtungen oder natürliche Personen, die Informationen gemäß dieser Verordnung erhalten, diese für keinen anderen Zweck als für die Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung verwenden.

Verantwortlich für die Aktivität: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Beteiligte Stakeholder:

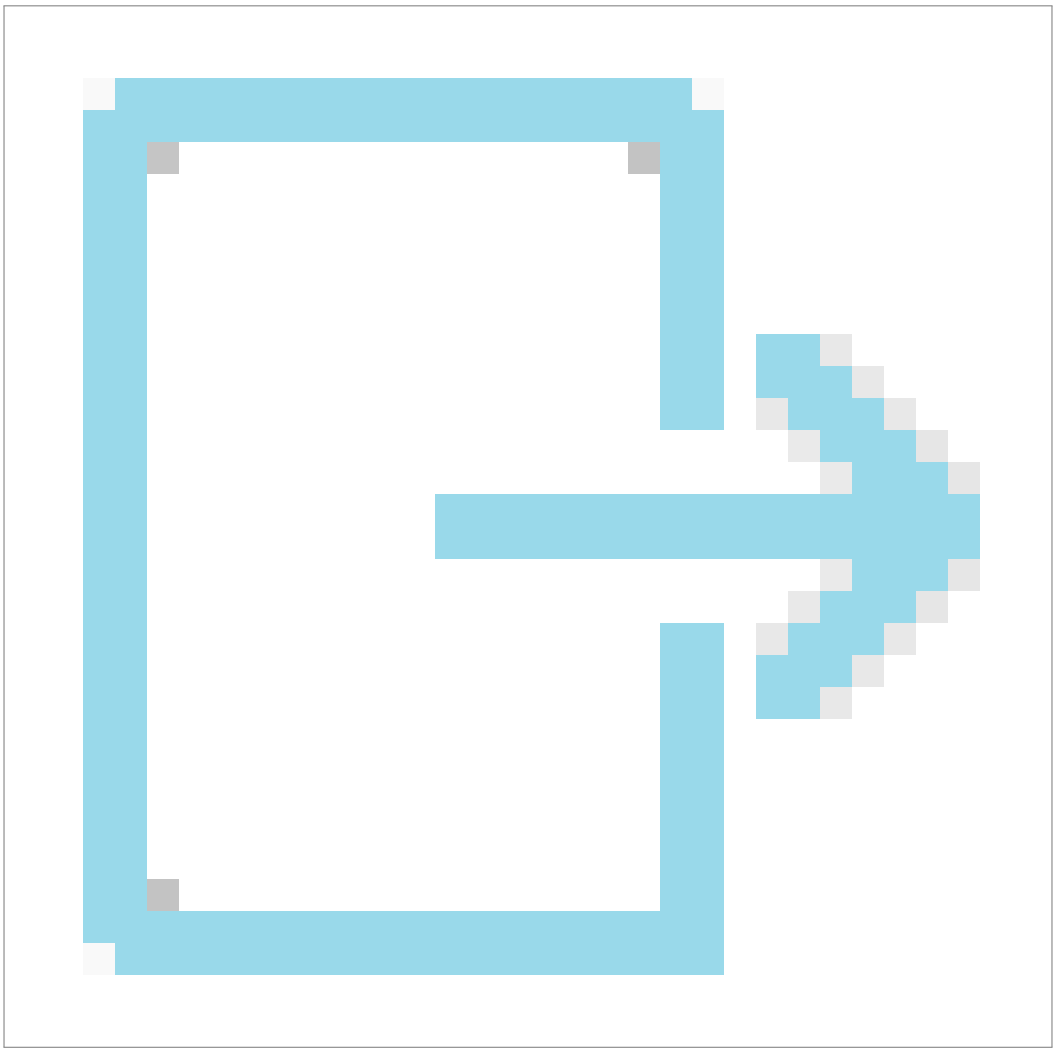
Beteiligt an der Aufgabenausführung: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

49.7 Absatz 7

Die ACER gibt nach Konsultation der ENISA, aller zuständigen Behörden, von ENTSO-E und der EU-VNBO bis zum 13 Juni 2025 Leitlinien für alle in Artikel 2 Absatz 1 aufgeführten Einrichtungen zu Mechanismen für den Austausch von Informationen und insbesondere zu den geplanten Kommunikationsflüssen und Methoden zur Anonymisierung und Aggregierung von Informationen für die Zwecke der Durchführung des vorliegenden Artikels heraus.

Relevante NCCS-Artikel

- Artikel 2 (1)



Output

- Anleitung zum Informationsfluss

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Juni 2025

Verantwortlich für die Aktivität: ACER

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ACER

Zu konsultieren: ENTSO-E, ENISA, EU DSO

Zu informieren: HIE, CIE, NCA, NRA, RP NCA, CS NCA

49.8 Absatz 8

Nach nationalem Recht oder Unionsrecht vertrauliche Informationen werden nur dann mit der Kommission und anderen zuständigen Behörden ausgetauscht, wenn ein solcher Austausch für die Anwendung dieser Verordnung erforderlich ist. Die auszutauschenden Informationen werden auf den für den Zweck dieses Informationsaustauschs erforderlichen und verhältnismäßigen Umfang beschränkt. Beim Informationsaustausch wird die Vertraulichkeit der Informationen gewahrt und die Sicherheit sowie die geschäftlichen Interessen von Einrichtungen mit kritischen oder erheblichen Auswirkungen werden geschützt.

Verantwortlich für die Aktivität: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Zu informieren: EC

Chapter 50

Artikel 48. : Übergangsbestimmungen

50.1 Absatz 1

Bis zur Genehmigung der Modalitäten oder Methoden gemäß Artikel 6 Absatz 2 oder der Pläne gemäß Artikel 6 Absatz 3 erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO unverbindliche Leitlinien zu folgenden Themen:

a. einem vorläufigen Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor (im Folgenden „ECII“) gemäß Absatz 2;

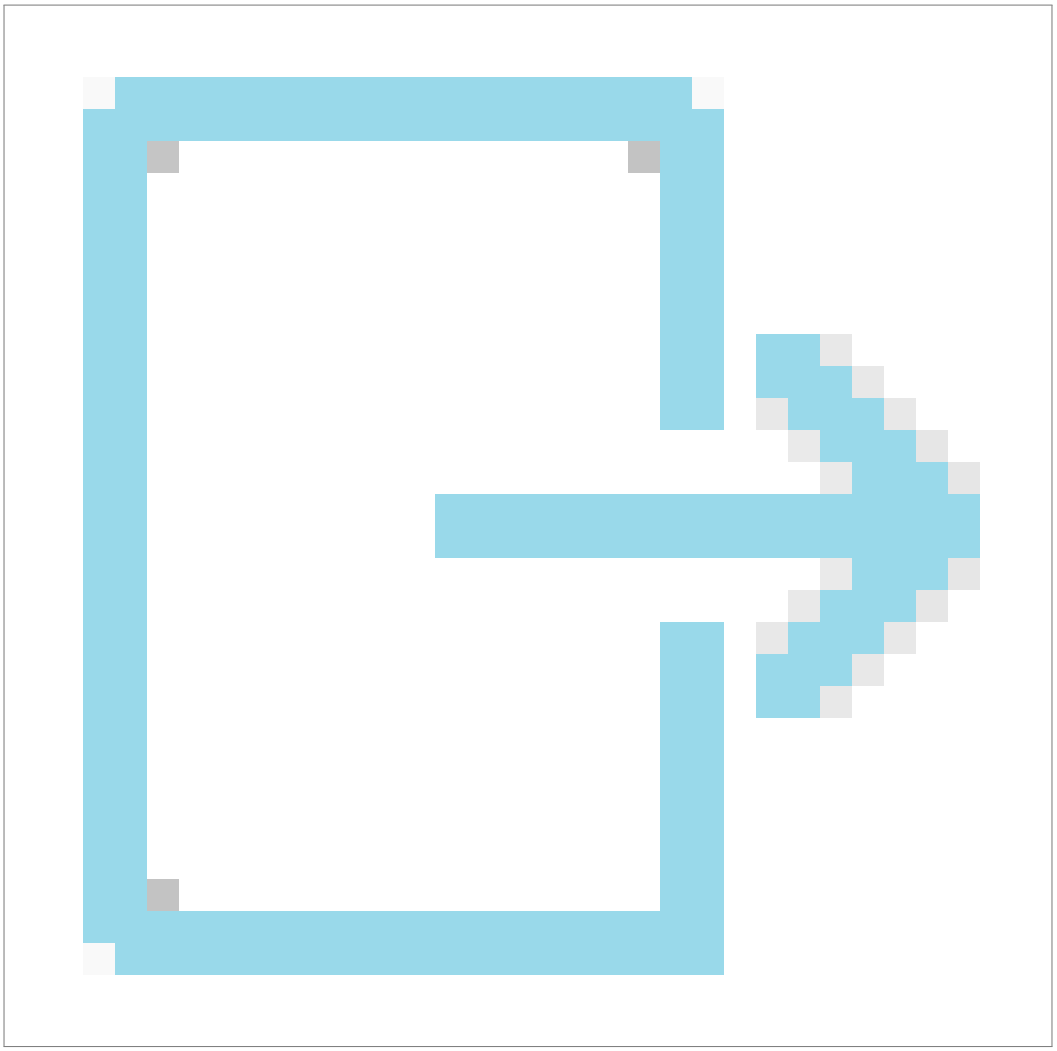
b. einer vorläufigen Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen gemäß Absatz 4 sowie

c. einer vorläufigen Liste europäischer und internationaler Normen und Kontrollen gemäß Absatz 6, die nach nationalen Rechtsvorschriften erforderlich und für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.

Relevante NCCS-Artikel

- Artikel 6 (2)

- Artikel 6 (3)
- Artikel 48 (2)
- Artikel 48 (4)
- Artikel 48 (6)



Output

- Vorläufige ECII
- Vorläufige Liste der unionsweiten Prozesse mit erheblicher und kritischer Auswirkung
- Vorläufige Liste der europäischen und internationalen Normen und Kontrollen

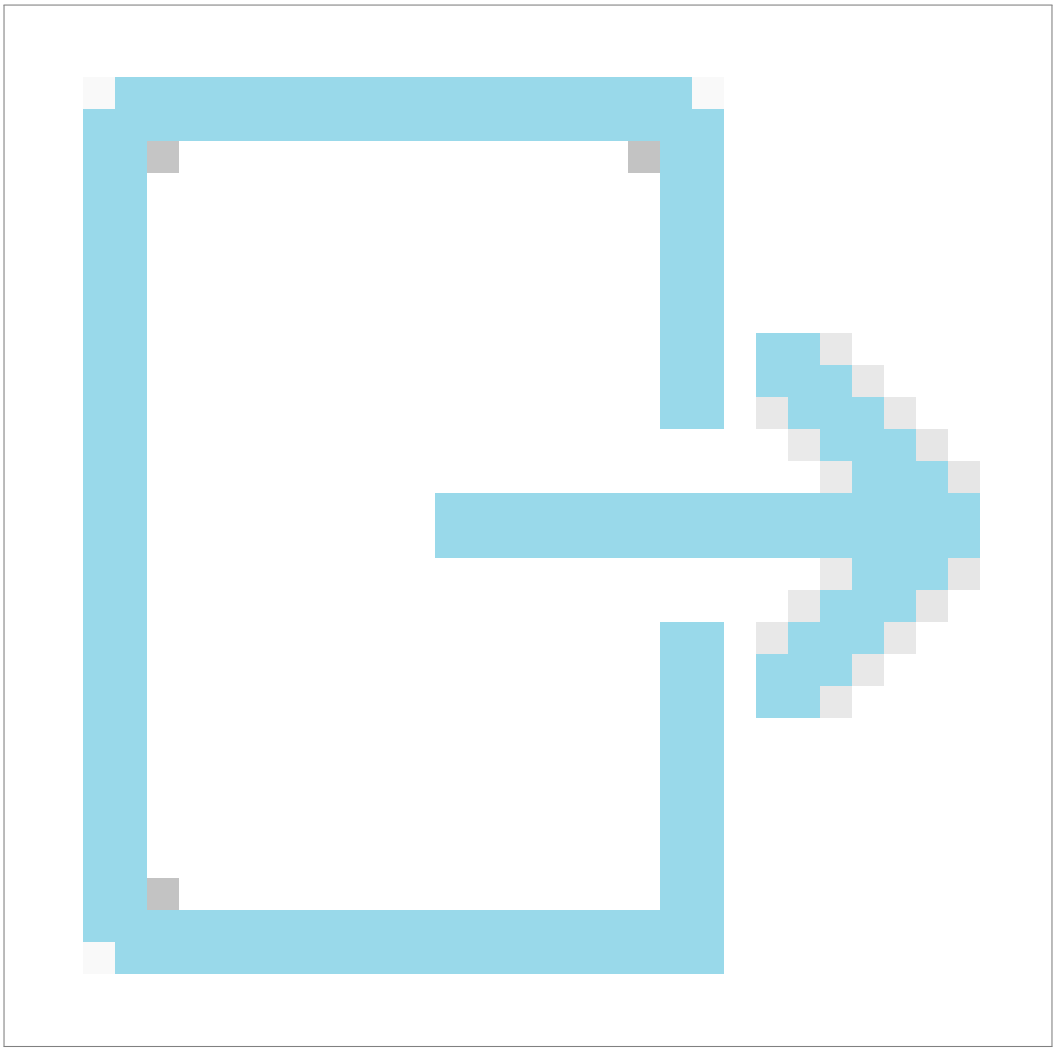
Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

50.2 Absatz 2

Bis zum 13 Oktober 2024 erarbeitet ENTSO-E in Zusammenarbeit mit der EU-VNBO eine Empfehlung für einen vorläufigen ECII. ENTSO-E teilt den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO den empfohlenen vorläufigen ECII mit.



Output

- Vorläufige ECII

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Oktober 2024

Verantwortlich für die Aktivität: ENTSO-E

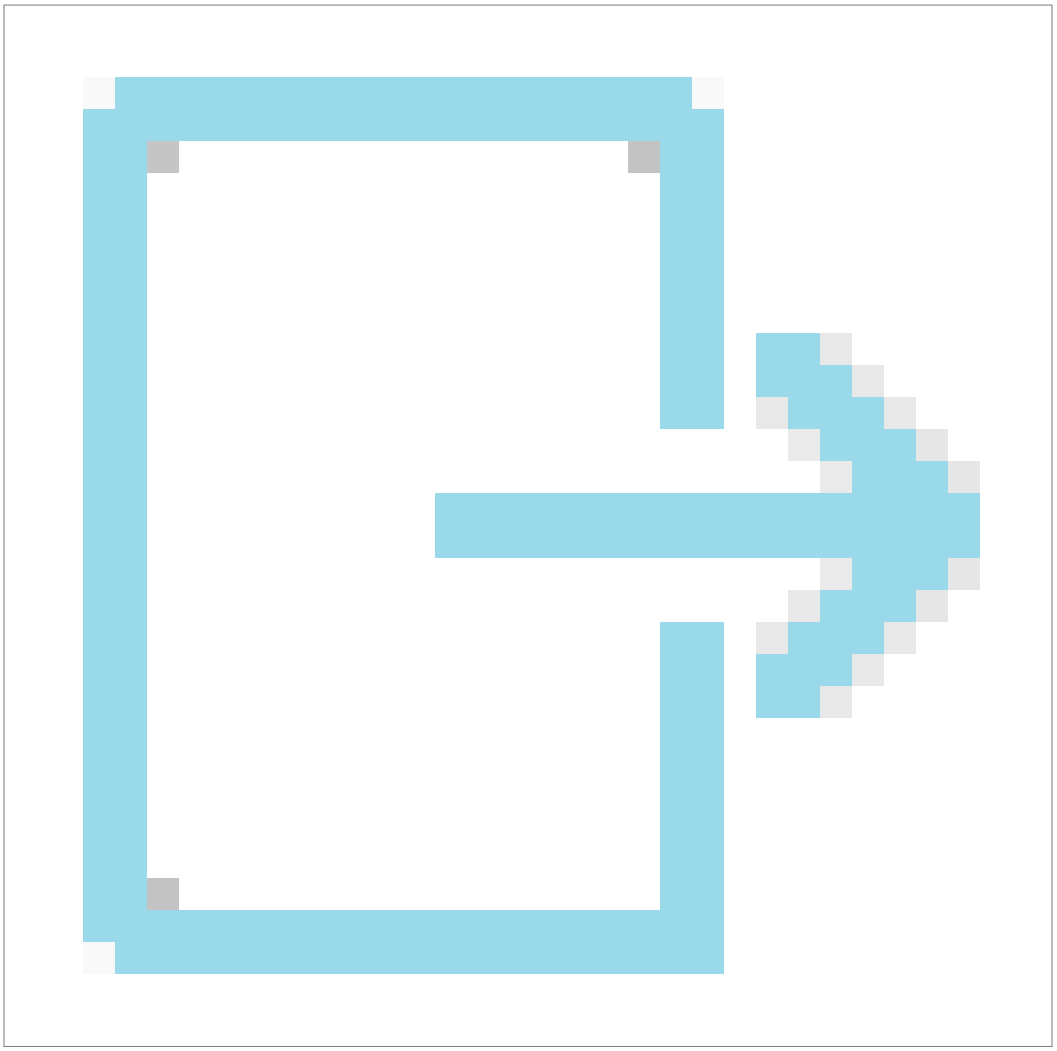
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu informieren: NCA

50.3 Absatz 3

Vier Monate nach Erhalt des empfohlenen vorläufigen ECII oder bis spätestens 13 Februar 2025 ermitteln die zuständigen Behörden auf der Grundlage des empfohlenen ECII Einrichtungen, die als Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat in Betracht kommen, und erstellen eine vorläufige Liste von Einrichtungen mit erheblichen oder kritischen Auswirkungen.



Output

- Mitteilung über vorläufig identifizierte Unternehmen

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Februar 2025

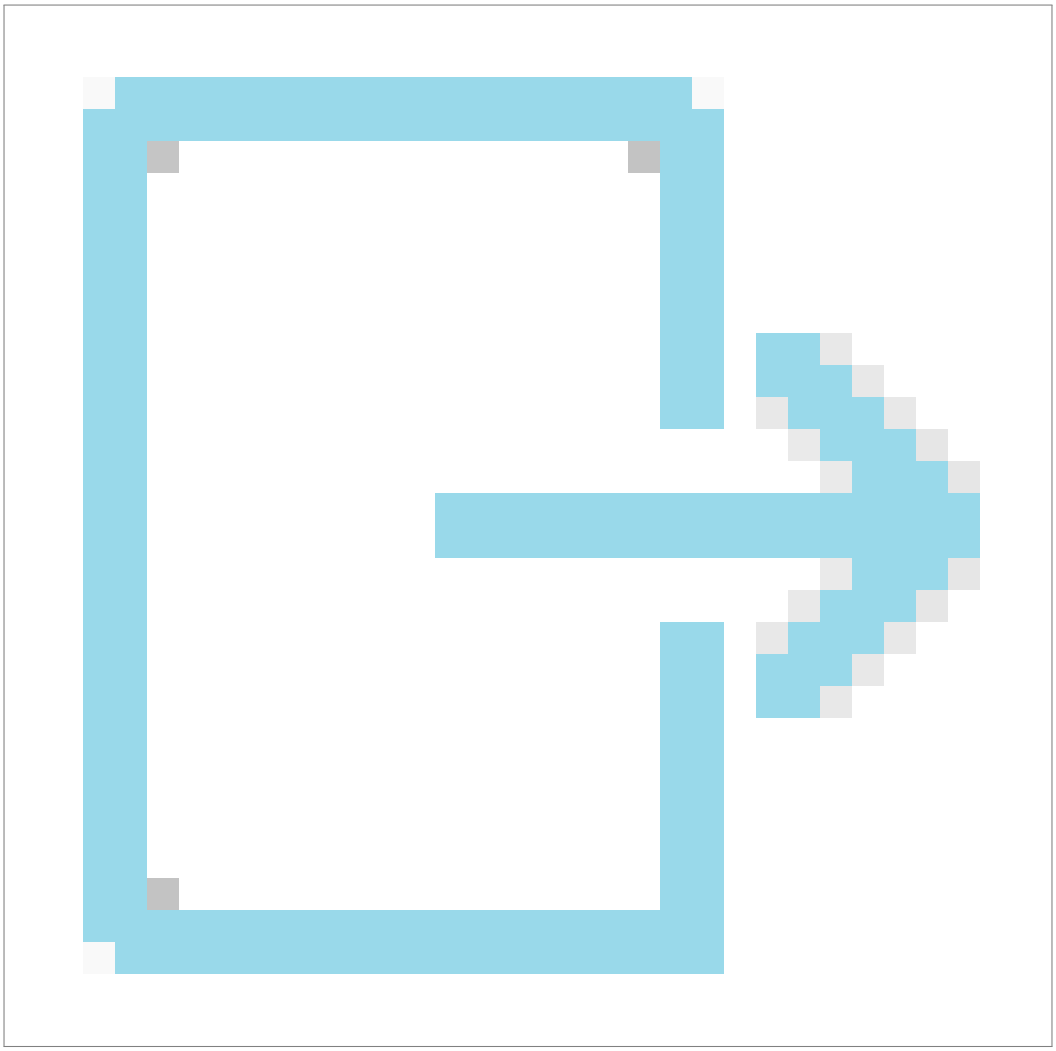
Verantwortlich für die Aktivität: NCA

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

50.4 Absatz 3

Die in der vorläufigen Liste aufgeführten Einrichtungen mit erheblichen oder kritischen Auswirkungen können ihren in dieser Verordnung festgelegten Verpflichtungen nach dem Vorsorgeprinzip freiwillig nachkommen. Bis zum 13 März 2025 teilen die zuständigen Behörden den in der vorläufigen Liste aufgeführten Einrichtungen mit, dass sie als Einrichtung mit erheblichen oder kritischen Auswirkungen eingestuft wurden.



Output

- Liste der vorläufig identifizierten Unternehmen

GOOD TO KNOW

Zeitpunkt

Bis zum 13. März 2025

Verantwortlich für die Aktivität: NCA

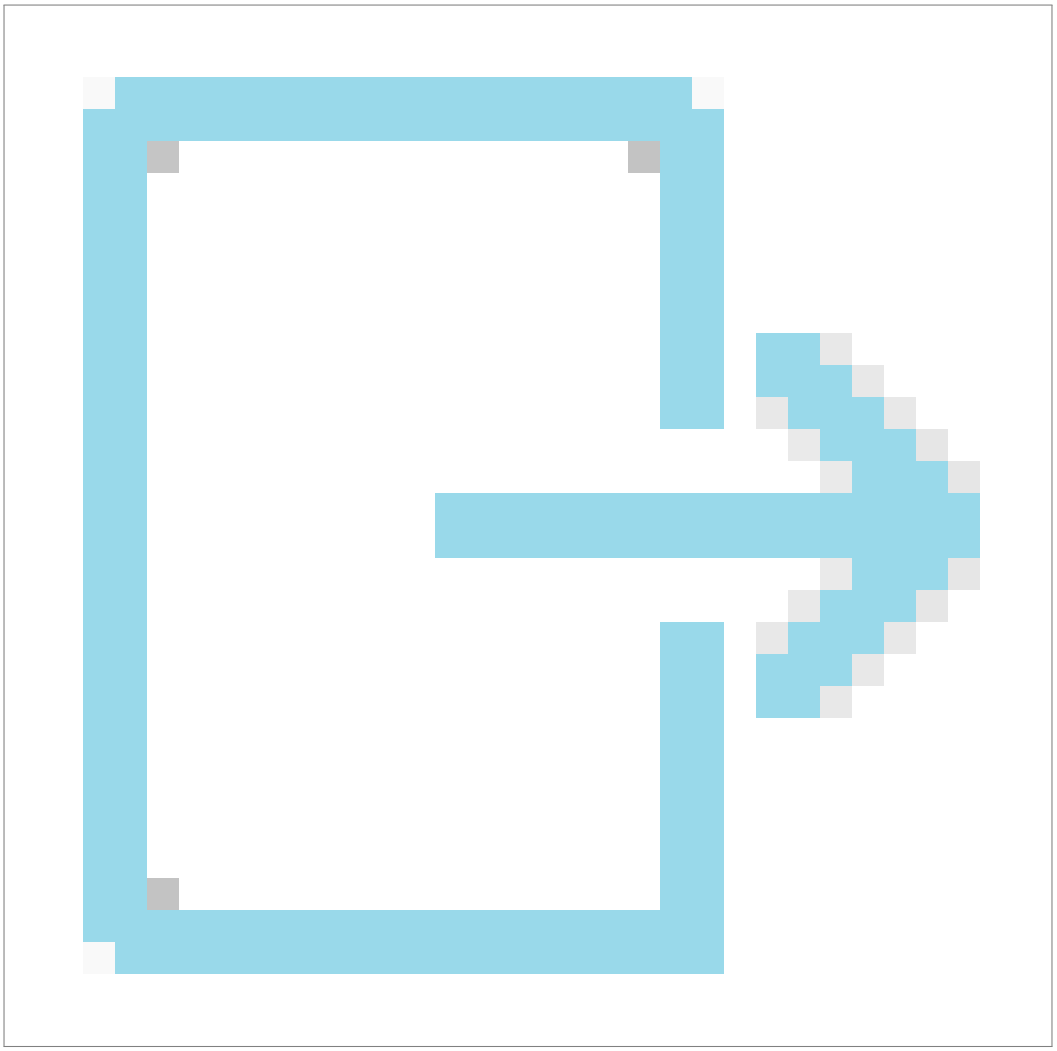
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu informieren: HIE, CIE

50.5 Absatz 4

Bis zum 13 Dezember 2024 erarbeitet ENTSO-E in Zusammenarbeit mit der EU-VNBO eine vorläufige Liste von unionsweiten Prozessen mit erheblichen oder kritischen Auswirkungen.



Output

- Vorläufige Liste der Prozesse mit erheblicher und kritischer Auswirkung

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Dezember 2024

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

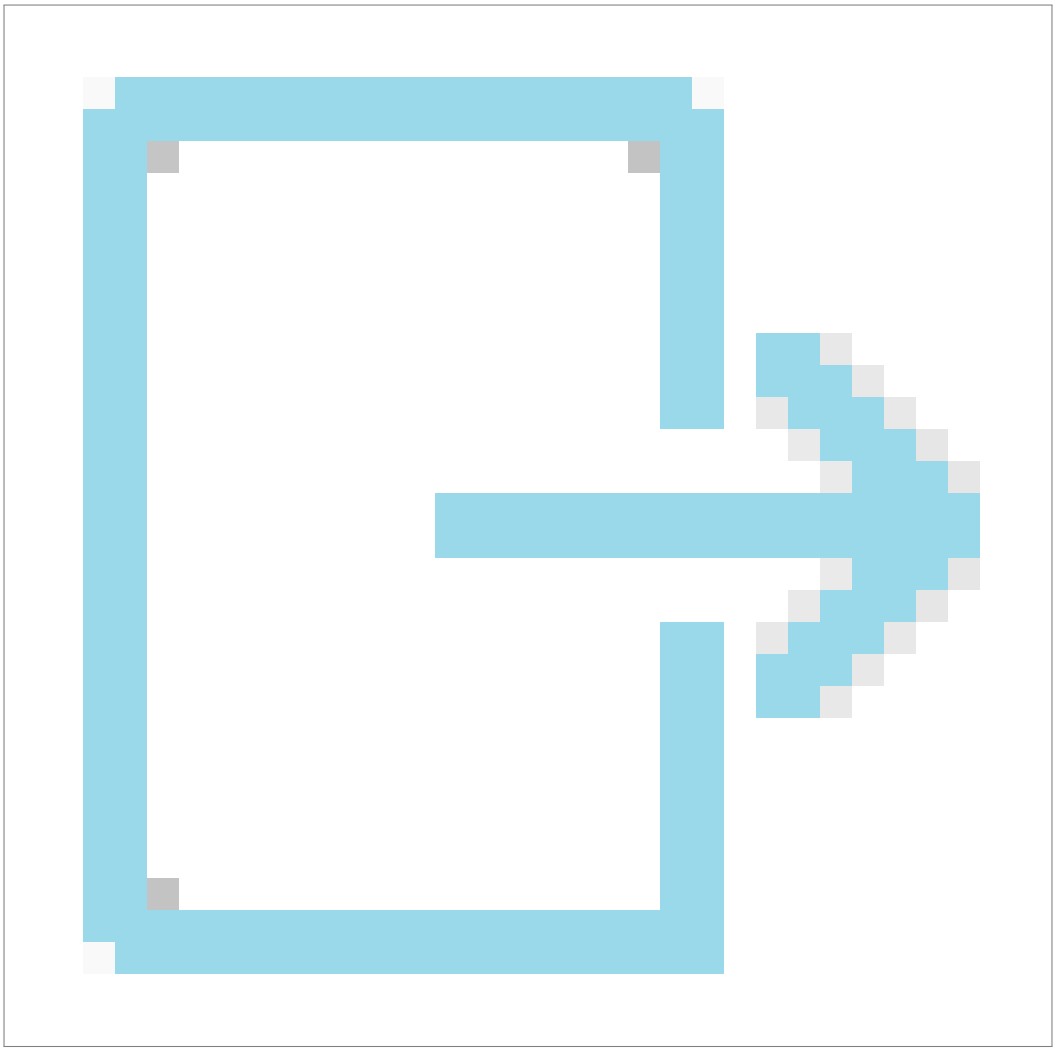
Zu informieren: NCA

50.6 Absatz 4

Die gemäß Absatz 3 unterrichteten Einrichtungen, die freiwillig beschließen, ihre in dieser Verordnung festgelegten Verpflichtungen nach dem Vorsorgeprinzip zu erfüllen, nutzen die vorläufige Liste von unionsweiten Prozessen mit erheblichen oder kritischen Auswirkungen, um vorläufige Perimeter mit erheblichen oder kritischen Auswirkungen zu bestimmen und um zu ermitteln, welche Vermögenswerte in die erste Bewertung des Cybersicherheitsrisikos auf Ebene der Einrichtung einzubeziehen sind.

Relevante NCCS-Artikel

- Artikel 48 (3)



Output

- Risikobewertungsbericht auf Unternehmensebene

GOOD TO KNOW

Zeitpunkt

12 Monate nach der Mitteilung

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

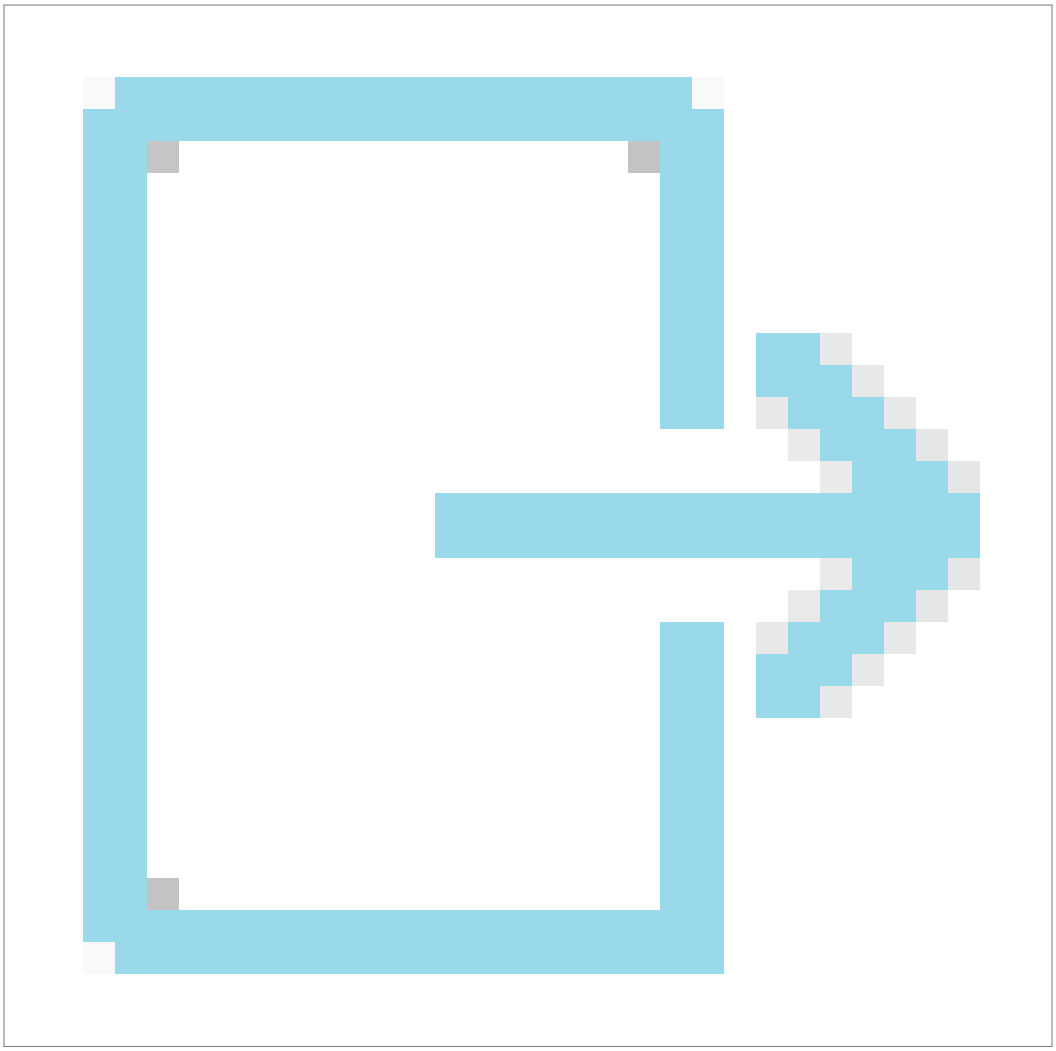
Zu informieren: ENTSO-E, ACER, NCA

50.7 Absatz 5

Bis zum 13 September 2024 übermittelt jede gemäß Artikel 4 Absatz 1 zuständige Behörde ENTSO-E und der EU-VNBO eine Liste ihrer nationalen Rechtsvorschriften, die für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.

Relevante NCCS-Artikel

- Artikel 4 (1)



Output

- Liste nationaler Rechtsvorschriften

GOOD TO KNOW

Zeitpunkt

Bis zum 13. September 2024

Verantwortlich für die Aktivität: NCA

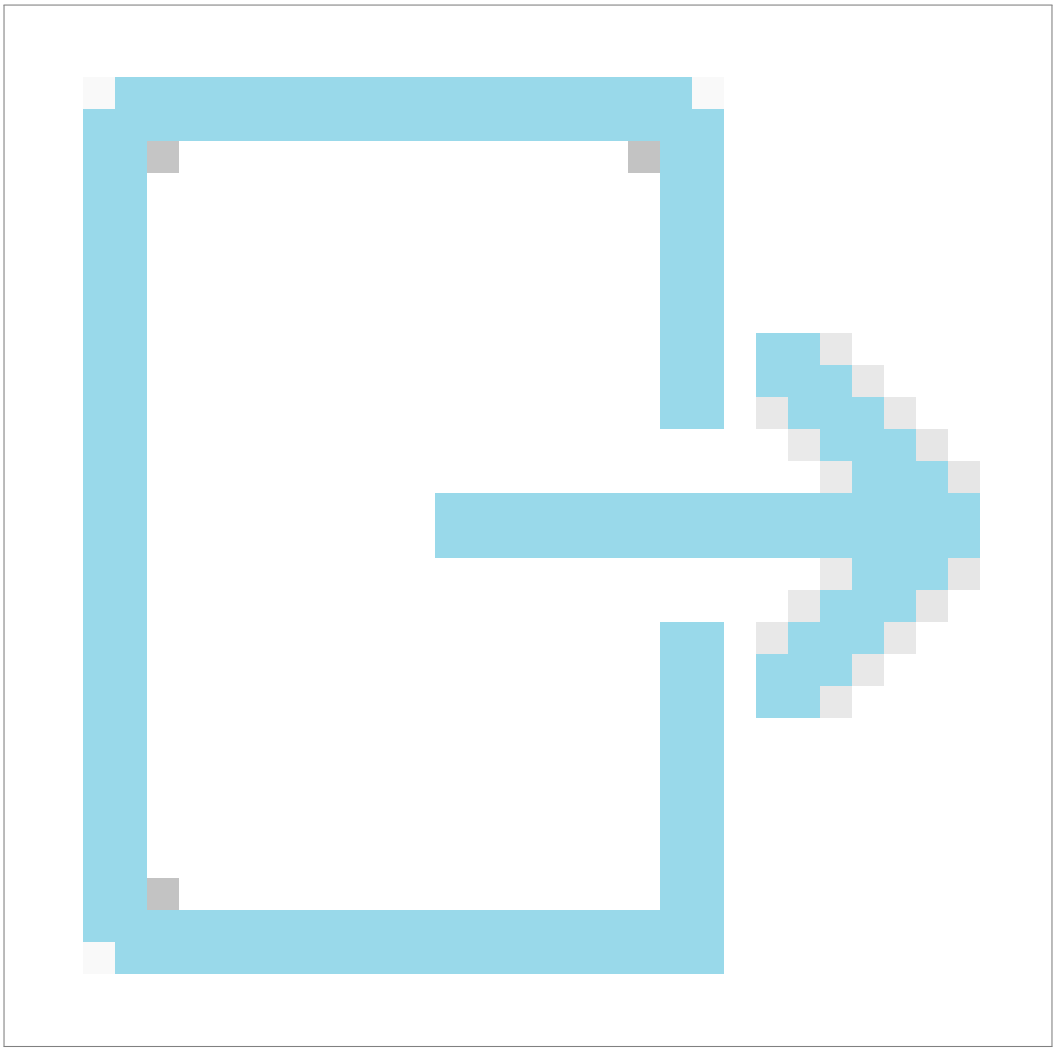
Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: NCA

Zu informieren: ENTSO-E, EU DSO

50.8 Absatz 6

Bis zum 13 Juni 2025 erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO unter Berücksichtigung der von den zuständigen Behörden bereitgestellten Informationen eine vorläufige Liste der nach nationalem Recht vorgeschriebenen europäischen und internationalen Normen und Kontrollen, die für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.



Output

- Vorläufige Liste europäischer und internationaler Normen und Kontrollen

GOOD TO KNOW

Zeitpunkt

Bis zum 13. Juni 2025

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO, NCA

50.9 Absatz 7

Die vorläufige Liste der europäischen und internationalen Normen und Kontrollen muss Folgendes enthalten:

a. europäische und internationale Normen und nationale Rechtsvorschriften, die Leitlinien für Methoden für das Risikomanagement im Bereich der Cybersicherheit auf Ebene der Einrichtungen enthalten, und

b. Cybersicherheitskontrollen, die denjenigen gleichwertig sind, die voraussichtlich Teil der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen sein werden.

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO, NCA

50.10 Absatz 8

ENTSO-E und die EU-VNBO berücksichtigen bei der Fertigstellung der vorläufigen Liste von Normen die Stellungnahmen der ENISA und der ACER. ENTSO-E und die EU-VNBO veröffentlichen die vorläufige Liste der europäischen und internationalen Normen und Kontrollen auf ihren Websites.

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, ACER, ENISA, EU DSO

50.11 Absatz 9

ENTSO-E und die EU-VNBO konsultieren die ENISA und die ACER zu den gemäß Absatz 1 erstellten Vorschlägen für unverbindliche Leitlinien.

Relevante NCCS-Artikel

- Artikel 48 (1)

Verantwortlich für die Aktivität: ENTSO-E

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: ENTSO-E, EU DSO

Zu konsultieren: ACER, ENISA

50.12 Absatz 10

Bis die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen gemäß Artikel 29 entwickelt und gemäß Artikel 8 angenommen sind, bemühen sich alle in Artikel 2 Absatz 1 aufgeführten Einrichtungen, die gemäß Absatz 1 des vorliegenden Artikels erstellten unverbindlichen Leitlinien nach und nach anzuwenden.

Relevante NCCS-Artikel

- Artikel 29
- Artikel 8
- Artikel 2
- Artikel 48 (1)

Verantwortlich für die Aktivität: HIE, CIE, TSO

Beteiligte Stakeholder:

Beteiligt an der Aufgabenausführung: HIE, CIE, TSO

Glossary

Agentur der Europäischen Union für Cybersicherheit (ENISA)

ENISA ist die Cybersicherheitsagentur der EU und unterstützt die Mitgliedstaaten bei der Abwehr von Cyberbedrohungen.

Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER)

Eine spezialisierte Agentur der Europäischen Union, die für die Förderung der Integration und des effizienten Funktionierens der EU-Energiemärkte zuständig ist.

https://www.acer.europa.eu/ [1]

VERORDNUNG (EU) 2019/942 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [2]

Anbieter kritischer IKT-Dienste

Bezeichnet eine Einrichtung, die einen IKT-Dienst oder einen IKT-Prozess bereitstellt, der für einen Prozess mit kritischen oder erheblichen Auswirkungen, der sich auf Cybersicherheitsaspekte grenzüberschreitender Stromflüsse auswirkt, erforderlich ist und bei dessen Kompromittierung ein Cyberangriff erfolgen könnte, dessen Auswirkungen den Schwellenwert für kritische oder erhebliche Auswirkungen überschreiten.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [3]

Artikel 10

Die ACER organisiert in enger Zusammenarbeit mit ENTSO-E und der EU-VNBO die Einbeziehung der Interessenträger, einschließlich regelmäßiger Treffen mit Interessenträgern, um Probleme

[1] https://www.acer.europa.eu/
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

zu ermitteln und Verbesserungen im Zusammenhang mit der Durchführung dieser Verordnung vorzuschlagen.

Artikel 10

Die ACER organisiert in enger Zusammenarbeit mit ENTSO-E und der EU-VNBO die Einbeziehung der Interessenträger, einschließlich regelmäßiger Treffen mit Interessenträgern, um Probleme zu ermitteln und Verbesserungen im Zusammenhang mit der Durchführung dieser Verordnung vorzuschlagen.

Artikel 11

1. Die Kosten, die aufgrund der Verpflichtungen aus dieser Verordnung bei ÜNB und VNB anfallen, die der Netzentgeltregulierung unterliegen, einschließlich der Kosten von ENTSO-E und der EU-VNBO, werden von der zuständigen NRB jedes Mitgliedstaats geprüft.
2. Als angemessen, effizient und verhältnismäßig bewertete Kosten werden durch Netzentgelte oder andere geeignete Mechanismen gedeckt, die von der zuständigen NRB festgelegt werden.
3. Auf Verlangen der zuständigen NRB stellen die in Absatz 1 genannten ÜNB und VNB innerhalb einer von der NRB festgelegten angemessenen Frist die erforderlichen Informationen bereit, um die Prüfung der entstandenen Kosten zu erleichtern.

Artikel 11(1)

Die Kosten, die aufgrund der Verpflichtungen aus dieser Verordnung bei ÜNB und VNB anfallen, die der Netzentgeltregulierung unterliegen, einschließlich der Kosten von ENTSO-E und der EU-VNBO, werden von der zuständigen NRB jedes Mitgliedstaats geprüft.

Artikel 11(2)

Als angemessen, effizient und verhältnismäßig bewertete Kosten werden durch Netzentgelte oder andere geeignete Mechanismen gedeckt, die von der zuständigen NRB festgelegt werden.

Artikel 11(3)

Auf Verlangen der zuständigen NRB stellen die in Absatz 1 genannten ÜNB und VNB innerhalb einer von der NRB festgelegten angemessenen Frist die erforderlichen Informationen bereit, um die Prüfung der entstandenen Kosten zu erleichtern.

Artikel 12

1. Die ACER überwacht die Durchführung dieser Verordnung gemäß Artikel 32 Absatz 1 der Verordnung (EU) 2019/943 und Artikel 4 Absatz 2 der Verordnung (EU) 2019/942. Bei der Durchführung der Überwachung kann die ACER mit der ENISA zusammenarbeiten und ENTSO-E und die EU-VNBO um Unterstützung ersuchen. Die ACER unterrichtet die Koordinierungsgruppe „Strom" und die NIS-Kooperationsgruppe regelmäßig über die Durchführung dieser Verordnung. Artikel 32(1) der Verordnung (EU) 2019/943 [4], Artikel 4(2) der Verordnung (EU) 2019/942 [5]

2. Die ACER veröffentlicht nach dem Inkrafttreten dieser Verordnung mindestens alle drei Jahre einen Bericht, um

   a. den Stand der Umsetzung der anwendbaren Risikomanagementmaßnahmen im Bereich der Cybersicherheit durch Einrichtungen mit erheblichen Auswirkungen und Einrichtungen mit kritischen Auswirkungen zu überprüfen;

   b. zu ermitteln, ob zur Prävention von Risiken für den Elektrizitätssektor zusätzliche Vorschriften über gemeinsame Anforderungen, Planung, Beobachtung, Berichterstattung und Krisenbewältigung erforderlich sein könnten, und

   c. Verbesserungsbedarf für die Überarbeitung dieser Verordnung zu bestimmen oder nicht abgedeckte Bereiche und neue Prioritäten zu ermitteln, die sich aufgrund technischer Entwicklungen ergeben können.

3. Bis zum 13 Juni 2025 kann die ACER in Zusammenarbeit mit der ENISA und nach Konsultation von ENTSO-E und der EU-VNBO auf der Grundlage der gemäß Absatz 5 festgelegten Leistungsindikatoren Leitlinien zu den relevanten Informationen, die der ACER zu Überwachungszwecken zu übermitteln sind, sowie zu dem Verfahren und der Häufigkeit der Einholung der Informationen vorlegen.

4. Die zuständigen Behörden können Zugang zu den einschlägigen Informationen erhalten, die sich im Besitz der ACER befinden und gemäß diesem Artikel erhoben wurden.

5. Die ACER legt in Zusammenarbeit mit der ENISA und mit Unterstützung von ENTSO-E und der EU-VNBO in Bezug auf Cybersicherheitsaspekte grenzüberschreitender Stromflüsse unverbindliche Leistungsindikatoren für die Bewertung der betrieblichen Zuverlässigkeit vor.

6. Die in Artikel 2 Absatz 1 dieser Verordnung aufgeführten Einrichtungen übermitteln der ACER die Informationen, die diese zur Wahrnehmung der in Absatz 2 genannten Aufgaben benötigt.

Artikel 12(1)

Die ACER überwacht die Durchführung dieser Verordnung gemäß Artikel 32 Absatz 1 der Verordnung (EU) 2019/943 und Artikel 4 Absatz 2 der Verordnung (EU) 2019/942. Bei der Durchführung der Überwachung kann die ACER mit der ENISA zusammenarbeiten und ENTSO-E und die EU-VNBO um Unterstützung ersuchen. Die ACER unterrichtet die Koordinierungsgruppe „Strom" und

[4] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943&qid=1733993709560#d1e3462-54-1

[5] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942#d1e519-22-1

die NIS-Kooperationsgruppe regelmäßig über die Durchführung dieser Verordnung. Article 32(1) of Regulation (EU) 2019/943 [6] Article 4(2) of Regulation (EU) 2019/942 [7]

Artikel 12(2)

Die ACER veröffentlicht nach dem Inkrafttreten dieser Verordnung mindestens alle drei Jahre einen Bericht, um

a. den Stand der Umsetzung der anwendbaren Risikomanagementmaßnahmen im Bereich der Cybersicherheit durch Einrichtungen mit erheblichen Auswirkungen und Einrichtungen mit kritischen Auswirkungen zu überprüfen;
b. zu ermitteln, ob zur Prävention von Risiken für den Elektrizitätssektor zusätzliche Vorschriften über gemeinsame Anforderungen, Planung, Beobachtung, Berichterstattung und Krisenbewältigung erforderlich sein könnten, und
c. Verbesserungsbedarf für die Überarbeitung dieser Verordnung zu bestimmen oder nicht abgedeckte Bereiche und neue Prioritäten zu ermitteln, die sich aufgrund technischer Entwicklungen ergeben können.

Artikel 12(3)

Bis zum 13 Juni 2025 kann die ACER in Zusammenarbeit mit der ENISA und nach Konsultation von ENTSO-E und der EU-VNBO auf der Grundlage der gemäß Absatz 5 festgelegten Leistungsindikatoren Leitlinien zu den relevanten Informationen, die der ACER zu Überwachungszwecken zu übermitteln sind, sowie zu dem Verfahren und der Häufigkeit der Einholung der Informationen vorlegen.

Artikel 12(4)

Die zuständigen Behörden können Zugang zu den einschlägigen Informationen erhalten, die sich im Besitz der ACER befinden und gemäß diesem Artikel erhoben wurden.

Artikel 12(5)

Die ACER legt in Zusammenarbeit mit der ENISA und mit Unterstützung von ENTSO-E und der EU-VNBO in Bezug auf Cybersicherheitsaspekte grenzüberschreitender Stromflüsse unverbindliche Leistungsindikatoren für die Bewertung der betrieblichen Zuverlässigkeit vor.

Artikel 12(6)

[6] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943&qid=1733993709560#d1e3462-54-1

[7] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942#d1e519-22-1

Die in Artikel 2 Absatz 1 dieser Verordnung aufgeführten Einrichtungen übermitteln der ACER die Informationen, die diese zur Wahrnehmung der in Absatz 2 genannten Aufgaben benötigt.

Artikel 13

1. Bis zum 13 Juni 2025 erstellt die ACER in Zusammenarbeit mit der ENISA einen unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit. In dem Leitfaden für die NRB werden die Grundsätze des Benchmarkings der durchgeführten Cybersicherheitskontrollen gemäß Absatz 2 erläutert, wobei die Kosten für die Durchführung der Kontrollen und die Wirksamkeit von Prozessen, Produkten, Diensten, Systemen und Lösungen, die zur Durchführung dieser Kontrollen genutzt werden, zu berücksichtigen sind. Die ACER berücksichtigt bei der Erstellung des unverbindlichen Leitfadens für das Benchmarking im Bereich der Cybersicherheit vorhandene Benchmarking-Berichte. Die ACER übermittelt den unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit den NRB zur Information.

2. Innerhalb von 12 Monaten nach Erstellung des Benchmarking-Leitfadens gemäß Absatz 1 führen die NRB eine Benchmarking-Analyse durch, um zu bewerten, ob die aktuellen Investitionen in die Cybersicherheit

   a. Risiken mit Auswirkungen auf grenzüberschreitende Stromflüsse mindern;
   b. zu den gewünschten Ergebnissen führen und die Effizienz bei der Entwicklung des Elektrizitätssystems verbessern;
   c. effizient sind und in die allgemeine Auftragsvergabe für Vermögenswerte und Dienstleistungen integriert werden.

3. Bei der Benchmarking-Analyse können die NRB den von der ACER erstellten unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit berücksichtigen, wobei sie insbesondere Folgendes bewerten:

   a. die durchschnittlichen Ausgaben für die Cybersicherheit zur Minderung von Risiken, die sich auf grenzüberschreitende Stromflüsse auswirken, insbesondere bei Einrichtungen mit erheblichen oder kritischen Auswirkungen;
   b. in Zusammenarbeit mit ENTSO-E und der EU-VNBO die Durchschnittspreise für Cybersicherheitsdienste, -systeme und -produkte, die in hohem Maß zur Verbesserung und Aufrechterhaltung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit in den verschiedenen Netzbetriebsregionen beitragen;
   c. das Vorhandensein von Cybersicherheitsdiensten, -systemen und -lösungen, die sich für die Durchführung dieser Verordnung eignen, sowie die Vergleichbarkeit der damit verbundenen Kosten und Funktionen, wobei sie mögliche Maßnahmen ermitteln, die zur Verbesserung der Effizienz der Ausgaben erforderlich sind, insbesondere wenn Investitionen in die Cybersicherheitstechnik erforderlich sein könnten.

4. Alle Informationen zu Benchmarking-Analysen werden gemäß den Anforderungen dieser Verordnung an dieDatenklassifizierung, die Mindest-Cybersicherheitskontrollen und den Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gehandhabt und verarbeitet. Die in den Absätzen 2 und 3 genannte Benchmarking-Analyse wird nicht veröffentlicht.

5. Unbeschadet der Vertraulichkeitsbestimmungen in Artikel 47 und der Notwendigkeit, die Sicherheit von Einrichtungen zu schützen, die den Bestimmungen dieser Verordnung unterliegen, wird die in den Absätzen 2 und 3 dieses Artikels genannte Benchmarking-Analyse allen NRB, allen zuständigen Behörden, der ACER, der ENISA und der Kommission übermittelt.

Artikel 13(1)

Bis zum 13 Juni 2025 erstellt die ACER in Zusammenarbeit mit der ENISA einen unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit. In dem Leitfaden für die NRB werden die Grundsätze des Benchmarkings der durchgeführten Cybersicherheitskontrollen gemäß Absatz 2 erläutert, wobei die Kosten für die Durchführung der Kontrollen und die Wirksamkeit von Prozessen, Produkten, Diensten, Systemen und Lösungen, die zur Durchführung dieser Kontrollen genutzt werden, zu berücksichtigen sind. Die ACER berücksichtigt bei der Erstellung des unverbindlichen Leitfadens für das Benchmarking im Bereich der Cybersicherheit vorhandene Benchmarking-Berichte. Die ACER übermittelt den unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit den NRB zur Information.

Artikel 13(2)

Innerhalb von 12 Monaten nach Erstellung des Benchmarking-Leitfadens gemäß Absatz 1 führen die NRB eine Benchmarking-Analyse durch, um zu bewerten, ob die aktuellen Investitionen in die Cybersicherheit

a. Risiken mit Auswirkungen auf grenzüberschreitende Stromflüsse mindern;
b. zu den gewünschten Ergebnissen führen und die Effizienz bei der Entwicklung des Elektrizitätssystems verbessern;
c. effizient sind und in die allgemeine Auftragsvergabe für Vermögenswerte und Dienstleistungen integriert werden.

Artikel 13(3)

Bei der Benchmarking-Analyse können die NRB den von der ACER erstellten unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit berücksichtigen, wobei sie insbesondere Folgendes bewerten:

a. die durchschnittlichen Ausgaben für die Cybersicherheit zur Minderung von Risiken, die sich auf grenzüberschreitende Stromflüsse auswirken, insbesondere bei Einrichtungen mit erheblichen oder kritischen Auswirkungen;
b. in Zusammenarbeit mit ENTSO-E und der EU-VNBO die Durchschnittspreise für Cybersicherheitsdienste, -systeme und -produkte, die in hohem Maß zur Verbesserung und Aufrechterhaltung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit in den verschiedenen Netzbetriebsregionen beitragen;

c. das Vorhandensein von Cybersicherheitsdiensten, -systemen und -lösungen, die sich für die Durchführung dieser Verordnung eignen, sowie die Vergleichbarkeit der damit verbundenen Kosten und Funktionen, wobei sie mögliche Maßnahmen ermitteln, die zur Verbesserung der Effizienz der Ausgaben erforderlich sind, insbesondere wenn Investitionen in die Cybersicherheitstechnik erforderlich sein könnten.

Artikel 13(4)

Alle Informationen zu Benchmarking-Analysen werden gemäß den Anforderungen dieser Verordnung an dieDatenklassifizierung, die Mindest-Cybersicherheitskontrollen und den Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gehandhabt und verarbeitet. Die in den Absätzen 2 und 3 genannte Benchmarking-Analyse wird nicht veröffentlicht.

Artikel 13(5)

Unbeschadet der Vertraulichkeitsbestimmungen in Artikel 47 und der Notwendigkeit, die Sicherheit von Einrichtungen zu schützen, die den Bestimmungen dieser Verordnung unterliegen, wird die in den Absätzen 2 und 3 dieses Artikels genannte Benchmarking-Analyse allen NRB, allen zuständigen Behörden, der ACER, der ENISA und der Kommission übermittelt.

Artikel 14

1. Innerhalb von 18 Monaten nach dem Inkrafttreten dieser Verordnung bemühen sich die ÜNB einer Netzbetriebsregion, die an ein Drittland angrenzt, um den Abschluss von Vereinbarungen mit ÜNB des benachbarten Drittlands, die mit dem einschlägigen Unionsrecht im Einklang stehen, die Grundlage für die Zusammenarbeit zum Cybersicherheitsschutz bilden und Regelungen für die Zusammenarbeit mit diesen ÜNB im Bereich der Cybersicherheit enthalten.
2. Die ÜNB unterrichten die zuständige Behörde über die gemäß Absatz 1 geschlossenen Vereinbarungen.

Artikel 14(1)

Innerhalb von 18 Monaten nach dem Inkrafttreten dieser Verordnung bemühen sich die ÜNB einer Netzbetriebsregion, die an ein Drittland angrenzt, um den Abschluss von Vereinbarungen mit ÜNB des benachbarten Drittlands, die mit dem einschlägigen Unionsrecht im Einklang stehen, die Grundlage für die Zusammenarbeit zum Cybersicherheitsschutz bilden und Regelungen für die Zusammenarbeit mit diesen ÜNB im Bereich der Cybersicherheit enthalten.

Artikel 14(2)

Die ÜNB unterrichten die zuständige Behörde über die gemäß Absatz 1 geschlossenen Vereinbarungen.

Artikel 15

1. Einrichtungen, die keine Niederlassung in der Union haben, aber Dienstleistungen für Einrichtungen in der Union erbringen und gemäß Artikel 24 Absatz 6 über ihren Status als Einrichtungen mit erheblichen oder kritischen Auswirkungen unterrichtet wurden, benennen innerhalb von drei Monaten nach der Unterrichtung schriftlich einen Vertreter in der Union und informieren die zuständige Behörde entsprechend.
2. Dieser Vertreter wird beauftragt, zusätzlich zu oder anstelle der Einrichtung mit erheblichen oder kritischen Auswirkungen als Ansprechpartner zu fungieren, an den sich jede zuständige Behörde und jedes CSIRT in der Union in Bezug auf die Verpflichtungen der Einrichtung aus dieser Verordnung wenden kann. Die Einrichtung mit erheblichen oder kritischen Auswirkungen stattet ihren gesetzlichen Vertreter mit den erforderlichen Befugnissen und ausreichenden Ressourcen aus, um eine effiziente und rechtzeitige Zusammenarbeit mit den jeweils zuständigen Behörden oder CSIRTs zu gewährleisten.
3. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Einrichtung ihre Dienste anbietet. Die Einrichtung gilt als der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegend, in dem der Vertreter niedergelassen ist. Einrichtungen mit erheblichen oder kritischen Auswirkungen melden der zuständigen Behörde des Mitgliedstaats, in dem ihr gesetzlicher Vertreter ansässig oder niedergelassen ist, den Namen, die Postanschrift, die E-Mail-Adresse und die Telefonnummer des gesetzlichen Vertreters.
4. Der benannte gesetzliche Vertreter kann für Verstöße gegen Pflichten aus dieser Verordnung haftbar gemacht werden; dies berührt nicht die Haftung und die rechtlichen Schritte, die gegen die Einrichtung mit erheblichen oder kritischen Auswirkungen eingeleitet werden können.
5. Wurde in der Union kein Vertreter im Sinne dieses Artikels benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienstleistungen erbringt, gegen die Einrichtung rechtliche Schritte wegen Verstößen gegen Pflichten aus dieser Verordnung einleiten.
6. Die Benennung eines gesetzlichen Vertreters in der Union gemäß Absatz 1 gilt nicht als Niederlassung in der Union.

Artikel 15(1)

Einrichtungen, die keine Niederlassung in der Union haben, aber Dienstleistungen für Einrichtungen in der Union erbringen und gemäß Artikel 24 Absatz 6 über ihren Status als Einrichtungen mit erheblichen oder kritischen Auswirkungen unterrichtet wurden, benennen innerhalb von drei Monaten nach der Unterrichtung schriftlich einen Vertreter in der Union und informieren die zuständige Behörde entsprechend.

Artikel 15(2)

Dieser Vertreter wird beauftragt, zusätzlich zu oder anstelle der Einrichtung mit erheblichen oder kritischen Auswirkungen als Ansprechpartner zu fungieren, an den sich jede zuständige Behörde und jedes CSIRT in der Union in Bezug auf die Verpflichtungen der Einrichtung aus dieser Verordnung wenden kann. Die Einrichtung mit erheblichen oder kritischen Auswirkungen stattet ihren gesetzlichen Vertreter mit den erforderlichen Befugnissen und ausreichenden Ressourcen aus, um eine effiziente und rechtzeitige Zusammenarbeit mit den jeweils zuständigen Behörden oder CSIRTs zu gewährleisten.

Artikel 15(3)

Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Einrichtung ihre Dienste anbietet. Die Einrichtung gilt als der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegend, in dem der Vertreter niedergelassen ist. Einrichtungen mit erheblichen oder kritischen Auswirkungen melden der zuständigen Behörde des Mitgliedstaats, in dem ihr gesetzlicher Vertreter ansässig oder niedergelassen ist, den Namen, die Postanschrift, die E-Mail-Adresse und die Telefonnummer des gesetzlichen Vertreters.

Artikel 15(4)

Der benannte gesetzliche Vertreter kann für Verstöße gegen Pflichten aus dieser Verordnung haftbar gemacht werden; dies berührt nicht die Haftung und die rechtlichen Schritte, die gegen die Einrichtung mit erheblichen oder kritischen Auswirkungen eingeleitet werden können.

Artikel 15(5)

Wurde in der Union kein Vertreter im Sinne dieses Artikels benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienstleistungen erbringt, gegen die Einrichtung rechtliche Schritte wegen Verstößen gegen Pflichten aus dieser Verordnung einleiten.

Artikel 15(6)

Die Benennung eines gesetzlichen Vertreters in der Union gemäß Absatz 1 gilt nicht als Niederlassung in der Union.

Artikel 16

1. ENTSO-E und die EU-VNBO arbeiten bei der Durchführung der Bewertungen des Cybersicherheitsrisikos gemäß Artikel 19 und Artikel 21 zusammen, insbesondere bei den folgenden Aufgaben:

    a. Entwicklung der Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 18 Absatz 1;

b. Erstellung des umfassenden Berichts über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23;
c. Entwicklung des gemeinsamen Rahmens für die Cybersicherheit im Elektrizitätssektor gemäß Kapitel III;
d. Erstellung der Empfehlung für die Cybersicherheit bei der Auftragsvergabe gemäß Artikel 35;
e. Entwicklung der Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8;
f. Entwicklung des vorläufigen Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor (ECII) gemäß Artikel 48 Absatz 1 Buchstabe a;
g. Erstellung der konsolidierten vorläufigen Liste der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 48 Absatz 3;
h. Erstellung der vorläufigen Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen gemäß Artikel 48 Absatz 4;
i. Erstellung der vorläufigen Liste europäischer und internationaler Normen und Kontrollen gemäß Artikel 48 Absatz 6;
j. Durchführung der unionsweiten Bewertung des Cybersicherheitsrisikos gemäß Artikel 19;
k. Durchführung der regionalen Bewertung des Cybersicherheitsrisikos gemäß Artikel 21;
l. Festlegung der regionalen Pläne zur Minderung des Cybersicherheitsrisikos gemäß Artikel 22;
m. Entwicklung von Leitlinien für europäische Schemata für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen gemäß Artikel 36;
n. Entwicklung von Leitlinien für die Durchführung dieser Verordnung, in Absprache mit der ACER und der ENISA.

2. Die Zusammenarbeit zwischen ENTSO-E und der EU-VNBO kann über eine Arbeitsgruppe für Cybersicherheitsrisiken erfolgen.

3. ENTSO-E und die EU-VNBO unterrichten die ACER, die ENISA, die NIS-Kooperationsgruppe und die Koordinierungsgruppe „Strom“ regelmäßig über die Fortschritte bei der Umsetzung der unionsweiten und regionalen Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 und Artikel 21.

Artikel 16(1)

ENTSO-E und die EU-VNBO arbeiten bei der Durchführung der Bewertungen des Cybersicherheitsrisikos gemäß Artikel 19 und Artikel 21 zusammen, insbesondere bei den folgenden Aufgaben:

a. Entwicklung der Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 18 Absatz 1;

b. Erstellung des umfassenden Berichts über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23;

c. Entwicklung des gemeinsamen Rahmens für die Cybersicherheit im Elektrizitätssektor gemäß Kapitel III;

d. Erstellung der Empfehlung für die Cybersicherheit bei der Auftragsvergabe gemäß Artikel 35;

e. Entwicklung der Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8;

f. Entwicklung des vorläufigen Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor (ECII) gemäß Artikel 48 Absatz 1 Buchstabe a;

g. Erstellung der konsolidierten vorläufigen Liste der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 48 Absatz 3;

h. Erstellung der vorläufigen Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen gemäß Artikel 48 Absatz 4;

i. Erstellung der vorläufigen Liste europäischer und internationaler Normen und Kontrollen gemäß Artikel 48 Absatz 6;

j. Durchführung der unionsweiten Bewertung des Cybersicherheitsrisikos gemäß Artikel 19;

k. Durchführung der regionalen Bewertung des Cybersicherheitsrisikos gemäß Artikel 21;

l. Festlegung der regionalen Pläne zur Minderung des Cybersicherheitsrisikos gemäß Artikel 22;

m. Entwicklung von Leitlinien für europäische Schemata für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen gemäß Artikel 36;

n. Entwicklung von Leitlinien für die Durchführung dieser Verordnung, in Absprache mit der ACER und der ENISA.

Artikel 16(2)

Die Zusammenarbeit zwischen ENTSO-E und der EU-VNBO kann über eine Arbeitsgruppe für Cybersicherheitsrisiken erfolgen.

Artikel 16(3)

ENTSO-E und die EU-VNBO unterrichten die ACER, die ENISA, die NIS-Kooperationsgruppe und die Koordinierungsgruppe „Strom“ regelmäßig über die Fortschritte bei der Umsetzung der unionsweiten und regionalen Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 und Artikel 21.

Artikel 17

1. Die ACER überwacht in Zusammenarbeit mit jeder zuständigen Behörde

(1) die Umsetzung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit gemäß Artikel 12 Absatz 2 Buchstabe a und der Berichterstattungspflichten gemäß den Artikeln 27 und 39 sowie

(2) das Verfahren zur Annahme der Modalitäten, Methoden oder Pläne gemäß Artikel 6 Absätze 2 und 3 und deren Umsetzung. Die Zusammenarbeit zwischen der ACER, der ENISA und jeder zuständigen Behörde kann über ein Gremium zur Überwachung von Cybersicherheitsrisiken erfolgen.

Artikel 17(1)

Die ACER überwacht in Zusammenarbeit mit jeder zuständigen Behörde

(1) die Umsetzung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit gemäß Artikel 12 Absatz 2 Buchstabe a und der Berichterstattungspflichten gemäß den Artikeln 27 und 39 sowie

(2) das Verfahren zur Annahme der Modalitäten, Methoden oder Pläne gemäß Artikel 6 Absätze 2 und 3 und deren Umsetzung. Die Zusammenarbeit zwischen der ACER, der ENISA und jeder zuständigen Behörde kann über ein Gremium zur Überwachung von Cybersicherheitsrisiken erfolgen.

Artikel 18

1. Bis zum 13 März 2025 legen die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und nach Konsultation der NIS-Kooperationsgruppe einen Vorschlag für die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten vor.
2. Die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten müssen Folgendes umfassen:
   a. eine Liste der zu berücksichtigenden Cyberbedrohungen, einschließlich mindestens der folgenden Bedrohungen der Lieferkette:
      i. schwere und unerwartete Kompromittierung der Lieferkette;
      ii. Nichtverfügbarkeit von IKT-Produkten, -Diensten oder -Prozessen aus der Lieferkette;
      iii. von Akteuren in der Lieferkette ausgelöste Cyberangriffe;
      iv. Weitergabe sensibler Informationen durch die Lieferkette, einschließlich der Nachverfolgung der Lieferkette;
      v. Einführung von Schwachstellen oder Hintertüren in IKT-Produkten, -Diensten oder -Prozessen durch Akteure in der Lieferkette;
   b. die Kriterien für die Einstufung der Auswirkungen von Cybersicherheitsrisiken als erheblich oder kritisch, wobei festgelegte Schwellenwerte für deren Folgen und Wahrscheinlichkeit zu nutzen sind;
   c. einen Ansatz zur Analyse der Cybersicherheitsrisiken, die sich aus Altsystemen, den Kaskadeneffekten von Cyberangriffen und dem Echtzeitcharakter der Netzbetriebssysteme ergeben;
   d. einen Ansatz zur Analyse der Cybersicherheitsrisiken, die sich aus der Abhängigkeit von einem einzigen Anbieter von IKT-Produkten, -Diensten oder -Prozessen ergeben.

3. Die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten müssen dieselbe Risiko-Auswirkungs-Matrix umfassen. Mit der Risiko-Auswirkungs-Matrix

   a. werden die Folgen von Cyberangriffen anhand folgender Kriterien gemessen:
      i. Lastverlust;
      ii. Verringerung der Stromerzeugung;
      iii. Kapazitätsverlust in der primären Frequenzreserve;
      iv. Verlust von Kapazitäten für die Wiederherstellung des Betriebs eines Stromnetzes ohne Rückgriff auf das externe Übertragungsnetz nach einer vollständigen oder teilweisen Abschaltung („Schwarzstart“);
      v. voraussichtliche Dauer eines Stromausfalls mit Auswirkungen auf die Kunden in Verbindung mit dem Ausmaß des Ausfalls (nach Zahl der Kunden) und
      vi. alle sonstigen quantitativen oder qualitativen Kriterien, die als sinnvolle Indikatoren für die Auswirkungen eines Cyberangriffs auf grenzüberschreitende Stromflüsse dienen könnten;
   b. wird die Wahrscheinlichkeit eines Vorfalls als Häufigkeit der Cyberangriffe pro Jahr gemessen.

4. In den Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene wird beschrieben, wie die ECIIS chwellenwerte für erhebliche und kritische Auswirkungen bestimmt werden. Der ECII muss es den Einrichtungen ermöglichen, im Rahmen der von ihnen gemäß Artikel 26 Absatz 4 Buchstabe c Ziffer i durchgeführten Folgenabschätzungen die Auswirkungen der Risiken auf ihre Geschäftsprozesse mithilfe der in Absatz 2 Buchstabe b genannten Kriterien abzuschätzen.

5. ENTSO-E unterrichtet die Koordinierungsgruppe „Strom“ in Abstimmung mit der EU-VNBO über die Vorschläge für die gemäß Absatz 1 zu entwickelnden Methoden zur Bewertung des Cybersicherheitsrisikos.

Artikel 18(1)

Bis zum 13 März 2025 legen die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und nach Konsultation der NIS-Kooperationsgruppe einen Vorschlag für die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten vor.

Artikel 18(2)

Die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten müssen Folgendes umfassen:

a. eine Liste der zu berücksichtigenden Cyberbedrohungen, einschließlich mindestens der folgenden Bedrohungen der Lieferkette:

   i. schwere und unerwartete Kompromittierung der Lieferkette;

ii. Nichtverfügbarkeit von IKT-Produkten, -Diensten oder -Prozessen aus der Lieferkette;
iii. von Akteuren in der Lieferkette ausgelöste Cyberangriffe;
iv. Weitergabe sensibler Informationen durch die Lieferkette, einschließlich der Nachverfolgung der Lieferkette;
v. Einführung von Schwachstellen oder Hintertüren in IKT-Produkten, -Diensten oder -Prozessen durch Akteure in der Lieferkette;

b. die Kriterien für die Einstufung der Auswirkungen von Cybersicherheitsrisiken als erheblich oder kritisch, wobei festgelegte Schwellenwerte für deren Folgen und Wahrscheinlichkeit zu nutzen sind;

c. einen Ansatz zur Analyse der Cybersicherheitsrisiken, die sich aus Altsystemen, den Kaskadeneffekten von Cyberangriffen und dem Echtzeitcharakter der Netzbetriebssysteme ergeben;

d. einen Ansatz zur Analyse der Cybersicherheitsrisiken, die sich aus der Abhängigkeit von einem einzigen Anbieter von IKT-Produkten, -Diensten oder -Prozessen ergeben.

Artikel 18(3)

Die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten müssen dieselbe Risiko-Auswirkungs-Matrix umfassen. Mit der Risiko-Auswirkungs-Matrix

a. werden die Folgen von Cyberangriffen anhand folgender Kriterien gemessen:

i. Lastverlust;
ii. Verringerung der Stromerzeugung;
iii. Kapazitätsverlust in der primären Frequenzreserve;
iv. Verlust von Kapazitäten für die Wiederherstellung des Betriebs eines Stromnetzes ohne Rückgriff auf das externe Übertragungsnetz nach einer vollständigen oder teilweisen Abschaltung („Schwarzstart“);
v. voraussichtliche Dauer eines Stromausfalls mit Auswirkungen auf die Kunden in Verbindung mit dem Ausmaß des Ausfalls (nach Zahl der Kunden) und
vi. alle sonstigen quantitativen oder qualitativen Kriterien, die als sinnvolle Indikatoren für die Auswirkungen eines Cyberangriffs auf grenzüberschreitende Stromflüsse dienen könnten;

b. wird die Wahrscheinlichkeit eines Vorfalls als Häufigkeit der Cyberangriffe pro Jahr gemessen.

Artikel 18(4)

In den Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene wird beschrieben, wie die ECIIS chwellenwerte für erhebliche und kritische Auswirkungen bestimmt werden. Der

ECII muss es den Einrichtungen ermöglichen, im Rahmen der von ihnen gemäß Artikel 26 Absatz 4 Buchstabe c Ziffer i durchgeführten Folgenabschätzungen die Auswirkungen der Risiken auf ihre Geschäftsprozesse mithilfe der in Absatz 2 Buchstabe b genannten Kriterien abzuschätzen.

Artikel 18(5)

ENTSO-E unterrichtet die Koordinierungsgruppe „Strom“ in Abstimmung mit der EU-VNBO über die Vorschläge für die gemäß Absatz 1 zu entwickelnden Methoden zur Bewertung des Cybersicherheitsrisikos.

Artikel 19

1. Innerhalb von neun Monaten nach der Genehmigung der Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 8 und danach alle drei Jahre führt ENTSO-E in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe unbeschadet des Artikels 22 der Richtlinie (EU) 2022/2555 [8] eine unionsweite Bewertung des Cybersicherheitsrisikos durch und erstellt einen Entwurf eines Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos. Dabei wenden sie die gemäß Artikel 18 entwickelten und gemäß Artikel 8 genehmigten Methoden an, um die möglichen Folgen von Cyberangriffen, die sich auf die Betriebssicherheit des Elektrizitätssystems auswirken und grenzüberschreitende Stromflüsse stören, zu ermitteln, zu analysieren und zu bewerten. Bei der unionsweiten Bewertung des Cybersicherheitsrisikos werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.
2. Der Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos muss Folgendes enthalten:
    a. die unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen;
    b. eine Risiko-Auswirkungs-Matrix, die Einrichtungen und die zuständigen Behörden nutzen müssen, um die Cybersicherheitsrisiken zu bewerten, die in der Bewertung des Cybersicherheitsrisikos auf der Ebene der Mitgliedstaaten gemäß Artikel 20 und in der Bewertung des Cybersicherheitsrisikos auf der Ebene von, Einrichtungen gemäß Artikel 26 Absatz 2 Buchstabe b ermittelt wurden.
3. In Bezug auf die unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen muss der Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos Folgendes enthalten:
    a. eine Bewertung der möglichen Folgen eines Cyberangriffs anhand der Parameter, die in der gemäß Artikel 18 Absätze 2, 3 und 4 entwickelten und gemäß Artikel 8 genehmigten Methode zur Bewertung des Cybersicherheitsrisikos festgelegt sind;
    b. den ECII und die Schwellenwerte für erhebliche und kritische Auswirkungen, die die zuständigen Behörden gemäß Artikel 24 Absätze 1 und 2 nutzen müssen, um Einrichtungen mit erheblichen oder kritischen Auswirkungen zu ermitteln, die an unionsweiten Prozessen mit erheblichen bzw. kritischen Auswirkungen beteiligt sind.

[8] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_22

4. ENTSO-E legt der ACER in Zusammenarbeit mit der EU-VNBO den Entwurf des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos mit den Ergebnissen der unionsweiten Bewertung des Cybersicherheitsrisikos zur Stellungnahme vor. Die ACER gibt innerhalb von drei Monaten nach Eingang eine Stellungnahme zu dem Entwurf des Berichts ab. ENTSO-E und die EU-VNBO tragen der Stellungnahme der ACER bei der Fertigstellung dieses Berichts so weit wie möglich Rechnung.
5. Innerhalb von drei Monaten nach Eingang der Stellungnahme der ACER übermittelt ENTSO-E in Zusammenarbeit mit der EU-VNBO der ACER, der Kommission, der ENISA und den zuständigen Behörden den endgültigen Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos.

Artikel 19(1)

Innerhalb von neun Monaten nach der Genehmigung der Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 8 und danach alle drei Jahre führt ENTSO-E in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe unbeschadet des Artikels 22 der Richtlinie (EU) 2022/2555 [9] eine unionsweite Bewertung des Cybersicherheitsrisikos durch und erstellt einen Entwurf eines Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos. Dabei wenden sie die gemäß Artikel 18 entwickelten und gemäß Artikel 8 genehmigten Methoden an, um die möglichen Folgen von Cyberangriffen, die sich auf die Betriebssicherheit des Elektrizitätssystems auswirken und grenzüberschreitende Stromflüsse stören, zu ermitteln, zu analysieren und zu bewerten. Bei der unionsweiten Bewertung des Cybersicherheitsrisikos werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

Artikel 19(2)

Der Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos muss Folgendes enthalten:

a. die unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen;
b. eine Risiko-Auswirkungs-Matrix, die Einrichtungen und die zuständigen Behörden nutzen müssen, um die Cybersicherheitsrisiken zu bewerten, die in der Bewertung des Cybersicherheitsrisikos auf der Ebene der Mitgliedstaaten gemäß Artikel 20 und in der Bewertung des Cybersicherheitsrisikos auf der Ebene von, Einrichtungen gemäß Artikel 26 Absatz 2 Buchstabe b ermittelt wurden.

Artikel 19(3)

In Bezug auf die unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen muss der Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos Folgendes enthalten:

[9] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_22

a. eine Bewertung der möglichen Folgen eines Cyberangriffs anhand der Parameter, die in der gemäß Artikel 18 Absätze 2, 3 und 4 entwickelten und gemäß Artikel 8 genehmigten Methode zur Bewertung des Cybersicherheitsrisikos festgelegt sind;

b. den ECII und die Schwellenwerte für erhebliche und kritische Auswirkungen, die die zuständigen Behörden gemäß Artikel 24 Absätze 1 und 2 nutzen müssen, um Einrichtungen mit erheblichen oder kritischen Auswirkungen zu ermitteln, die an unionsweiten Prozessen mit erheblichen bzw. kritischen Auswirkungen beteiligt sind.

Artikel 19(4)

ENTSO-E legt der ACER in Zusammenarbeit mit der EU-VNBO den Entwurf des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos mit den Ergebnissen der unionsweiten Bewertung des Cybersicherheitsrisikos zur Stellungnahme vor.

Die ACER gibt innerhalb von drei Monaten nach Eingang eine Stellungnahme zu dem Entwurf des Berichts ab. ENTSO-E und die EU-VNBO tragen der Stellungnahme der ACER bei der Fertigstellung dieses Berichts so weit wie möglich Rechnung.

Artikel 19(5)

Innerhalb von drei Monaten nach Eingang der Stellungnahme der ACER übermittelt ENTSO-E in Zusammenarbeit mit der EU-VNBO der ACER, der Kommission, der ENISA und den zuständigen Behörden den endgültigen Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos.

Artikel 2: Anwendungsbereich

1. Diese Verordnung gilt für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse bei den Tätigkeiten der folgenden Einrichtungen, soweit diese gemäß Artikel 24 [10] als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft werden:
   a. Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944; [11]
   b. nominierte Strommarktbetreiber (NEMOs) im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/943; [12]
   c. organisierte Marktplätze oder organisierte Märkte im Sinne des Artikels 2 Nummer 4 der Durchführungsverordnung (EU) Nr. 1348/2014 der Kommission [13] (14), die Transaktionen mit Produkten arrangieren, die für grenzüberschreitende Stromflüsse relevant sind;
   d. Anbieter kritischer IKT-Dienste im Sinne des Artikels 3 Nummer 9 dieser Verordnung [14]

[10] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366
[11] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[12] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[13] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R1348
[14] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_3

e. ENTSO-E, das gemäß Artikel 28 der Verordnung (EU) 2019/943 [15] eingerichtet wurde;

f. die EU-VNBO, die gemäß Artikel 52 der Verordnung (EU) 2019/943 [16] eingerichtet wurde;

g. Bilanzkreisverantwortliche im Sinne des Artikels 2 Nummer 14 der Verordnung (EU) 2019/943; [17]

h. Betreiber von Ladepunkten im Sinne des Anhangs I der Richtlinie (EU) 2022/2555; [18]

i. regionale Koordinierungszentren (RCC) gemäß Artikel 35 der Verordnung (EU) 2019/943; [19]

j. Anbieter verwalteter Sicherheitsdienste (MSSP) gemäß Artikel 6 Nummer 40 der Richtlinie (EU) 2022/2555; [20]

k. alle sonstigen Einrichtungen oder Dritte, denen gemäß dieser Verordnung [21] Zuständigkeiten übertragen oder zugewiesen werden.

2. Die folgenden Behörden sind im Rahmen ihres derzeitigen Auftrags für die Wahrnehmung der in dieser Verordnung [22] festgelegten Aufgaben zuständig:

a. die mit der Verordnung (EU) 2019/942 des Europäischen Parlaments und des Rates [23] eingerichtete Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER)

b. die nationalen zuständigen Behörden, die für die Wahrnehmung der ihnen gemäß dieser Verordnung [24] übertragenen Aufgaben verantwortlich sind und von den Mitgliedstaaten gemäß Artikel 4 als „zuständige Behörde“ benannt wurden;

c. die gemäß Artikel 57 Absatz 1 der Richtlinie (EU) 2019/944; [25] benannten nationalen Regulierungsbehörden (NRB) der einzelnen Mitgliedstaaten;

d. die gemäß Artikel 3 der Verordnung (EU) 2019/941; [26] benannten für die Risikovorsorge zuständigen Behörden (RP-NCA);

e. die gemäß Artikel 10 der Richtlinie (EU) 2022/2555; [27] benannten oder eingerichteten Computer-Notfallteams (CSIRTs);

f. die gemäß Artikel 8 der Richtlinie (EU) 2022/2555; [28] benannten oder eingerichteten für die Cybersicherheit zuständigen Behörden (CS-NCA);

g. die gemäß der Verordnung (EU) 2019/881 [29]; errichtete Agentur der Europäischen Union für Cybersicherheit;

[15] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[16] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[17] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[18] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art
[19] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[20] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366
[21] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366
[22] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366
[23] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942
[24] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[25] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[26] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941
[27] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[28] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[29] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881

h. alle sonstigen Behörden oder Dritte, denen gemäß Artikel 4 Absatz 3 [30] Zuständigkeiten übertragen oder zugewiesen werden.

3. Diese Verordnung gilt auch für alle Einrichtungen, die nicht in der Union niedergelassen sind, aber Dienstleistungen für Einrichtungen in der Union erbringen, sofern sie von den zuständigen Behörden gemäß Artikel 24 Absatz 2 [31] als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

4. Diese Verordnung lässt die Zuständigkeit der Mitgliedstaaten in Bezug auf die Aufrechterhaltung der nationalen Sicherheit und ihre Befugnis zum Schutz anderer wesentlicher staatlicher Funktionen, einschließlich der Wahrung der territorialen Unversehrtheit des Staates und der Aufrechterhaltung der öffentlichen Ordnung, unberührt.

5. Diese Verordnung lässt die Zuständigkeit der Mitgliedstaaten für die Aufrechterhaltung der nationalen Sicherheit in Bezug auf Tätigkeiten zur Stromerzeugung in Kernkraftwerken, einschließlich Tätigkeiten innerhalb der nuklearen Wertschöpfungskette, im Einklang mit den Verträgen unberührt.

6. Soweit dies für die Zwecke dieser Verordnung erforderlich ist, werden personenbezogene Daten von Einrichtungen, den zuständigen Behörden, den zentralen Anlaufstellen auf Ebene der Einrichtung und den CSIRTs im Einklang mit der Verordnung (EU) 2016/679 [32], insbesondere auf der Grundlage von Artikel 6 der genannten Verordnung, verarbeitet.

Artikel 2: Anwendungsbereich

1. Diese Verordnung gilt für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse bei den Tätigkeiten der folgenden Einrichtungen, soweit diese gemäß Artikel 24 [33] als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft werden:

   a. Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944; [34]

   b. nominierte Strommarktbetreiber (NEMOs) im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/943; [35]

   c. organisierte Marktplätze oder organisierte Märkte im Sinne des Artikels 2 Nummer 4 der Durchführungsverordnung (EU) Nr. 1348/2014 der Kommission [36] (14), die Transaktionen mit Produkten arrangieren, die für grenzüberschreitende Stromflüsse relevant sind;

   d. Anbieter kritischer IKT-Dienste im Sinne des Artikels 3 Nummer 9 dieser Verordnung [37]

   e. ENTSO-E, das gemäß Artikel 28 der Verordnung (EU) 2019/943 [38] eingerichtet wurde;

[30] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[31] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366
[32] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679
[33] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[34] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[35] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[36] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R1348
[37] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_3
[38] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943

f. die EU-VNBO, die gemäß Artikel 52 der Verordnung (EU) 2019/943 [39] eingerichtet wurde;
g. Bilanzkreisverantwortliche im Sinne des Artikels 2 Nummer 14 der Verordnung (EU) 2019/943; [40]
h. Betreiber von Ladepunkten im Sinne des Anhangs I der Richtlinie (EU) 2022/2555; [41]
i. regionale Koordinierungszentren (RCC) gemäß Artikel 35 der Verordnung (EU) 2019/943; [42]
j. Anbieter verwalteter Sicherheitsdienste (MSSP) gemäß Artikel 6 Nummer 40 der Richtlinie (EU) 2022/2555; [43]
k. alle sonstigen Einrichtungen oder Dritte, denen gemäß dieser Verordnung [44] Zuständigkeiten übertragen oder zugewiesen werden.

Artikel 2: Anwendungsbereich

1. Die folgenden Behörden sind im Rahmen ihres derzeitigen Auftrags für die Wahrnehmung der in dieser Verordnung [45] festgelegten Aufgaben zuständig:
   a. die mit der Verordnung (EU) 2019/942 des Europäischen Parlaments und des Rates [46] eingerichtete Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER)
   b. die nationalen zuständigen Behörden, die für die Wahrnehmung der ihnen gemäß dieser Verordnung [47] übertragenen Aufgaben verantwortlich sind und von den Mitgliedstaaten gemäß Artikel 4 als „zuständige Behörde“ benannt wurden;
   c. die gemäß Artikel 57 Absatz 1 der Richtlinie (EU) 2019/944; [48] benannten nationalen Regulierungsbehörden (NRB) der einzelnen Mitgliedstaaten;
   d. die gemäß Artikel 3 der Verordnung (EU) 2019/941; [49] benannten für die Risikovorsorge zuständigen Behörden (RP-NCA);
   e. die gemäß Artikel 10 der Richtlinie (EU) 2022/2555; [50] benannten oder eingerichteten Computer-Notfallteams (CSIRTs);
   f. die gemäß Artikel 8 der Richtlinie (EU) 2022/2555; [51] benannten oder eingerichteten für die Cybersicherheit zuständigen Behörden (CS-NCA);
   g. die gemäß der Verordnung (EU) 2019/881 [52]; errichtete Agentur der Europäischen Union für Cybersicherheit;

[39] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[40] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[41] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art
[42] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[43] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[44] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[45] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[46] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942
[47] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[48] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[49] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941
[50] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[51] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[52] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881

h. alle sonstigen Behörden oder Dritte, denen gemäß Artikel 4 Absatz 3 [53] Zuständigkeiten übertragen oder zugewiesen werden.

2. Diese Verordnung gilt auch für alle Einrichtungen, die nicht in der Union niedergelassen sind, aber Dienstleistungen für Einrichtungen in der Union erbringen, sofern sie von den zuständigen Behörden gemäß Artikel 24 Absatz 2 [54] als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

3. Diese Verordnung lässt die Zuständigkeit der Mitgliedstaaten in Bezug auf die Aufrechterhaltung der nationalen Sicherheit und ihre Befugnis zum Schutz anderer wesentlicher staatlicher Funktionen, einschließlich der Wahrung der territorialen Unversehrtheit des Staates und der Aufrechterhaltung der öffentlichen Ordnung, unberührt.

4. Diese Verordnung lässt die Zuständigkeit der Mitgliedstaaten für die Aufrechterhaltung der nationalen Sicherheit in Bezug auf Tätigkeiten zur Stromerzeugung in Kernkraftwerken, einschließlich Tätigkeiten innerhalb der nuklearen Wertschöpfungskette, im Einklang mit den Verträgen unberührt.

5. Soweit dies für die Zwecke dieser Verordnung erforderlich ist, werden personenbezogene Daten von Einrichtungen, den zuständigen Behörden, den zentralen Anlaufstellen auf Ebene der Einrichtung und den CSIRTs im Einklang mit der Verordnung (EU) 2016/679 [55], insbesondere auf der Grundlage von Artikel 6 der genannten Verordnung, verarbeitet.

Artikel 20

1. Jede zuständige Behörde führt in Bezug auf alle Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat eine Bewertung des Cybersicherheitsrisikos des Mitgliedstaats durch und nutzt dabei die gemäß Artikel 18 entwickelten und gemäß Artikel 8 genehmigten Methoden. Bei der Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten werden die Risiken von Cyberangriffen ermittelt und analysiert, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören. Bei der Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

2. Innerhalb von 21 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre übermittelt jede zuständige Behörde mit Unterstützung des CSIRT und nach Konsultation der für Elektrizität zuständigen CS-NCA dem ENTSO-E und der EU-VNBO einen Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats, der in Bezug auf jeden Geschäftsprozess mit erheblichen oder kritischen Auswirkungen folgende Informationen enthält:

   a. den Stand der Umsetzung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskorntrollen gemäß Artikel 29;

[53] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[54] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[55] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679

b. eine Liste aller in den letzten drei Jahren gemäß Artikel 38 Absatz 3 gemeldeten Cyberangriffe;

c. eine Zusammenfassung aller in den letzten drei Jahren gemäß Artikel 38 Absatz 6 gemeldeten Informationen zu Cyberbedrohungen;

d. für jeden unionsweiten Prozess mit erheblichen oder kritischen Auswirkungen eine Schätzung der mit einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten verbundenen Risiken;

e. erforderlichenfalls eine Liste zusätzlicher Einrichtungen, die gemäß Artikel 24 Absätze 1, 2, 3 und 5 als Einrichtungen mit erheblichen oder kritischen Auswirkungen ermittelt wurden.

3. Der Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats muss dem gemäß Artikel 10 der Verordnung (EU) 2019/941 [56] erstellten Risikovorsorgeplan des Mitgliedstaats Rechnung tragen.

4. Die Informationen in dem Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats gemäß Absatz 2 Buchstaben a bis d dürfen nicht mit bestimmten Einrichtungen oder Vermögenswerten verknüpft sein. In dem Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats sind auch die Risiken im Zusammenhang mit den von den zuständigen Behörden der Mitgliedstaaten gemäß Artikel 30 gewährten befristeten Ausnahmen zu bewerten.

5. ENTSO-E und die EU-VNBO können im Zusammenhang mit den in Unterabsatz 2 Buchstaben a und c genannten Aufgaben die zuständigen Behörden um zusätzliche Informationen ersuchen.

6. Die zuständigen Behörden stellen sicher, dass die von ihnen bereitgestellten Informationen genau und zutreffend sind.

Artikel 20(1)

Jede zuständige Behörde führt in Bezug auf alle Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat eine Bewertung des Cybersicherheitsrisikos des Mitgliedstaats durch und nutzt dabei die gemäß Artikel 18 entwickelten und gemäß Artikel 8 genehmigten Methoden. Bei der Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten werden die Risiken von Cyberangriffen ermittelt und analysiert, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören. Bei der Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

Artikel 20(2)

Innerhalb von 21 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre übermittelt jede

[56] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e928-1-1

zuständige Behörde mit Unterstützung des CSIRT und nach Konsultation der für Elektrizität zuständigen CS-NCA dem ENTSO-E und der EU-VNBO einen Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats, der in Bezug auf jeden Geschäftsprozess mit erheblichen oder kritischen Auswirkungen folgende Informationen enthält:

a. den Stand der Umsetzung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskorntrollen gemäß Artikel 29;

b. eine Liste aller in den letzten drei Jahren gemäß Artikel 38 Absatz 3 gemeldeten Cyberangriffe;

c. eine Zusammenfassung aller in den letzten drei Jahren gemäß Artikel 38 Absatz 6 gemeldeten Informationen zu Cyberbedrohungen;

d. für jeden unionsweiten Prozess mit erheblichen oder kritischen Auswirkungen eine Schätzung der mit einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten verbundenen Risiken;

e. erforderlichenfalls eine Liste zusätzlicher Einrichtungen, die gemäß Artikel 24 Absätze 1, 2, 3 und 5 als Einrichtungen mit erheblichen oder kritischen Auswirkungen ermittelt wurden.

Artikel 20(3)

Der Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats muss dem gemäß Artikel 10 der Verordnung (EU) 2019/941 [57] erstellten Risikovorsorgeplan des Mitgliedstaats Rechnung tragen.

Artikel 20(4)

Die Informationen in dem Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats gemäß Absatz 2 Buchstaben a bis d dürfen nicht mit bestimmten Einrichtungen oder Vermögenswerten verknüpft sein. In dem Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats sind auch die Risiken im Zusammenhang mit den von den zuständigen Behörden der Mitgliedstaaten gemäß Artikel 30 gewährten befristeten Ausnahmen zu bewerten.

Artikel 20(5)

ENTSO-E und die EU-VNBO können im Zusammenhang mit den in Unterabsatz 2 Buchstaben a und c genannten Aufgaben die zuständigen Behörden um zusätzliche Informationen ersuchen.

Artikel 20(6)

[57] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e928-1-1

Die zuständigen Behörden stellen sicher, dass die von ihnen bereitgestellten Informationen genau und zutreffend sind.

Artikel 21

1. ENTSO-E führt in Zusammenarbeit mit der EU-VNBO und in Absprache mit dem zuständigen regionalen Koordinierungszentrum für jede Netzbetriebsregion eine regionale Bewertung des Cybersicherheitsrisikos durch und nutzt dabei die gemäß Artikel 19 entwickelten und gemäß Artikel 8 genehmigten Methoden, um die Risiken von Cyberangriffen, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören, zu ermitteln, zu analysieren und zu bewerten. Bei der regionalen Bewertung des Cybersicherheitsrisikos werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.
2. Innerhalb von 30 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe für jede Netzbetriebsregion einen Bericht über die regionale Bewertung des Cybersicherheitsrisikos.
3. Der Bericht über die regionale Bewertung des Cybersicherheitsrisikos muss den einschlägigen Informationen Rechnung tragen, die in den Berichten über die unionsweite Bewertung des Cybersicherheitsrisikos und in den Berichten der Mitgliedstaaten über die Bewertung des Cybersicherheitsrisikos enthalten sind.
4. Bei der regionalen Bewertung des Cybersicherheitsrisikos werden die gemäß Artikel 6 der Verordnung (EU) 2019/941 [58] bestimmten regionalen Szenarien für Stromversorgungskrisen im Bereich der Cybersicherheit berücksichtigt.

Artikel 21(1)

ENTSO-E führt in Zusammenarbeit mit der EU-VNBO und in Absprache mit dem zuständigen regionalen Koordinierungszentrum für jede Netzbetriebsregion eine regionale Bewertung des Cybersicherheitsrisikos durch und nutzt dabei die gemäß Artikel 19 entwickelten und gemäß Artikel 8 genehmigten Methoden, um die Risiken von Cyberangriffen, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören, zu ermitteln, zu analysieren und zu bewerten. Bei der regionalen Bewertung des Cybersicherheitsrisikos werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

Artikel 21(2)

Innerhalb von 30 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre erstellt ENTSO-E in

[58] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e698-1-1

Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe für jede Netzbetriebsregion einen Bericht über die regionale Bewertung des Cybersicherheitsrisikos.

Artikel 21(3)

Der Bericht über die regionale Bewertung des Cybersicherheitsrisikos muss den einschlägigen Informationen Rechnung tragen, die in den Berichten über die unionsweite Bewertung des Cybersicherheitsrisikos und in den Berichten der Mitgliedstaaten über die Bewertung des Cybersicherheitsrisikos enthalten sind.

Artikel 21(4)

Bei der regionalen Bewertung des Cybersicherheitsrisikos werden die gemäß Artikel 6 der Verordnung (EU) 2019/941 [59] bestimmten regionalen Szenarien für Stromversorgungskrisen im Bereich der Cybersicherheit berücksichtigt.

Artikel 22

1. Innerhalb von 36 Monaten nach Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6, spätestens jedoch am 13 Juni 2031, und danach alle drei Jahre erstellen die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit den regionalen Koordinierungszentren und der NIS-Kooperationsgruppe für jede Netzbetriebsregion einen regionalen Plan zur Minderung des Cybersicherheitsrisikos.
2. Die regionalen Pläne zur Minderung des Cybersicherheitsrisikos müssen Folgendes enthalten:
   a. die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen, die die Einrichtungen mit erheblichen bzw. kritischen Auswirkungen in der Netzbetriebsregion anwenden müssen;
   b. die verbleibenden Cybersicherheitsrisiken in den Netzbetriebsregionen nach Anwendung der unter Buchstabe a genannten Kontrollen.
3. ENTSO-E legt die regionalen Pläne zur Minderung des Cybersicherheitsrisikos den relevanten Übertragungsnetzbetreibern, den zuständigen Behörden und der Koordinierungsgruppe „Strom“ vor. Die Koordinierungsgruppe „Strom“ kann Änderungen empfehlen.
4. Die ÜNB aktualisieren mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe die regionalen Risikominderungspläne alle drei Jahre, soweit aufgrund der Umstände keine häufigere Aktualisierung erforderlich ist.

Artikel 22(1)

[59] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e698-1-1

Innerhalb von 36 Monaten nach Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6, spätestens jedoch am 13 Juni 2031, und danach alle drei Jahre erstellen die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit den regionalen Koordinierungszentren und der NIS-Kooperationsgruppe für jede Netzbetriebsregion einen regionalen Plan zur Minderung des Cybersicherheitsrisikos.

Artikel 22(2)

Die regionalen Pläne zur Minderung des Cybersicherheitsrisikos müssen Folgendes enthalten:

a. die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen, die die Einrichtungen mit erheblichen bzw. kritischen Auswirkungen in der Netzbetriebsregion anwenden müssen;
b. die verbleibenden Cybersicherheitsrisiken in den Netzbetriebsregionen nach Anwendung der unter Buchstabe a genannten Kontrollen.

Artikel 22(3)

ENTSO-E legt die regionalen Pläne zur Minderung des Cybersicherheitsrisikos den relevanten Übertragungsnetzbetreibern, den zuständigen Behörden und der Koordinierungsgruppe „Strom“ vor. Die Koordinierungsgruppe „Strom“ kann Änderungen empfehlen.

Artikel 22(4)

Die ÜNB aktualisieren mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe die regionalen Risikominderungspläne alle drei Jahre, soweit aufgrund der Umstände keine häufigere Aktualisierung erforderlich ist.

Artikel 23

1. Innerhalb von 40 Monaten nach Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre übermitteln die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe der Koordinierungsgruppe „Strom“ einen Bericht über die Ergebnisse der Bewertung der Cybersicherheitsrisiken in Bezug auf grenzüberschreitende Stromflüsse (im Folgenden „umfassender Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse“).
2. Der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse stützt sich auf den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos, die Berichte der Mitgliedstaaten über die Bewertung des Cybersicherheitsrisikos und die Berichte über die regionale Bewertung des Cybersicherheitsrisikos und muss folgende Informationen enthalten:

a. die Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen, die im Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 2 Buchstabe a ermittelt wurden, einschließlich der Schätzung der Wahrscheinlichkeit und der Auswirkungen von Cybersicherheitsrisiken, die in den Berichten über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 und Artikel 19 Absatz 3 Buchstabe a bewertet wurden;

b. aktuelle Cyberbedrohungen, insbesondere neu aufkommende Bedrohungen und Risiken für das Elektrizitätssystem;

c. Cyberangriffe im vorangegangenen Zeitraum auf Unionsebene mit einem kritischen Überblick darüber, wie sich diese Cyberangriffe auf grenzüberschreitende Stromflüsse ausgewirkt haben könnten;

d. allgemeiner Stand der Umsetzung der Cybersicherheitsmaßnahmen;

e. Stand der Umsetzung der Informationsflüsse gemäß den Artikeln 37 und 38;

f. Liste der Informationen oder spezifische Kriterien für die Klassifizierung von Informationen gemäß Artikel 46;

g. ermittelte und besonders zu beachtende Risiken, die sich aus einem unsicheren Lieferkettenmanagement ergeben können;

h. Ergebnisse der regionalen und überregionalen Cybersicherheitsübungen gemäß Artikel 44 und dabei insgesamt gewonnene Erfahrungen;

i. eine Analyse der Entwicklung des allgemeinen Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse seit den letzten regionalen Bewertungen des Cybersicherheitsrisikos;

j. alle sonstigen Informationen, die nützlich sein können, um mögliche Verbesserungen dieser Verordnung oder die Notwendigkeit einer Überarbeitung dieser Verordnung oder ihrer Instrumente zu ermitteln, sowie

k. aggregierte und anonymisierte Informationen über die gemäß Artikel 30 Absatz 3 gewährten Ausnahmen.

3. Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen können zur Ausarbeitung des umfassenden Berichts über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse beitragen, wobei sie die Vertraulichkeit der Informationen gemäß Artikel 47 wahren müssen. Die ÜNB konsultieren diese Einrichtungen mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO frühzeitig.

4. Der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse unterliegt den Bestimmungen des Artikels 46 über den Schutz ausgetauschter Informationen. Unbeschadet des Artikels 10 Absatz 4 und des Artikels 47 Absatz 4 veröffentlichen ENTSO-E und die EU-VNBO eine öffentliche Fassung dieses Berichts, die keine Informationen enthält, die den in Artikel 2 Absatz 1 aufgeführten Einrichtungen schaden können. Die öffentliche Fassung dieses Berichts wird nur mit Zustimmung der NIS-Kooperationsgruppe und der Koordinierungsgruppe „Strom“ veröffentlicht. ENTSO-E ist in Abstimmung mit der EU-VNBO für die Zusammenstellung und Veröffentlichung der öffentlichen Fassung des Berichts verantwortlich.

Artikel 23(1)

Innerhalb von 40 Monaten nach Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre übermitteln die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe der Koordinierungsgruppe „Strom" einen Bericht über die Ergebnisse der Bewertung der Cybersicherheitsrisiken in Bezug auf grenzüberschreitende Stromflüsse (im Folgenden „umfassender Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse").

Artikel 23(2)

Der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse stützt sich auf den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos, die Berichte der Mitgliedstaaten über die Bewertung des Cybersicherheitsrisikos und die Berichte über die regionale Bewertung des Cybersicherheitsrisikos und muss folgende Informationen enthalten:

a. die Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen, die im Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 2 Buchstabe a ermittelt wurden, einschließlich der Schätzung der Wahrscheinlichkeit und der Auswirkungen von Cybersicherheitsrisiken, die in den Berichten über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 und Artikel 19 Absatz 3 Buchstabe a bewertet wurden;

b. aktuelle Cyberbedrohungen, insbesondere neu aufkommende Bedrohungen und Risiken für das Elektrizitätssystem;

c. Cyberangriffe im vorangegangenen Zeitraum auf Unionsebene mit einem kritischen Überblick darüber, wie sich diese Cyberangriffe auf grenzüberschreitende Stromflüsse ausgewirkt haben könnten;

d. allgemeiner Stand der Umsetzung der Cybersicherheitsmaßnahmen;

e. Stand der Umsetzung der Informationsflüsse gemäß den Artikeln 37 und 38;

f. Liste der Informationen oder spezifische Kriterien für die Klassifizierung von Informationen gemäß Artikel 46;

g. ermittelte und besonders zu beachtende Risiken, die sich aus einem unsicheren Lieferkettenmanagement ergeben können;

h. Ergebnisse der regionalen und überregionalen Cybersicherheitsübungen gemäß Artikel 44 und dabei insgesamt gewonnene Erfahrungen;

i. eine Analyse der Entwicklung des allgemeinen Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse seit den letzten regionalen Bewertungen des Cybersicherheitsrisikos;

j. alle sonstigen Informationen, die nützlich sein können, um mögliche Verbesserungen dieser Verordnung oder die Notwendigkeit einer Überarbeitung dieser Verordnung oder ihrer Instrumente zu ermitteln, sowie

k. aggregierte und anonymisierte Informationen über die gemäß Artikel 30 Absatz 3 gewährten Ausnahmen.

Artikel 23(3)

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen können zur Ausarbeitung des umfassenden Berichts über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse beitragen, wobei sie die Vertraulichkeit der Informationen gemäß Artikel 47 wahren müssen. Die ÜNB konsultieren diese Einrichtungen mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO frühzeitig.

Artikel 23(4)

Der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse unterliegt den Bestimmungen des Artikels 46 über den Schutz ausgetauschter Informationen. Unbeschadet des Artikels 10 Absatz 4 und des Artikels 47 Absatz 4 veröffentlichen ENTSO-E und die EU-VNBO eine öffentliche Fassung dieses Berichts, die keine Informationen enthält, die den in Artikel 2 Absatz 1 aufgeführten Einrichtungen schaden können.

Die öffentliche Fassung dieses Berichts wird nur mit Zustimmung der NIS-Kooperationsgruppe und der Koordinierungsgruppe „Strom“ veröffentlicht. ENTSO-E ist in Abstimmung mit der EU-VNBO für die Zusammenstellung und Veröffentlichung der öffentlichen Fassung des Berichts verantwortlich.

Artikel 24

1. Jede zuständige Behörde ermittelt anhand des ECII und der Schwellenwerte für erhebliche und kritische Auswirkungen, die im Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 3 Buchstabe b enthalten sind, die Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat, die an unionsweiten Prozessen mit erheblichen bzw. kritischen Auswirkungen beteiligt sind. Die zuständigen Behörden können von einer Einrichtung in ihrem Mitgliedstaat Informationen anfordern, um die ECII-Werte für diese Einrichtung zu bestimmen. Liegt der ermittelte ECII einer Einrichtung über dem Schwellenwert für erhebliche oder kritische Auswirkungen, wird die ermittelte Einrichtung in dem in Artikel 20 Absatz 2 genannten Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats aufgeführt.
2. Jede zuständige Behörde ermittelt anhand des ECII und der Schwellenwerte für erhebliche und kritische Auswirkungen aus dem Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 3 Buchstabe b die nicht in der Union niedergelassenen Einrichtungen mit erheblichen oder kritischen Auswirkungen, soweitsie in der Union tätig sind. Die zuständige Behörde kann von einer nicht in der Union niedergelassenen Einrichtung Informationen anfordern, um die ECII-Werte für die Einrichtung zu bestimmen.
3. Jede zuständige Behörde kann weitere Einrichtungen in ihrem Mitgliedstaat als Einrichtun-

gen mit erheblichen oder kritischen Auswirkungen einstufen, wenn die folgenden Kriterien erfüllt sind:

a. Die Einrichtung ist Teil einer Gruppe von Einrichtungen, für die ein erhebliches Risiko besteht, dass sie zeitgleich Ziel eines Cyberangriffs sein könnten;
b. der über die Gruppe von Einrichtungen aggregierte ECII liegt über dem Schwellenwert für erhebliche oder kritische Auswirkungen.

4. Ermittelt eine zuständige Behörde gemäß Absatz 3 zusätzliche Einrichtungen, so gelten alle Prozesse dieser Einrichtungen, deren über die Gruppe aggregierter ECII über dem Schwellenwert für erhebliche Auswirkungen liegt, als Prozesse mit erheblichen Auswirkungen, und alle Prozesse, deren über die Gruppe aggregierter ECII über den Schwellenwerten für kritische Auswirkungen liegt, gelten als Prozesse mit kritischen Auswirkungen.

5. Ermittelt eine zuständige Behörde Einrichtungen gemäß Absatz 3 Buchstabe a in mehr als einem Mitgliedstaat, so unterrichtet sie die anderen zuständigen Behörden, ENTSO-E und die EU-VNBO. ENTSO-E übermittelt den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO auf der Grundlage der von allen zuständigen Behörden übermittelten Informationen eine Analyse der Aggregierung von Einrichtungen in mehr als einem Mitgliedstaat, die zu einer von verschiedenen Punkten ausgehenden Störung der grenzüberschreitenden Stromflüsse führen und einen Cyberangriff nach sich ziehen können. Wird eine Gruppe von Einrichtungen in mehreren Mitgliedstaaten als Aggregierung ermittelt, deren ECII über dem Schwellenwert für erhebliche oder kritische Auswirkungen liegt, so stufen alle betroffenen zuständigen Behörden die Einrichtungen in dieser Gruppe für ihren jeweiligen Mitgliedstaat auf der Grundlage des aggregierten ECII für die Gruppe der Einrichtungen als Einrichtungen mit erheblichen bzw. kritischen Auswirkungen ein, und die ermittelten Einrichtungen werden in den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos aufgenommen.

6. Jede zuständige Behörde unterrichtet innerhalb von neun Monaten, nachdem ENTSO-E und die EU-VNBO den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 5 übermittelt haben, spätestens jedoch bis zum 13 Juni 2028, die in der Liste aufgeführten Einrichtungen, dass sie in ihrem Mitgliedstaat als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

7. Wird einer zuständigen Behörde ein Diensteanbieter als Anbieter kritischer IKT-Dienste gemäß Artikel 27 Buchstabe c gemeldet, so teilt sie dies den zuständigen Behörden der Mitgliedstaaten mit, in deren Hoheitsgebiet sich der Sitz oder der Vertreter befindet. Die letztgenannte zuständige Behörde teilt dem Diensteanbieter mit, dass er als Anbieter kritischer Dienste eingestuft wurde.

Artikel 24(1)

Jede zuständige Behörde ermittelt anhand des ECII und der Schwellenwerte für erhebliche und kritische Auswirkungen, die im Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 3 Buchstabe b enthalten sind, die Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat, die an unionsweiten Prozessen mit erheblichen bzw. kritischen Auswirkungen beteiligt sind. Die zuständigen Behörden können von einer

Einrichtung in ihrem Mitgliedstaat Informationen anfordern, um die ECII-Werte für diese Einrichtung zu bestimmen. Liegt der ermittelte ECII einer Einrichtung über dem Schwellenwert für erhebliche oder kritische Auswirkungen, wird die ermittelte Einrichtung in dem in Artikel 20 Absatz 2 genannten Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats aufgeführt.

Artikel 24(2)

Jede zuständige Behörde ermittelt anhand des ECII und der Schwellenwerte für erhebliche und kritische Auswirkungen aus dem Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 3 Buchstabe b die nicht in der Union niedergelassenen Einrichtungen mit erheblichen oder kritischen Auswirkungen, soweitsie in der Union tätig sind. Die zuständige Behörde kann von einer nicht in der Union niedergelassenen Einrichtung Informationen anfordern, um die ECII-Werte für die Einrichtung zu bestimmen.

Artikel 24(3)

Jede zuständige Behörde kann weitere Einrichtungen in ihrem Mitgliedstaat als Einrichtungen mit erheblichen oder kritischen Auswirkungen einstufen, wenn die folgenden Kriterien erfüllt sind:

a. Die Einrichtung ist Teil einer Gruppe von Einrichtungen, für die ein erhebliches Risiko besteht, dass sie zeitgleich Ziel eines Cyberangriffs sein könnten;

b. der über die Gruppe von Einrichtungen aggregierte ECII liegt über dem Schwellenwert für erhebliche oder kritische Auswirkungen.

Artikel 24(4)

Ermittelt eine zuständige Behörde gemäß Absatz 3 zusätzliche Einrichtungen, so gelten alle Prozesse dieser Einrichtungen, deren über die Gruppe aggregierter ECII über dem Schwellenwert für erhebliche Auswirkungen liegt, als Prozesse mit erheblichen Auswirkungen, und alle Prozesse, deren über die Gruppe aggregierter ECII über den Schwellenwerten für kritische Auswirkungen liegt, gelten als Prozesse mit kritischen Auswirkungen.

Artikel 24(5)

Ermittelt eine zuständige Behörde Einrichtungen gemäß Absatz 3 Buchstabe a in mehr als einem Mitgliedstaat, so unterrichtet sie die anderen zuständigen Behörden, ENTSO-E und die EU-VNBO.

ENTSO-E übermittelt den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO auf der Grundlage der von allen zuständigen Behörden übermittelten Informationen eine Analyse der Aggregierung von Einrichtungen in mehr als einem Mitgliedstaat, die zu einer von verschiede-

nen Punkten ausgehenden Störung der grenzüberschreitenden Stromflüsse führen und einen Cyberangriff nach sich ziehen können.

Wird eine Gruppe von Einrichtungen in mehreren Mitgliedstaaten als Aggregierung ermittelt, deren ECII über dem Schwellenwert für erhebliche oder kritische Auswirkungen liegt, so stufen alle betroffenen zuständigen Behörden die Einrichtungen in dieser Gruppe für ihren jeweiligen Mitgliedstaat auf der Grundlage des aggregierten ECII für die Gruppe der Einrichtungen als Einrichtungen mit erheblichen bzw. kritischen Auswirkungen ein, und die ermittelten Einrichtungen werden in den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos aufgenommen.

Artikel 24(6)

Jede zuständige Behörde unterrichtet innerhalb von neun Monaten, nachdem ENTSO-E und die EU-VNBO den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 5 übermittelt haben, spätestens jedoch bis zum 13 Juni 2028, die in der Liste aufgeführten Einrichtungen, dass sie in ihrem Mitgliedstaat als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

Artikel 24(7)

Wird einer zuständigen Behörde ein Diensteanbieter als Anbieter kritischer IKT-Dienste gemäß Artikel 27 Buchstabe c gemeldet, so teilt sie dies den zuständigen Behörden der Mitgliedstaaten mit, in deren Hoheitsgebiet sich der Sitz oder der Vertreter befindet. Die letztgenannte zuständige Behörde teilt dem Diensteanbieter mit, dass er als Anbieter kritischer Dienste eingestuft wurde.

Artikel 25

1. Die zuständigen Behörden können ein nationales Überprüfungssystem einrichten, um zu überprüfen, ob die gemäß Artikel 24 Absatz 1 ermittelten Einrichtungen mit kritischen Auswirkungen den nationalen Rechtsrahmen umgesetzt haben, der in der Vergleichsmatrix gemäß Artikel 34 aufgeführt ist. Das nationale Überprüfungssystem kann sich auf eine von der zuständigen Behörde durchgeführte Inspektion, unabhängige Sicherheitsaudits oder gegenseitige Peer Reviews durch Einrichtungen mit kritischen Auswirkungen in demselben Mitgliedstaat, die von der zuständigen Behörde beaufsichtigt werden, stützen.
2. Beschließt eine zuständige Behörde, ein nationales Überprüfungssystem einzurichten, so stellt sie sicher, dass die Überprüfung nach den folgenden Anforderungen durchgeführt wird:
    a. Jede Partei, die die Peer Review, das Audit oder die Inspektion durchführt, muss von der zu überprüfenden Einrichtung mit kritischen Auswirkungen unabhängig sein und darf sich nicht in einem Interessenkonflikt befinden;
    b. das Personal, das die Peer Reviews, Audits oder Inspektionen durchführt, muss nachweislich Kenntnisse haben über
        i. die Cybersicherheit im Elektrizitätssektor;

ii. Cybersicherheitsmanagementsysteme;
iii. Audit-Grundsätze;
iv. die Bewertung von Cybersicherheitsrisiken;
v. den gemeinsamen Rahmen für die Cybersicherheit im Elektrizitätssektor;
vi. den nationalen Rechts- und Verwaltungsrahmen sowie europäische und internationale Normen, die für die Überprüfung relevant sind;
vii. die Prozesse mit kritischen Auswirkungen, die Gegenstand der Überprüfung sind;

c. die Partei, die die Peer Reviews, Audits oder Inspektionen durchführt, erhält ausreichend Zeit für die Durchführung dieser Tätigkeiten;
d. die Partei, die die Peer Reviews, Audits oder Inspektionen durchführt, ergreift geeignete Maßnahmen, um die bei der Überprüfung erhobenen Informationen im Einklang mit ihrem Vertraulichkeitsgrad zu schützen, und
e. Peer Reviews, Audits oder Inspektionen werden mindestens einmal jährlich durchgeführt und umfassen mindestens alle drei Jahre den gesamten Prüfumfang.

3. Beschließt eine zuständige Behörde, ein nationales Überprüfungssystem einzurichten, so teilt sie der ACER jährlich mit, wie oft sie Inspektionen im Rahmen dieses Systems durchgeführt hat.

Artikel 25(1)

Die zuständigen Behörden können ein nationales Überprüfungssystem einrichten, um zu überprüfen, ob die gemäß Artikel 24 Absatz 1 ermittelten Einrichtungen mit kritischen Auswirkungen den nationalen Rechtsrahmen umgesetzt haben, der in der Vergleichsmatrix gemäß Artikel 34 aufgeführt ist. Das nationale Überprüfungssystem kann sich auf eine von der zuständigen Behörde durchgeführte Inspektion, unabhängige Sicherheitsaudits oder gegenseitige Peer Reviews durch Einrichtungen mit kritischen Auswirkungen in demselben Mitgliedstaat, die von der zuständigen Behörde beaufsichtigt werden, stützen.

Artikel 25(2)

Beschließt eine zuständige Behörde, ein nationales Überprüfungssystem einzurichten, so stellt sie sicher, dass die Überprüfung nach den folgenden Anforderungen durchgeführt wird:

a. Jede Partei, die die Peer Review, das Audit oder die Inspektion durchführt, muss von der zu überprüfenden Einrichtung mit kritischen Auswirkungen unabhängig sein und darf sich nicht in einem Interessenkonflikt befinden;
b. das Personal, das die Peer Reviews, Audits oder Inspektionen durchführt, muss nachweislich Kenntnisse haben über
   i. die Cybersicherheit im Elektrizitätssektor;
   ii. Cybersicherheitsmanagementsysteme;
   iii. Audit-Grundsätze;

iv. die Bewertung von Cybersicherheitsrisiken;

v. den gemeinsamen Rahmen für die Cybersicherheit im Elektrizitätssektor;

vi. den nationalen Rechts- und Verwaltungsrahmen sowie europäische und internationale Normen, die für die Überprüfung relevant sind;

vii. die Prozesse mit kritischen Auswirkungen, die Gegenstand der Überprüfung sind;

c. die Partei, die die Peer Reviews, Audits oder Inspektionen durchführt, erhält ausreichend Zeit für die Durchführung dieser Tätigkeiten;

d. die Partei, die die Peer Reviews, Audits oder Inspektionen durchführt, ergreift geeignete Maßnahmen, um die bei der Überprüfung erhobenen Informationen im Einklang mit ihrem Vertraulichkeitsgrad zu schützen, und

e. Peer Reviews, Audits oder Inspektionen werden mindestens einmal jährlich durchgeführt und umfassen mindestens alle drei Jahre den gesamten Prüfumfang.

Artikel 25(3)

Beschließt eine zuständige Behörde, ein nationales Überprüfungssystem einzurichten, so teilt sie der ACER jährlich mit, wie oft sie Inspektionen im Rahmen dieses Systems durchgeführt hat.

Artikel 26

1. Jede von den zuständigen Behörden gemäß Artikel 24 Absatz 1 ermittelte Einrichtung mit erheblichen oder kritischen Auswirkungen führt das Cybersicherheitsrisikomanagement für alle ihre Vermögenswerte in ihren Perimetern mit erheblichen oder kritischen Auswirkungen durch. Jede Einrichtung mit erheblichen oder kritischen Auswirkungen führt alle drei Jahre ein Risikomanagement durch, das die in Absatz 2 genannten Phasen umfasst.

2. Jede Einrichtung mit erheblichen oder kritischen Auswirkungen stützt ihr Cybersicherheitsrisikomanagement auf einen Ansatz, der auf den Schutz ihrer Netz- und Informationssysteme abzielt und folgende Phasen umfasst:

   a. Bestimmung des Kontexts;

   b. Bewertung des Cybersicherheitsrisikos auf der Ebene der Einrichtung;

   c. Behandlung von Cybersicherheitsrisiken;

   d. Akzeptanz von Cybersicherheitsrisiken.

3. Bei der Bestimmung des Kontexts trifft jede Einrichtung mit erheblichen oder kritischen Auswirkungen folgende Maßnahmen:

   a. Festlegung des Umfangs der Bewertung des Cybersicherheitsrisikos, einschließlich der von ENTSO-E und der EU-VNBO ermittelten Prozesse mit erheblichen oder kritischen Auswirkungen sowie anderer Prozesse, die Ziel von Cyberangriffen mit erheblichen oder kritischen Auswirkungen auf grenzüberschreitende Stromflüsse sein können, und

b. Festlegung der Kriterien für die Risikobewertung und die Risikoakzeptanz im Einklang mit der Risiko-AuswirkungsMatrix, die Einrichtungen und die zuständigen Behörden nach den von ENTSO-E und der EU-VNBO gemäß Artikel 19 Absatz 2 entwickelten Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf Ebene der Mitgliedstaaten nutzen müssen, um Cybersicherheitsrisiken zu bewerten.

4. Bei der Bewertung des Cybersicherheitsrisikos muss jede Einrichtung mit erheblichen oder kritischen Auswirkungen

   a. Cybersicherheitsrisiken unter Berücksichtigung folgender Aspekte ermitteln:

      i. aller Vermögenswerte, die unionsweite Prozesse mit erheblichen oder kritischen Auswirkungen unterstützen, wobei die möglichen Auswirkungen auf grenzüberschreitende Stromflüsse für den Fall einer Kompromittierung des Vermögenswerts zu bewerten sind;
      ii. möglicher Cyberbedrohungen unter Berücksichtigung der Cyberbedrohungen, die im jüngsten umfassenden Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23 ermittelt wurden, sowie Bedrohungen der Lieferkette;
      iii. Schwachstellen, einschließlich Schwachstellen in Altsystemen;
      iv. möglicher Szenarien von Cyberangriffen, einschließlich Cyberangriffen, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören;
      v. einschlägiger Risikobeurteilungen und -bewertungen auf Unionsebene, einschließlich koordinierter Risikobewertungen kritischer Lieferketten gemäß Artikel 22 der Richtlinie (EU) 2022/2555 [60], und
      vi. bestehender umgesetzter Kontrollen;

   b. die Wahrscheinlichkeit und Folgen der unter Buchstabe a genannten Cybersicherheitsrisiken analysieren und das Ausmaß des Cybersicherheitsrisikos anhand der Risiko-Auswirkungs-Matrix bestimmen, die in den von den ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO gemäß Artikel 19 Absatz 2 entwickelten Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf Ebene der Mitgliedstaaten genutzt wird, um Cybersicherheitsrisiken zu bewerten;

   c. Vermögenswerte nach den möglichen Folgen einer Beeinträchtigung der Cybersicherheit klassifizieren und Perimeter mit erheblichen oder kritischen Auswirkungen wie folgt ermitteln:

      i. Durchführung einer Folgenabschätzung für Geschäftsprozesse anhand des ECII für alle Prozesse, die Gegenstand der Bewertung des Cybersicherheitsrisikos sind;
      ii. Einstufung eines Prozesses als Prozess mit erheblichen oder kritischen Auswirkungen, wenn sein ECII über dem Schwellenwert für erhebliche bzw. kritische Auswirkungen liegt;
      iii. Bestimmung aller Vermögenswerte mit erheblichen oder kritischen Auswirkungen als die Vermögenswerte, die für Prozesse mit erheblichen bzw. kritischen Auswirkungen erforderlich sind;
      iv. Bestimmung der Perimeter mit erheblichen oder kritischen Auswirkungen als Perimeter, die alle Vermögenswerte mit erheblichen bzw. kritischen Auswirkungen umfassen, damit der Zugang zu diesen Perimetern kontrolliert werden kann;

[60] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_22

d. Cybersicherheitsrisiken durch Priorisierung anhand von Risikobewertungs- und Risikoakzeptanzkriterien gemäß Absatz 3 Buchstabe b beurteilen.

5. Bei der Behandlung des Cybersicherheitsrisikos erstellt jede Einrichtung mit erheblichen oder kritischen Auswirkungen einen Risikominderungsplan auf Ebene der Einrichtung, wobei sie geeignete Optionen für die Behandlung des Risikos wählt, um die Risiken zu bewältigen und das Restrisiko zu bestimmen.
6. Bei der Akzeptanz von Cybersicherheitsrisiken entscheidet jede Einrichtung mit erheblichen oder kritischen Auswirkungen auf der Grundlage der in Absatz 3 Buchstabe b festgelegten Risikoakzeptanzkriterien, ob sie das Restrisiko akzeptiert.
7. Jede Einrichtung mit erheblichen oder kritischen Auswirkungen erfasst die in Absatz 1 genannten Vermögenswerte in einem Vermögensinventar. Dieses Vermögensinventar ist nicht Teil des Berichts über die Risikobewertung.
8. Die zuständige Behörde kann die im Vermögensinventar enthaltenen Vermögenswerte während der Inspektionen einsehen.

Artikel 26(1)

Jede von den zuständigen Behörden gemäß Artikel 24 Absatz 1 ermittelte Einrichtung mit erheblichen oder kritischen Auswirkungen führt das Cybersicherheitsrisikomanagement für alle ihre Vermögenswerte in ihren Perimetern mit erheblichen oder kritischen Auswirkungen durch. Jede Einrichtung mit erheblichen oder kritischen Auswirkungen führt alle drei Jahre ein Risikomanagement durch, das die in Absatz 2 genannten Phasen umfasst.

Artikel 26(2)

Jede Einrichtung mit erheblichen oder kritischen Auswirkungen stützt ihr Cybersicherheitsrisikomanagement auf einen Ansatz, der auf den Schutz ihrer Netz- und Informationssysteme abzielt und folgende Phasen umfasst:

a. Bestimmung des Kontexts;
b. Bewertung des Cybersicherheitsrisikos auf der Ebene der Einrichtung;
c. Behandlung von Cybersicherheitsrisiken;
d. Akzeptanz von Cybersicherheitsrisiken.

Artikel 26(3)

Bei der Bestimmung des Kontexts trifft jede Einrichtung mit erheblichen oder kritischen Auswirkungen folgende Maßnahmen:

a. Festlegung des Umfangs der Bewertung des Cybersicherheitsrisikos, einschließlich der von ENTSO-E und der EU-VNBO ermittelten Prozesse mit erheblichen oder kritischen Auswirkungen sowie anderer Prozesse, die Ziel von Cyberangriffen mit erheblichen oder kritischen Auswirkungen auf grenzüberschreitende Stromflüsse sein können, und

b. Festlegung der Kriterien für die Risikobewertung und die Risikoakzeptanz im Einklang mit der Risiko-AuswirkungsMatrix, die Einrichtungen und die zuständigen Behörden nach den von ENTSO-E und der EU-VNBO gemäß Artikel 19 Absatz 2 entwickelten Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf Ebene der Mitgliedstaaten nutzen müssen, um Cybersicherheitsrisiken zu bewerten.

Artikel 26(4)

Bei der Bewertung des Cybersicherheitsrisikos muss jede Einrichtung mit erheblichen oder kritischen Auswirkungen

a. Cybersicherheitsrisiken unter Berücksichtigung folgender Aspekte ermitteln:

   i. aller Vermögenswerte, die unionsweite Prozesse mit erheblichen oder kritischen Auswirkungen unterstützen, wobei die möglichen Auswirkungen auf grenzüberschreitende Stromflüsse für den Fall einer Kompromittierung des Vermögenswerts zu bewerten sind;

   ii. möglicher Cyberbedrohungen unter Berücksichtigung der Cyberbedrohungen, die im jüngsten umfassenden Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23 ermittelt wurden, sowie Bedrohungen der Lieferkette;

   iii. Schwachstellen, einschließlich Schwachstellen in Altsystemen;

   iv. möglicher Szenarien von Cyberangriffen, einschließlich Cyberangriffen, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören;

   v. einschlägiger Risikobeurteilungen und -bewertungen auf Unionsebene, einschließlich koordinierter Risikobewertungen kritischer Lieferketten gemäß Artikel 22 der Richtlinie (EU) 2022/2555 [61], und

   vi. bestehender umgesetzter Kontrollen;

b. die Wahrscheinlichkeit und Folgen der unter Buchstabe a genannten Cybersicherheitsrisiken analysieren und das Ausmaß des Cybersicherheitsrisikos anhand der Risiko-Auswirkungs-Matrix bestimmen, die in den von den ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO gemäß Artikel 19 Absatz 2 entwickelten Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf Ebene der Mitgliedstaaten genutzt wird, um Cybersicherheitsrisiken zu bewerten;

c. Vermögenswerte nach den möglichen Folgen einer Beeinträchtigung der Cybersicherheit klassifizieren und Perimeter mit erheblichen oder kritischen Auswirkungen wie folgt ermitteln:

[61] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_22

i. Durchführung einer Folgenabschätzung für Geschäftsprozesse anhand des ECII für alle Prozesse, die Gegenstand der Bewertung des Cybersicherheitsrisikos sind;
ii. Einstufung eines Prozesses als Prozess mit erheblichen oder kritischen Auswirkungen, wenn sein ECII über dem Schwellenwert für erhebliche bzw. kritische Auswirkungen liegt;
iii. Bestimmung aller Vermögenswerte mit erheblichen oder kritischen Auswirkungen als die Vermögenswerte, die für Prozesse mit erheblichen bzw. kritischen Auswirkungen erforderlich sind;
iv. Bestimmung der Perimeter mit erheblichen oder kritischen Auswirkungen als Perimeter, die alle Vermögenswerte mit erheblichen bzw. kritischen Auswirkungen umfassen, damit der Zugang zu diesen Perimetern kontrolliert werden kann;

d. Cybersicherheitsrisiken durch Priorisierung anhand von Risikobewertungs- und Risikoakzeptanzkriterien gemäß Absatz 3 Buchstabe b beurteilen.

Artikel 26(5)

Bei der Behandlung des Cybersicherheitsrisikos erstellt jede Einrichtung mit erheblichen oder kritischen Auswirkungen einen Risikominderungsplan auf Ebene der Einrichtung, wobei sie geeignete Optionen für die Behandlung des Risikos wählt, um die Risiken zu bewältigen und das Restrisiko zu bestimmen.

Artikel 26(6)

Bei der Akzeptanz von Cybersicherheitsrisiken entscheidet jede Einrichtung mit erheblichen oder kritischen Auswirkungen auf der Grundlage der in Absatz 3 Buchstabe b festgelegten Risikoakzeptanzkriterien, ob sie das Restrisiko akzeptiert.

Artikel 26(7)

Jede Einrichtung mit erheblichen oder kritischen Auswirkungen erfasst die in Absatz 1 genannten Vermögenswerte in einem Vermögensinventar. Dieses Vermögensinventar ist nicht Teil des Berichts über die Risikobewertung.

Artikel 26(8)

Die zuständige Behörde kann die im Vermögensinventar enthaltenen Vermögenswerte während der Inspektionen einsehen.

Artikel 27

Innerhalb von 12 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre legt jede Einrichtung

mit erheblichen oder kritischen Auswirkungen der zuständigen Behörde einen Bericht vor, der folgende Informationen enthält:

1. eine Liste der für den Risikominderungsplan auf Ebene der Einrichtung gemäß Artikel 26 Absatz 5 ausgewählten Kontrollen mit dem aktuellen Stand der Umsetzung jeder Kontrolle;
2. für jeden unionsweiten Prozess mit erheblichen oder kritischen Auswirkungen eine Schätzung des Risikos einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten. Die Schätzung dieses Risikos ist im Einklang mit der Risiko-Auswirkungs-Matrix gemäß Artikel 19 Absatz 2 zu bestimmen;
3. für ihre Prozesse mit kritischen Auswirkungen eine Liste der Anbieter kritischer IKT-Dienste.

Artikel 27(1)

Innerhalb von 12 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre legt jede Einrichtung mit erheblichen oder kritischen Auswirkungen der zuständigen Behörde einen Bericht vor, der folgende Informationen enthält:

1. eine Liste der für den Risikominderungsplan auf Ebene der Einrichtung gemäß Artikel 26 Absatz 5 ausgewählten Kontrollen mit dem aktuellen Stand der Umsetzung jeder Kontrolle;
2. für jeden unionsweiten Prozess mit erheblichen oder kritischen Auswirkungen eine Schätzung des Risikos einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten. Die Schätzung dieses Risikos ist im Einklang mit der Risiko-Auswirkungs-Matrix gemäß Artikel 19 Absatz 2 zu bestimmen;
3. für ihre Prozesse mit kritischen Auswirkungen eine Liste der Anbieter kritischer IKT-Dienste.

Artikel 28

1. Der gemeinsame Rahmen für die Cybersicherheit im Elektrizitätssektor umfasst die folgenden Kontrollen und Systeme für das Cybersicherheitsmanagement:
   a. die gemäß Artikel 29 entwickelten Mindest-Cybersicherheitskontrollen;
   b. die gemäß Artikel 29 entwickelten erweiterten Cybersicherheitskontrollen;
   c. die gemäß Artikel 34 entwickelte Vergleichsmatrix, in der die Kontrollen gemäß den Buchstaben a und b anhand ausgewählter europäischer und internationaler Normen und nationaler Rechts- oder Verwaltungsrahmen verglichen werden;
   d. das gemäß Artikel 32 eingerichtete Cybersicherheitsmanagementsystem.
2. Alle Einrichtungen mit erheblichen Auswirkungen wenden die Mindest-Cybersicherheitskontrollen gemäß Absatz 1 Buchstabe a innerhalb ihres Perimeters mit erheblichen Auswirkungen an.

3. Alle Einrichtungen mit kritischen Auswirkungen wenden die erweiterten Cybersicherheitskontrollen gemäß Absatz 1 Buchstabe b innerhalb ihres Perimeters mit kritischen Auswirkungen an.
4. Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 wird der in Absatz 1 genannte gemeinsame Rahmen für die Cybersicherheit im Elektrizitätssektor durch die gemäß Artikel 33 entwickelten Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen in der Lieferkette ergänzt.

Artikel 28(1)

Der gemeinsame Rahmen für die Cybersicherheit im Elektrizitätssektor umfasst die folgenden Kontrollen und Systeme für das Cybersicherheitsmanagement:

a. die gemäß Artikel 29 entwickelten Mindest-Cybersicherheitskontrollen;
b. die gemäß Artikel 29 entwickelten erweiterten Cybersicherheitskontrollen;
c. die gemäß Artikel 34 entwickelte Vergleichsmatrix, in der die Kontrollen gemäß den Buchstaben a und b anhand ausgewählter europäischer und internationaler Normen und nationaler Rechts- oder Verwaltungsrahmen verglichen werden;
d. das gemäß Artikel 32 eingerichtete Cybersicherheitsmanagementsystem.

Artikel 28(2)

Alle Einrichtungen mit erheblichen Auswirkungen wenden die Mindest-Cybersicherheitskontrollen gemäß Absatz 1 Buchstabe a innerhalb ihres Perimeters mit erheblichen Auswirkungen an.

Artikel 28(3)

Alle Einrichtungen mit kritischen Auswirkungen wenden die erweiterten Cybersicherheitskontrollen gemäß Absatz 1 Buchstabe b innerhalb ihres Perimeters mit kritischen Auswirkungen an.

Artikel 28(4)

Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 wird der in Absatz 1 genannte gemeinsame Rahmen für die Cybersicherheit im Elektrizitätssektor durch die gemäß Artikel 33 entwickelten Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen in der Lieferkette ergänzt.

Artikel 29

1. Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO einen Vorschlag für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen.

2. Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO der zuständigen Behörde eine Änderung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

3. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen müssen überprüft werden können; dazu werden sie entweder im Einklang mit dem Verfahren gemäß Artikel 31 in ein nationales Überprüfungssystem einbezogen oder Sicherheitsaudits durch unabhängige Dritte gemäß den in Artikel 25 Absatz 2 aufgeführten Anforderungen unterzogen.

4. Die gemäß Absatz 1 entwickelten anfänglichen Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen müssen auf den Risiken beruhen, die in dem Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 5 ermittelt wurden. Die gemäß Absatz 2 entwickelten geänderten MindestCybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen müssen auf dem in Artikel 21 Absatz 2 genannten Bericht über die regionale Bewertung des Cybersicherheitsrisikos beruhen.

5. Die Mindest-Cybersicherheitskontrollen müssen im Einklang mit Artikel 46 Kontrollen zum Schutz der ausgetauschten Informationen umfassen.

6. Innerhalb von 12 Monaten nach der Genehmigung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 8 Absatz 5 und nach jeder Aktualisierung gemäß Artikel 8 Absatz 10 wenden die in Artikel 2 Absatz 1 genannten Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden, bei der Festlegung des Risikominderungsplans auf Ebene der Einrichtung gemäß Artikel 26 Absatz 5 innerhalb der Perimeter mit erheblichen Auswirkungen die Mindest-Cybersicherheitskontrollen und innerhalb der Perimeter mit kritischen Auswirkungen die erweiterten Cybersicherheitskontrollen an.

Artikel 29(1)

Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO einen Vorschlag für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen.

Artikel 29(2)

Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO der zuständigen Behörde eine Änderung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

Artikel 29(3)

Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen müssen überprüft werden können; dazu werden sie entweder im Einklang mit dem Verfahren gemäß Artikel 31 in ein nationales Überprüfungssystem einbezogen oder Sicherheitsaudits durch unabhängige Dritte gemäß den in Artikel 25 Absatz 2 aufgeführten Anforderungen unterzogen.

Artikel 29(4)

Die gemäß Absatz 1 entwickelten anfänglichen Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen müssen auf den Risiken beruhen, die in dem Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 5 ermittelt wurden. Die gemäß Absatz 2 entwickelten geänderten MindestCybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen müssen auf dem in Artikel 21 Absatz 2 genannten Bericht über die regionale Bewertung des Cybersicherheitsrisikos beruhen.

Artikel 29(5)

Die Mindest-Cybersicherheitskontrollen müssen im Einklang mit Artikel 46 Kontrollen zum Schutz der ausgetauschten Informationen umfassen.

Artikel 29(6)

Innerhalb von 12 Monaten nach der Genehmigung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 8 Absatz 5 und nach jeder Aktualisierung gemäß Artikel 8 Absatz 10 wenden die in Artikel 2 Absatz 1 genannten Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden, bei der Festlegung des Risikominderungsplans auf Ebene der Einrichtung gemäß Artikel 26 Absatz 5 innerhalb der Perimeter mit erheblichen Auswirkungen die Mindest-Cybersicherheitskontrollen und innerhalb der Perimeter mit kritischen Auswirkungen die erweiterten Cybersicherheitskontrollen an.

Innerhalb von 12 Monaten nach der Genehmigung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 8 Absatz 5 und nach jeder Aktualisierung gemäß Artikel 8 Absatz 10 wenden die in Artikel 2 Absatz 1 genannten Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden, bei der Festlegung des Risikominderungsplans auf Ebene der Einrichtung gemäß Artikel

26 Absatz 5 innerhalb der Perimeter mit erheblichen Auswirkungen die Mindest-Cybersicherheitskontrollen und innerhalb der Perimeter mit kritischen Auswirkungen die erweiterten Cybersicherheitskontrollen an.

Artikel 30

1. Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen können bei der jeweils zuständigen Behörde eine Ausnahme von ihrer Verpflichtung zur Anwendung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 29 Absatz 6 beantragen. Die zuständige Behörde kann eine solche Ausnahme aus folgenden Gründen gewähren:

    a. unter außergewöhnlichen Umständen, wenn die Einrichtung nachweisen kann, dass die Kosten für die Durchführung geeigneter Cybersicherheitskontrollen den Nutzen erheblich übersteigen. Die ACER und ENTSO-E können in Zusammenarbeit mit der EU-VNBO zur Unterstützung der Einrichtungen gemeinsam Leitlinien für die Schätzung der Kosten von Cybersicherheitskontrollen ausarbeiten;
    b. bei Vorlage eines Risikobehandlungsplans auf Ebene der Einrichtung, mit dem die Cybersicherheitsrisiken durch alternative Kontrollen auf ein Niveau verringert werden, das nach den in Artikel 26 Absatz 3 Buchstabe b genannten Risikoakzeptanzkriterien akzeptiert werden kann.

2. Innerhalb von drei Monaten nach Eingang des in Absatz 1 genannten Antrags entscheidet jede zuständige Behörde, ob eine Ausnahme von den Mindest-Cybersicherheitskontrollen und den erweiterten Cybersicherheitskontrollen gewährt wird. Ausnahmen von den Mindest-Cybersicherheitskontrollen oder den erweiterten Cybersicherheitskontrollen werden für höchstens drei Jahre gewährt und können verlängert werden.

3. Aggregierte und anonymisierte Informationen zu den gewährten Ausnahmen werden dem umfassenden Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23 als Anhang beigefügt. ENTSO-E und die EU-VNBO aktualisieren die Liste bei Bedarf gemeinsam.

Artikel 30(1)

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen können bei der jeweils zuständigen Behörde eine Ausnahme von ihrer Verpflichtung zur Anwendung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 29 Absatz 6 beantragen.

Die zuständige Behörde kann eine solche Ausnahme aus folgenden Gründen gewähren:

a. unter außergewöhnlichen Umständen, wenn die Einrichtung nachweisen kann, dass die Kosten für die Durchführung geeigneter Cybersicherheitskontrollen den Nutzen erheblich übersteigen. Die ACER und ENTSO-E können in Zusammenarbeit mit der EU-VNBO zur Unterstützung der Einrichtungen gemeinsam Leitlinien für die Schätzung der Kosten von Cybersicherheitskontrollen ausarbeiten;

b. bei Vorlage eines Risikobehandlungsplans auf Ebene der Einrichtung, mit dem die Cybersicherheitsrisiken durch alternative Kontrollen auf ein Niveau verringert werden, das nach den in Artikel 26 Absatz 3 Buchstabe b genannten Risikoakzeptanzkriterien akzeptiert werden kann.

Artikel 30(2)

Innerhalb von drei Monaten nach Eingang des in Absatz 1 genannten Antrags entscheidet jede zuständige Behörde, ob eine Ausnahme von den Mindest-Cybersicherheitskontrollen und den erweiterten Cybersicherheitskontrollen gewährt wird. Ausnahmen von den Mindest-Cybersicherheitskontrollen oder den erweiterten Cybersicherheitskontrollen werden für höchstens drei Jahre gewährt und können verlängert werden.

Artikel 30(3)

Aggregierte und anonymisierte Informationen zu den gewährten Ausnahmen werden dem umfassenden Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23 als Anhang beigefügt. ENTSO-E und die EU-VNBO aktualisieren die Liste bei Bedarf gemeinsam.

Artikel 31

1. Spätestens 24 Monate nach der Annahme der in Artikel 28 Absatz 1 Buchstaben a, b und c genannten Kontrollen und der Einrichtung des in Buchstabe d jenes Artikels genannten Cybersicherheitsmanagementsystems muss jede gemäß Artikel 24 Absatz 1 ermittelte Einrichtung mit kritischen Auswirkungen in der Lage sein, auf Verlangen der zuständigen Behörde nachzuweisen, dass sie das Cybersicherheitsmanagementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet.
2. Jede Einrichtung mit kritischen Auswirkungen muss die in Absatz 1 genannte Verpflichtung erfüllen, indem sie sich einem von unabhängigen Dritten durchgeführten Sicherheitsaudit gemäß den Anforderungen aus Artikel 25 Absatz 2 unterzieht oder sich an einem nationalen Überprüfungssystem gemäß Artikel 25 Absatz 1 beteiligt.
3. Die Überprüfung, ob eine Einrichtung mit kritischen Auswirkungen das Cybersicherheitsmanagementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet, erstreckt sich auf alle Vermögenswerte der Einrichtung mit kritischen Auswirkungen innerhalb ihres Perimeters mit kritischen Auswirkungen.
4. Die Überprüfung, ob eine Einrichtung mit kritischen Auswirkungen das Cybersicherheitsmanagementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet, erstreckt sich auf alle Vermögenswerte der Einrichtung mit kritischen Auswirkungen innerhalb ihres Perimeters mit kritischen Auswirkungen.
5. Jede gemäß Artikel 24 ermittelte Einrichtung mit kritischen Auswirkungen muss die Einhaltung der in Artikel 28 Absatz 1 Buchstaben a, b und c genannten Kontrollen und die Einrich-

tung des unter Buchstabe d jenes Artikels genannten Cybersicherheitsmanagementsystems nachweisen, indem sie der zuständigen Behörde über das Ergebnis der Überprüfung der Einhaltung Bericht erstattet.

Artikel 31(1)

Spätestens 24 Monate nach der Annahme der in Artikel 28 Absatz 1 Buchstaben a, b und c genannten Kontrollen und der Einrichtung des in Buchstabe d jenes Artikels genannten Cybersicherheitsmanagementsystems muss jede gemäß Artikel 24 Absatz 1 ermittelte Einrichtung mit kritischen Auswirkungen in der Lage sein, auf Verlangen der zuständigen Behörde nachzuweisen, dass sie das Cybersicherheitsmanagementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet.

Artikel 31(2)

Jede Einrichtung mit kritischen Auswirkungen muss die in Absatz 1 genannte Verpflichtung erfüllen, indem sie sich einem von unabhängigen Dritten durchgeführten Sicherheitsaudit gemäß den Anforderungen aus Artikel 25 Absatz 2 unterzieht oder sich an einem nationalen Überprüfungssystem gemäß Artikel 25 Absatz 1 beteiligt.

Artikel 31(3)

Die Überprüfung, ob eine Einrichtung mit kritischen Auswirkungen das Cybersicherheitsmanagementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet, erstreckt sich auf alle Vermögenswerte der Einrichtung mit kritischen Auswirkungen innerhalb ihres Perimeters mit kritischen Auswirkungen.

Artikel 31(4)

Die Überprüfung, ob eine Einrichtung mit kritischen Auswirkungen das Cybersicherheitsmanagementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet, erstreckt sich auf alle Vermögenswerte der Einrichtung mit kritischen Auswirkungen innerhalb ihres Perimeters mit kritischen Auswirkungen.

Artikel 31(5)

Jede gemäß Artikel 24 ermittelte Einrichtung mit kritischen Auswirkungen muss die Einhaltung der in Artikel 28 Absatz 1 Buchstaben a, b und c genannten Kontrollen und die Einrichtung des unter Buchstabe d jenes Artikels genannten Cybersicherheitsmanagementsystems nachweisen, indem sie der zuständigen Behörde über das Ergebnis der Überprüfung der Einhaltung Bericht erstattet.

Artikel 32

1. Innerhalb von 24 Monaten, nachdem sie von der zuständigen Behörde darüber unterrichtet wurde, dass sie gemäß Artikel 24 Absatz 6 als Einrichtung mit erheblichen oder kritischen Auswirkungen eingestuft wurde, richtet jede Einrichtung mit erheblichen oder kritischen Auswirkungen ein Cybersicherheitsmanagementsystem ein, das sie danach alle drei Jahre überprüft, um

   a. den Umfang des Cybersicherheitsmanagementsystems unter Berücksichtigung von Schnittstellen und Abhängigkeiten mit anderen Einrichtungen festzulegen;
   b. sicherzustellen, dass die gesamte obere Führungsebene über einschlägige rechtliche Verpflichtungen informiert ist und durch rechtzeitige Entscheidungen und rasche Reaktionen aktiv zur Umsetzung des Cybersicherheitsmanagementsystems beiträgt;
   c. sicherzustellen, dass die für das Cybersicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen;
   d. ein Cybersicherheitskonzept festzulegen, das dokumentiert und innerhalb der Einrichtung sowie den von den Sicherheitsrisiken betroffenen Parteien bekannt gegeben wird;
   e. Zuständigkeiten für Aufgaben, die für die Cybersicherheit relevant sind, zuzuweisen und bekannt zu geben;
   f. das Cybersicherheitsrisikomanagement auf der Ebene der Einrichtungen gemäß Artikel 26 durchzuführen;
   g. die für die Umsetzung, Pflege und kontinuierliche Verbesserung des Cybersicherheitsmanagementsystems erforderlichen Ressourcen festzulegen und bereitzustellen, wobei die erforderlichen Kompetenzen und die Sensibilisierung für Cybersicherheitsressourcen zu berücksichtigen sind;
   h. die für die Cybersicherheit relevante interne und externe Kommunikation festzulegen;
   i. dokumentierte Informationen im Zusammenhang mit dem Cybersicherheitsmanagementsystem zu erstellen, zu aktualisieren und zu kontrollieren;
   j. die Ergebnisse und Wirksamkeit des Cybersicherheitsmanagementsystems zu beurteilen;
   k. in geplanten Zeitabständen interne Audits durchzuführen, um sicherzustellen, dass das Cybersicherheitsmanagementsystem wirksam umgesetzt und gepflegt wird;
   l. die Umsetzung des Cybersicherheitsmanagementsystems in geplanten Zeitabständen zu überprüfen und Abweichungen der Ressourcen und Tätigkeiten von den Konzepten, Verfahren und Leitlinien des Cybersicherheitsmanagementsystems zu kontrollieren und zu beheben.

2. Der Anwendungsbereich des Cybersicherheitsmanagementsystems der Einrichtung mit erheblichen Auswirkungen umfasst alle Vermögenswerte innerhalb ihres Perimeters mit erheblichen Auswirkungen.

3. Die zuständigen Behörden regen an, für die Sicherheit von Netz- und Informationssystemen relevante europäische oder internationaler Normen und Spezifikationen anzuwenden, ohne dabei die Nutzung einer bestimmten Technologie vorzuschreiben oder zu begünstigen.

Artikel 32(1)

Innerhalb von 24 Monaten, nachdem sie von der zuständigen Behörde darüber unterrichtet wurde, dass sie gemäß Artikel 24 Absatz 6 als Einrichtung mit erheblichen oder kritischen Auswirkungen eingestuft wurde, richtet jede Einrichtung mit erheblichen oder kritischen Auswirkungen ein Cybersicherheitsmanagementsystem ein, das sie danach alle drei Jahre überprüft, um

a. den Umfang des Cybersicherheitsmanagementsystems unter Berücksichtigung von Schnittstellen und Abhängigkeiten mit anderen Einrichtungen festzulegen;

b. sicherzustellen, dass die gesamte obere Führungsebene über einschlägige rechtliche Verpflichtungen informiert ist und durch rechtzeitige Entscheidungen und rasche Reaktionen aktiv zur Umsetzung des Cybersicherheitsmanagementsystems beiträgt;

c. sicherzustellen, dass die für das Cybersicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen;

d. ein Cybersicherheitskonzept festzulegen, das dokumentiert und innerhalb der Einrichtung sowie den von den Sicherheitsrisiken betroffenen Parteien bekannt gegeben wird;

e. Zuständigkeiten für Aufgaben, die für die Cybersicherheit relevant sind, zuzuweisen und bekannt zu geben;

f. das Cybersicherheitsrisikomanagement auf der Ebene der Einrichtungen gemäß Artikel 26 durchzuführen;

g. die für die Umsetzung, Pflege und kontinuierliche Verbesserung des Cybersicherheitsmanagementsystems erforderlichen Ressourcen festzulegen und bereitzustellen, wobei die erforderlichen Kompetenzen und die Sensibilisierung für Cybersicherheitsressourcen zu berücksichtigen sind;

h. die für die Cybersicherheit relevante interne und externe Kommunikation festzulegen;

i. dokumentierte Informationen im Zusammenhang mit dem Cybersicherheitsmanagementsystem zu erstellen, zu aktualisieren und zu kontrollieren;

j. die Ergebnisse und Wirksamkeit des Cybersicherheitsmanagementsystems zu beurteilen;

k. in geplanten Zeitabständen interne Audits durchzuführen, um sicherzustellen, dass das Cybersicherheitsmanagementsystem wirksam umgesetzt und gepflegt wird;

l. die Umsetzung des Cybersicherheitsmanagementsystems in geplanten Zeitabständen zu überprüfen und Abweichungen der Ressourcen und Tätigkeiten von den Konzepten, Verfahren und Leitlinien des Cybersicherheitsmanagementsystems zu kontrollieren und zu beheben.

Artikel 32(2)

Der Anwendungsbereich des Cybersicherheitsmanagementsystems der Einrichtung mit erheblichen Auswirkungen umfasst alle Vermögenswerte innerhalb ihres Perimeters mit erheblichen Auswirkungen.

Artikel 32(3)

Die zuständigen Behörden regen an, für die Sicherheit von Netz- und Informationssystemen relevante europäische oder internationaler Normen und Spezifikationen anzuwenden, ohne dabei die Nutzung einer bestimmten Technologie vorzuschreiben oder zu begünstigen.

Artikel 33

1. Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO einen Vorschlag für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen in der Lieferkette, mit denen die in den unionsweiten Bewertungen des Cybersicherheitsrisikos ermittelten Risiken für die Lieferketten gemindert werden, um die gemäß Artikel 29 entwickelten Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen zu ergänzen. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette werden zusammen mit den Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen gemäß Artikel 29 entwickelt. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette erstrecken sich auf den gesamten Lebenszyklus aller IKT-Produkte, -Dienste und -Prozesse einer Einrichtung mit erheblichen oder kritischen Auswirkungen innerhalb ihrer Perimeter mit erheblichen oder kritischen Auswirkungen. Bei der Entwicklung des Vorschlags für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen in der Lieferkette wird die NIS-Kooperationsgruppe konsultiert.
2. Die Mindest-Cybersicherheitskontrollen in der Lieferkette bestehen aus Kontrollen für Einrichtungen mit erheblichen oder kritischen Auswirkungen, die
    a. auf Cybersicherheitsspezifikationen bezogene Empfehlungen für die Beschaffung von IKT-Produkten, -Diensten und -Prozessen enthalten und mindestens Folgendes abdecken:
        i. Zuverlässigkeitsüberprüfungen der Mitarbeiter des Anbieters, die an der Lieferkette beteiligt sind und sich mit sensiblen Informationen befassen oder Zugang zu Vermögenswerten mit erheblichen oder kritischen Auswirkungen der Einrichtung haben. Die Zuverlässigkeitsüberprüfung kann eine Überprüfung der Identität und des Hintergrunds von Mitarbeitern oder Auftragnehmern einer Einrichtung im Einklang mit den nationalen Rechtsvorschriften und Verfahren sowie dem einschlägigen und geltenden Unionsrecht umfassen, einschließlich der Verordnung (EU) 2016/679 [62] und der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates [63] Zuverlässigkeitsüberprüfungen müssen verhältnismäßig und strikt auf das Notwendige beschränkt sein. Sie werden ausschließlich zum Zweck der Bewertung eines potenziellen Sicherheitsrisikos für die betreffende Einrichtung durchgeführt. Sie müssen in einem angemessenen Verhältnis zu den Geschäftserfordernissen, der Klassifizierung der einzusehenden Informationen und den wahrgenommenen Risiken stehen und können von der Einrichtung selbst, einem externen Unternehmen, das ein Screening durchführt, oder durch staatliches Clearing vorgenommen werden;

[62] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679
[63] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016L0680

ii. die Prozesse für eine sichere und kontrollierte Gestaltung, Entwicklung und Herstellung von IKT-Produkten, -Diensten und -Prozessen, die Förderung der Gestaltung und Entwicklung von IKT-Produkten, -Diensten und -Prozessen, die geeignete technische Maßnahmen zur Gewährleistung der Cybersicherheit umfassen;
iii. die Gestaltung von Netz- und Informationssystemen, in denen Geräte selbst dann nicht als vertrauenswürdig gelten, wenn sie sich in einem sicheren Perimeter befinden, eine Überprüfung aller eingegangenen Anfragen erfordern und das Prinzip der minimalen Berechtigung angewandt wird;
iv. den Zugang des Anbieters zu den Vermögenswerten der Einrichtung;
v. die vertraglichen Verpflichtungen des Anbieters zum Schutz sensibler Informationen der Einrichtung und zur Beschränkung des Zugangs zu diesen Informationen;
vi. die zugrunde liegenden Spezifikationen für die Cybersicherheit bei der Auftragsvergabe an Unterauftragnehmer des Anbieters;
vii. die Rückverfolgbarkeit der Anwendung der Cybersicherheitsspezifikationen von der Entwicklung über die Produktion bis zur Bereitstellung von IKT-Produkten, -Diensten oder -Prozessen;
viii. die Unterstützung von Sicherheitsaktualisierungen während der gesamten Lebensdauer von IKT-Produkten, -Diensten oder -Prozessen;
ix. das Recht auf Prüfung der Cybersicherheit in den Konzeptions-, Entwicklungs- und Produktionsprozessen des Anbieters sowie
x. die Bewertung des Risikoprofils des Anbieters;

b. diese Einrichtungen dazu verpflichten, die unter Buchstabe a genannten Empfehlungen für die Auftragsvergabe zu berücksichtigen, wenn sie Verträge mit Anbietern, Kooperationspartnern und anderen Parteien in der Lieferkette schließen, sowohl in Bezug auf normale Lieferungen von IKT-Produkten, -Diensten und -Prozessen als auch in Bezug auf ungeplante Ereignisse und Umstände wie die Kündigung und den Übergang von Verträgen im Falle von Fahrlässigkeit des Vertragspartners;
c. diese Einrichtungen dazu verpflichten, die Ergebnisse einschlägiger koordinierter Sicherheitsrisikobewertungen kritischer Lieferketten gemäß Artikel 22 Absatz 1 der Richtlinie (EU) 2022/2555 zu berücksichtigen;
d. Kriterien für die Auswahl von Anbietern und die Auftragsvergabe an Anbieter enthalten, die die unter Buchstabe a genannten Cybersicherheitsspezifikationen erfüllen können und über ein Maß an Cybersicherheit verfügen, das den Cybersicherheitsrisiken des vom Anbieter bereitgestellten IKT-Produkts, -Dienstes oder -Prozesses angemessen ist;
e. Kriterien für die Diversifizierung der Bezugsquellen für IKT-Produkte, -Dienste und -Prozesse und zur Verringerung des Risikos eines Anbieter-Lock-ins enthalten;
f. Kriterien für die regelmäßige Überwachung, Überprüfung oder Prüfung der Cybersicherheitsspezifikationen für interne Betriebsprozesse des Anbieters während des gesamten Lebenszyklus jedes IKT-Produkts, -Dienstes und -Prozesses enthalten.

3. Für die Cybersicherheitsspezifikationen in der in Absatz 2 Buchstabe a genannten Empfehlung zur Cybersicherheit bei der Auftragsvergabe wenden Einrichtungen mit erheblichen oder kritischen Auswirkungen im Einklang mit Artikel 35 Absatz 4 die Grundsätze der Auftragsvergabe aus der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates [64] an oder legen ihre eigenen Spezifikationen auf der Grundlage der Ergebnisse der Bewertung des Cybersicherheitsrisikos auf der Ebene der Einrichtung fest.

[64] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014L0024#d1e3478-65-1

4. Die erweiterten Cybersicherheitskontrollen in der Lieferkette müssen Kontrollen für Einrichtungen mit kritischen Auswirkungen umfassen, um bei der Auftragsvergabe zu überprüfen, ob IKT-Produkte, -Dienste und -Prozesse, die als Vermögenswerte mit kritischen Auswirkungen verwendet werden sollen, den Cybersicherheitsspezifikationen entsprechen. Das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess wird entweder durch ein europäisches Schema für die Cybersicherheitszertifizierung gemäß Artikel 31 oder mit von der Einrichtung ausgewählten und organisierten Überprüfungsmaßnahmen überprüft. Die Überprüfungsmaßnahmen müssen ausreichend gründlich und umfassend sein, um zu gewährleisten, dass das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess genutzt werden kann, um die in der Risikobewertung auf Ebene der Einrichtung ermittelten Risiken zu mindern. Die Einrichtung mit kritischen Auswirkungen dokumentiert die Maßnahmen zur Verringerung der ermittelten Risiken.

5. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für die Beschaffung relevanter IKT-Produkte, -Dienste und -Prozesse. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit kritischen oder erheblichen Auswirkungen ermittelt wurden, bei der Auftragsvergabe ab sechs Monaten nach der Annahme oder Aktualisierung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 29.

6. Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO der zuständigen Behörde eine Änderung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen in der Lieferkette vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

Artikel 33(1)

Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO einen Vorschlag für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen in der Lieferkette, mit denen die in den unionsweiten Bewertungen des Cybersicherheitsrisikos ermittelten Risiken für die Lieferketten gemindert werden, um die gemäß Artikel 29 entwickelten Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen zu ergänzen. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette werden zusammen mit den Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen gemäß Artikel 29 entwickelt. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette erstrecken sich auf den gesamten Lebenszyklus aller IKT-Produkte, -Dienste und -Prozesse einer Einrichtung mit erheblichen oder kritischen Auswirkungen innerhalb ihrer Perimeter mit erheblichen oder kritischen Auswirkungen. Bei der Entwicklung des Vorschlags für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen in der Lieferkette wird die NIS-Kooperationsgruppe konsultiert.

Artikel 33(2)

Die Mindest-Cybersicherheitskontrollen in der Lieferkette bestehen aus Kontrollen für Einrichtungen mit erheblichen oder kritischen Auswirkungen, die

a. auf Cybersicherheitsspezifikationen bezogene Empfehlungen für die Beschaffung von IKT-Produkten, -Diensten und -Prozessen enthalten und mindestens Folgendes abdecken:

   i. Zuverlässigkeitsüberprüfungen der Mitarbeiter des Anbieters, die an der Lieferkette beteiligt sind und sich mit sensiblen Informationen befassen oder Zugang zu Vermögenswerten mit erheblichen oder kritischen Auswirkungen der Einrichtung haben. Die Zuverlässigkeitsüberprüfung kann eine Überprüfung der Identität und des Hintergrunds von Mitarbeitern oder Auftragnehmern einer Einrichtung im Einklang mit den nationalen Rechtsvorschriften und Verfahren sowie dem einschlägigen und geltenden Unionsrecht umfassen, einschließlich der Verordnung (EU) 2016/679 [65] und der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates [66]. Zuverlässigkeitsüberprüfungen müssen verhältnismäßig und strikt auf das Notwendige beschränkt sein. Sie werden ausschließlich zum Zweck der Bewertung eines potenziellen Sicherheitsrisikos für die betreffende Einrichtung durchgeführt. Sie müssen in einem angemessenen Verhältnis zu den Geschäftserfordernissen, der Klassifizierung der einzusehenden Informationen und den wahrgenommenen Risiken stehen und können von der Einrichtung selbst, einem externen Unternehmen, das ein Screening durchführt, oder durch staatliches Clearing vorgenommen werden;

   ii. die Prozesse für eine sichere und kontrollierte Gestaltung, Entwicklung und Herstellung von IKT-Produkten, -Diensten und -Prozessen, die Förderung der Gestaltung und Entwicklung von IKT-Produkten, -Diensten und -Prozessen, die geeignete technische Maßnahmen zur Gewährleistung der Cybersicherheit umfassen;

   iii. die Gestaltung von Netz- und Informationssystemen, in denen Geräte selbst dann nicht als vertrauenswürdig gelten, wenn sie sich in einem sicheren Perimeter befinden, eine Überprüfung aller eingegangenen Anfragen erfordern und das Prinzip der minimalen Berechtigung angewandt wird;

   iv. den Zugang des Anbieters zu den Vermögenswerten der Einrichtung;

   v. die vertraglichen Verpflichtungen des Anbieters zum Schutz sensibler Informationen der Einrichtung und zur Beschränkung des Zugangs zu diesen Informationen;

   vi. die zugrunde liegenden Spezifikationen für die Cybersicherheit bei der Auftragsvergabe an Unterauftragnehmer des Anbieters;

   vii. die Rückverfolgbarkeit der Anwendung der Cybersicherheitsspezifikationen von der Entwicklung über die Produktion bis zur Bereitstellung von IKT-Produkten, -Diensten oder -Prozessen;

   viii. die Unterstützung von Sicherheitsaktualisierungen während der gesamten Lebensdauer von IKT-Produkten, -Diensten oder -Prozessen;

   ix. das Recht auf Prüfung der Cybersicherheit in den Konzeptions-, Entwicklungs- und Produktionsprozessen des Anbieters sowie

   x. die Bewertung des Risikoprofils des Anbieters;

[65] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679
[66] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016L0680

b. diese Einrichtungen dazu verpflichten, die unter Buchstabe a genannten Empfehlungen für die Auftragsvergabe zu berücksichtigen, wenn sie Verträge mit Anbietern, Kooperationspartnern und anderen Parteien in der Lieferkette schließen, sowohl in Bezug auf normale Lieferungen von IKT-Produkten, -Diensten und -Prozessen als auch in Bezug auf ungeplante Ereignisse und Umstände wie die Kündigung und den Übergang von Verträgen im Falle von Fahrlässigkeit des Vertragspartners;

c. diese Einrichtungen dazu verpflichten, die Ergebnisse einschlägiger koordinierter Sicherheitsrisikobewertungen kritischer Lieferketten gemäß Artikel 22 Absatz 1 der Richtlinie (EU) 2022/2555 zu berücksichtigen;

d. Kriterien für die Auswahl von Anbietern und die Auftragsvergabe an Anbieter enthalten, die die unter Buchstabe a genannten Cybersicherheitsspezifikationen erfüllen können und über ein Maß an Cybersicherheit verfügen, das den Cybersicherheitsrisiken des vom Anbieter bereitgestellten IKT-Produkts, -Dienstes oder -Prozesses angemessen ist;

e. Kriterien für die Diversifizierung der Bezugsquellen für IKT-Produkte, -Dienste und -Prozesse und zur Verringerung des Risikos eines Anbieter-Lock-ins enthalten;

f. Kriterien für die regelmäßige Überwachung, Überprüfung oder Prüfung der Cybersicherheitsspezifikationen für interne Betriebsprozesse des Anbieters während des gesamten Lebenszyklus jedes IKT-Produkts, -Dienstes und -Prozesses enthalten.

Artikel 33(3)

Für die Cybersicherheitsspezifikationen in der in Absatz 2 Buchstabe a genannten Empfehlung zur Cybersicherheit bei der Auftragsvergabe wenden Einrichtungen mit erheblichen oder kritischen Auswirkungen im Einklang mit Artikel 35 Absatz 4 die Grundsätze der Auftragsvergabe aus der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates [67] an oder legen ihre eigenen Spezifikationen auf der Grundlage der Ergebnisse der Bewertung des Cybersicherheitsrisikos auf der Ebene der Einrichtung fest.

Artikel 33(4)

Die erweiterten Cybersicherheitskontrollen in der Lieferkette müssen Kontrollen für Einrichtungen mit kritischen Auswirkungen umfassen, um bei der Auftragsvergabe zu überprüfen, ob IKT-Produkte, -Dienste und -Prozesse, die als Vermögenswerte mit kritischen Auswirkungen verwendet werden sollen, den Cybersicherheitsspezifikationen entsprechen. Das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess wird entweder durch ein europäisches Schema für die Cybersicherheitszertifizierung gemäß Artikel 31 oder mit von der Einrichtung ausgewählten und organisierten Überprüfungsmaßnahmen überprüft. Die Überprüfungsmaßnahmen müssen ausreichend gründlich und umfassend sein, um zu gewährleisten, dass das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess genutzt werden kann, um die in der Risikobewertung auf Ebene der Einrichtung ermittelten Risiken zu mindern. Die Einrichtung mit kritischen Auswirkungen dokumentiert die Maßnahmen zur Verringerung der ermittelten Risiken.

[67] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014L0024#d1e3478-65-1

Artikel 33(5)

Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für die Beschaffung relevanter IKT-Produkte, -Dienste und -Prozesse. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit kritischen oder erheblichen Auswirkungen ermittelt wurden, bei der Auftragsvergabe ab sechs Monaten nach der Annahme oder Aktualisierung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 29.

Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für die Beschaffung relevanter IKT-Produkte, -Dienste und -Prozesse. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit kritischen oder erheblichen Auswirkungen ermittelt wurden, bei der Auftragsvergabe ab sechs Monaten nach der Annahme oder Aktualisierung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 29.

Artikel 33(6)

Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO der zuständigen Behörde eine Änderung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen in der Lieferkette vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

Artikel 34

1. Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der ENISA einen Vorschlag für eine Matrix, mit der die Kontrollen gemäß Artikel 28 Absatz 1 Buchstaben a und b anhand ausgewählter europäischer und internationaler Normen sowie einschlägiger technischer Spezifikationen verglichen werden (im Folgenden „Vergleichsmatrix“). ENTSO-E und die EU-VNBO dokumentieren die Gleichwertigkeit der verschiedenen Kontrollen mit den in Artikel 28 Absatz 1 Buchstaben a und b genannten Kontrollen.
2. Die zuständigen Behörden können ENTSO-E und der EU-VNBO einen Vergleich der in Artikel 28 Absatz 1 Buchstaben a und b genannten Kontrollen mit dem entsprechenden nationalen Rechts- und Verwaltungsrahmen, einschließlich der einschlägigen nationalen Normen der Mitgliedstaaten gemäß Artikel 25 der Richtlinie (EU) 2022/2555 [68], übermitteln. Stellt die zuständige Behörde eines Mitgliedstaats einen solchen Vergleich bereit, so integrieren ENTSO-E und die EU-VNBO diesen nationalen Vergleich in die Vergleichsmatrix.

[68] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid=1733994458451#art_25

3. Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sowie in Absprache mit der ENISA der zuständigen Behörde eine Änderung der Vergleichsmatrix vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

Artikel 34(1)

Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der ENISA einen Vorschlag für eine Matrix, mit der die Kontrollen gemäß Artikel 28 Absatz 1 Buchstaben a und b anhand ausgewählter europäischer und internationaler Normen sowie einschlägiger technischer Spezifikationen verglichen werden (im Folgenden „Vergleichsmatrix“).

ENTSO-E und die EU-VNBO dokumentieren die Gleichwertigkeit der verschiedenen Kontrollen mit den in Artikel 28 Absatz 1 Buchstaben a und b genannten Kontrollen.

Artikel 34(2)

Die zuständigen Behörden können ENTSO-E und der EU-VNBO einen Vergleich der in Artikel 28 Absatz 1 Buchstaben a und b genannten Kontrollen mit dem entsprechenden nationalen Rechts- und Verwaltungsrahmen, einschließlich der einschlägigen nationalen Normen der Mitgliedstaaten gemäß Artikel 25 der Richtlinie (EU) 2022/2555 [69], übermitteln.

Stellt die zuständige Behörde eines Mitgliedstaats einen solchen Vergleich bereit, so integrieren ENTSO-E und die EU-VNBO diesen nationalen Vergleich in die Vergleichsmatrix.

Artikel 34(3)

Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sowie in Absprache mit der ENISA der zuständigen Behörde eine Änderung der Vergleichsmatrix vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

Artikel 35

1. Die ÜNB entwickeln mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO in einem Arbeitsprogramm, das jedes Mal bei der Annahme eines Berichts über die

[69] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid=1733994458451#art_25

regionale Bewertung des Cybersicherheitsrisikos erstellt und aktualisiert wird, eine Reihe von unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe, die Einrichtungen mit erheblichen oder kritischen Auswirkungen als Grundlage für die Beschaffung von IKT-Produkten, -Diensten und -Prozessen in den Perimetern mit erheblichen oder kritischen Auswirkungen nutzen können. Dieses Arbeitsprogramm umfasst

   a. eine Beschreibung und Klassifizierung der Arten von IKT-Produkten, -Diensten und -Prozessen, die von Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Perimeter mit erheblichen oder kritischen Auswirkungen verwendet werden;
   b. eine Liste der Arten von IKT-Produkten, -Diensten und -Prozessen, für die eine Reihe unverbindlicher Cybersicherheitsempfehlungen auf der Grundlage der einschlägigen Berichte über die regionale Bewertung des Cybersicherheitsrisikos und der Prioritäten von Einrichtungen mit erheblichen oder kritischen Auswirkungen zu erstellen sind.

2. ENTSO-E übermittelt der ACER in Zusammenarbeit mit der EU-VNBO innerhalb von sechs Monaten nach Annahme oder Aktualisierung des Berichts über die regionale Bewertung des Cybersicherheitsrisikos eine Zusammenfassung dieses Arbeitsprogramms.

3. Die ÜNB bemühen sich mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sicherzustellen, dass die auf der Grundlage der einschlägigen regionalen Bewertung des Cybersicherheitsrisikos entwickelten unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe in allen Netzbetriebsregionen ähnlich oder vergleichbar sind. Die Empfehlungen für die Cybersicherheit bei der Auftragsvergabe müssen mindestens die in Artikel 33 Absatz 2 Buchstabe a genannten Spezifikationen umfassen. Soweit möglich, werden die Spezifikationen aus europäischen und internationalen Normen ausgewählt.

4. Die ÜNB stellen mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sicher, dass die Empfehlungen für die Cybersicherheit bei der Auftragsvergabe

   a. den Grundsätzen der Auftragsvergabe aus der Richtlinie 2014/24/EU entsprechen und
   b. mit den neuesten verfügbaren europäischen Schemata für die Cybersicherheitszertifizierung, die für das IKT-Produkt, den IKT-Dienst oder den IKT-Prozess relevant sind, vereinbar sind und diesen Rechnung tragen.

Artikel 35(1)

Die ÜNB entwickeln mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO in einem Arbeitsprogramm, das jedes Mal bei der Annahme eines Berichts über die regionale Bewertung des Cybersicherheitsrisikos erstellt und aktualisiert wird, eine Reihe von unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe, die Einrichtungen mit erheblichen oder kritischen Auswirkungen als Grundlage für die Beschaffung von IKT-Produkten, -Diensten und -Prozessen in den Perimetern mit erheblichen oder kritischen Auswirkungen nutzen können. Dieses Arbeitsprogramm umfasst

a. eine Beschreibung und Klassifizierung der Arten von IKT-Produkten, -Diensten und -Prozessen, die von Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Perimeter mit erheblichen oder kritischen Auswirkungen verwendet werden;

b. eine Liste der Arten von IKT-Produkten, -Diensten und -Prozessen, für die eine Reihe unverbindlicher Cybersicherheitsempfehlungen auf der Grundlage der einschlägigen Berichte über die regionale Bewertung des Cybersicherheitsrisikos und der Prioritäten von Einrichtungen mit erheblichen oder kritischen Auswirkungen zu erstellen sind.

Artikel 35(2)

ENTSO-E übermittelt der ACER in Zusammenarbeit mit der EU-VNBO innerhalb von sechs Monaten nach Annahme oder Aktualisierung des Berichts über die regionale Bewertung des Cybersicherheitsrisikos eine Zusammenfassung dieses Arbeitsprogramms.

Artikel 35(3)

Die ÜNB bemühen sich mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sicherzustellen, dass die auf der Grundlage der einschlägigen regionalen Bewertung des Cybersicherheitsrisikos entwickelten unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe in allen Netzbetriebsregionen ähnlich oder vergleichbar sind. Die Empfehlungen für die Cybersicherheit bei der Auftragsvergabe müssen mindestens die in Artikel 33 Absatz 2 Buchstabe a genannten Spezifikationen umfassen. Soweit möglich, werden die Spezifikationen aus europäischen und internationalen Normen ausgewählt.

Artikel 35(4)

Die ÜNB stellen mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sicher, dass die Empfehlungen für die Cybersicherheit bei der Auftragsvergabe

a. den Grundsätzen der Auftragsvergabe aus der Richtlinie 2014/24/EU entsprechen und
b. mit den neuesten verfügbaren europäischen Schemata für die Cybersicherheitszertifizierung, die für das IKT-Produkt, den IKT-Dienst oder den IKT-Prozess relevant sind, vereinbar sind und diesen Rechnung tragen.

Artikel 36

1. Unbeschadet des Rahmens für die Schaffung europäischer Schemata für die Cybersicherheitszertifizierung gemäß Artikel 46 der Verordnung (EU) 2019/881 [70] können die gemäß Artikel 35 entwickelten unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe sektorspezifische Leitlinien für die Verwendung europäischer Schemata für die Cybersicherheitszertifizierung umfassen, wenn für eine von Einrichtungen mit kritischen Auswirkungen verwendete Art von IKT-Produkten, -Diensten oder -Prozessen ein geeignetes Schema zur Verfügung steht.

[70] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e3205-15-1

2. Die ÜNB arbeiten mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO eng mit der ENISA zusammen, um die sektorspezifischen Leitlinien bereitzustellen, die in den unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe gemäß Absatz 1 enthalten sind.

Artikel 36(1)

Unbeschadet des Rahmens für die Schaffung europäischer Schemata für die Cybersicherheitszertifizierung gemäß Artikel 46 der Verordnung (EU) 2019/881 [71] können die gemäß Artikel 35 entwickelten unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe sektorspezifische Leitlinien für die Verwendung europäischer Schemata für die Cybersicherheitszertifizierung umfassen, wenn für eine von Einrichtungen mit kritischen Auswirkungen verwendete Art von IKT-Produkten, -Diensten oder -Prozessen ein geeignetes Schema zur Verfügung steht.

Artikel 36(2)

Die ÜNB arbeiten mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO eng mit der ENISA zusammen, um die sektorspezifischen Leitlinien bereitzustellen, die in den unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe gemäß Absatz 1 enthalten sind.

Artikel 37

1. Erhält eine zuständige Behörde Informationen über einen meldepflichtigen Cyberangriff,
    a. bewertet sie den Grad der Vertraulichkeit dieser Informationen und unterrichtet die Einrichtung unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Eingang der Informationen, über das Ergebnis ihrer Bewertung;
    b. versucht sie, andere ähnliche Cyberangriffe in der Union zu ermitteln, die anderen zuständigen Behörden gemeldet wurden, um die zu dem meldepflichtigen Cyberangriff eingegangenen Informationen mit Informationen zu vergleichen, die zu anderen Cyberangriffen bereitgestellt wurden, und um vorhandene Informationen zu ergänzen sowie die Reaktion im Bereich der Cybersicherheit zu stärken und zu koordinieren;
    c. ist sie für die Entfernung von Geschäftsgeheimnissen und die Anonymisierung der Informationen im Einklang mit den einschlägigen nationalen Vorschriften und Unionsvorschriften verantwortlich;
    d. übermittelt sie die Informationen unverzüglich, spätestens jedoch 24 Stunden nach Eingang der Informationen über einen meldepflichtigen Cyberangriff, den nationalen zentralen Anlaufstellen, den CSIRTs und allen gemäß Artikel 4 benannten zuständigen Behörden anderer Mitgliedstaten und stellt diesen Behörden oder Stellen regelmäßig aktualisierte Informationen zur Verfügung;

[71] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e3205-15-1

e. übermittelt sie die Informationen über den Cyberangriff nach Anonymisierung und Entfernung von Geschäftsgeheimnissen gemäß Absatz 1 Buchstabe c unverzüglich, spätestens jedoch 24 Stunden nach Eingang der Informationen gemäß Absatz 1 Buchstabe a, den Einrichtungen mit kritischen oder erheblichen Auswirkungen in ihrem Mitgliedstaat und stellt regelmäßig aktualisierte Informationen bereit, um den Einrichtungen einen wirksamen Schutz zu ermöglichen;

f. kann sie die meldende Einrichtung mit erheblichen oder kritischen Auswirkungen auffordern, die meldepflichtigen Informationen über Cyberangriffe auf sichere Weise an andere möglicherweise betroffene Einrichtungen weiterzuleiten, um den Elektrizitätssektor für die Lage zu sensibilisieren und zu verhindern, dass ein Risiko eintritt, das dort zu einem grenzüberschreitenden Cybersicherheitsvorfall eskalieren könnte;

g. übermittelt sie der ENISA nach Anonymisierung und Entfernung von Geschäftsgeheimnissen einen zusammenfassenden Bericht mit den Informationen zu dem Cyberangriff.

2. Erhält ein CSIRT Kenntnis von einer aktiv ausgenutzten Schwachstelle ohne Patch, so

   a. teilt es diese der ENISA unverzüglich über einen geeigneten Kanal für den sicheren Informationsaustausch mit, sofern in anderen Rechtsvorschriften der Union nichts anderes bestimmt ist;

   b. unterstützt es die betroffene Einrichtung dabei, vom Hersteller oder Anbieter eine wirksame, koordinierte und rasche Behandlung der aktiv ausgenutzten Schwachstelle ohne Patch oder wirksame und effiziente Abhilfemaßnahmen zu erhalten;

   c. tauscht es die verfügbaren Informationen mit dem Verkäufer aus und fordert den Hersteller oder Anbieter auf, möglichst eine Liste der CSIRTs in den Mitgliedstaaten vorzulegen, die von der aktiv ausgenutzten Schwachstelle ohne Patch betroffen sind und informiert werden müssen;

   d. tauscht es verfügbare Informationen nach dem Grundsatz „Kenntnis nur, wenn nötig“ mit den unter obigem Buchstaben genannten CSIRTs aus;

   e. stellt es Informationen über etwaige vorhandene Abhilfestrategien und -maßnahmen in Bezug auf die aktiv ausgenutzte Schwachstelle ohne Patch bereit.

3. Erhält eine zuständige Behörde Kenntnis von einer aktiv ausgenutzten Schwachstelle ohne Patch, so

   a. informiert sie in Abstimmung mit den CSIRTs in ihrem Mitgliedstaat über etwaige vorhandene Abhilfestrategien und -maßnahmen in Bezug auf die aktiv ausgenutzte Schwachstelle ohne Patch;

   b. übermittelt sie die Informationen an ein CSIRT in dem Mitgliedstaat, in dem die aktiv ausgenutzte Schwachstelle ohne Patch gemeldet wurde.

4. Erhält die zuständige Behörde Kenntnis von einer Schwachstelle ohne Patch, in Bezug auf die keine Beweise für eine aktive Ausnutzung vorliegen, stimmt sie sich unverzüglich mit dem CSIRT im Hinblick auf eine koordinierte Offenlegung von Schwachstellen gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 [72] ab.

[72] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_12

5. Erhält ein CSIRT gemäß Artikel 38 Absatz 6 von einer oder mehreren Einrichtungen mit erheblichen oder kritischen Auswirkungen Informationen in Bezug auf Cyberbedrohungen, so leitet es diese oder andere Informationen, die für die Verhütung, Erkennung, Behandlung oder Minderung des damit verbundenen Risikos von Bedeutung sind, an die Einrichtungen mit kritischen oder erheblichen Auswirkungen in seinem Mitgliedstaat und gegebenenfalls an alle betroffenen CSIRTs und seine nationale zentralen Anlaufstelle unverzüglich, spätestens jedoch vier Stunden nach Eingang der Informationen, weiter.

6. Erhält eine zuständige Behörde von einer oder mehreren Einrichtungen mit erheblichen oder kritischen Auswirkungen Informationen über Cyberbedrohungen, so leitet sie diese Informationen für die Zwecke des Absatzes 5 an das CSIRT weiter.

7. Die zuständigen Behörden können die Zuständigkeiten nach den Absätzen 3 und 4 in Bezug auf eine oder mehrere Einrichtungen mit erheblichen oder kritischen Auswirkungen, die in mehr als einem Mitgliedstaat tätig sind, ganz oder teilweise an eine andere zuständige Behörde in einem dieser Mitgliedstaaten delegieren, sofern sich die betroffenen zuständigen Behörden darauf geeinigt haben.

8. Die ÜNB entwickeln mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO bis zum 13 Juni 2025 eine Klassifizierungsmethode für Cyberangriffe. Die ÜNB können mit Unterstützung von ENTSO-E und der EU-VNBO die zuständigen Behörden ersuchen, die ENISA und ihre für Cybersicherheit zuständigen Behörden zur Unterstützung bei der Entwicklung einer solchen Klassifizierungsskala zu konsultieren. Die Methode muss fünf Stufen für die Schwere eines Cyberangriffs enthalten, wobei „erheblich“ und „kritisch“ die höchsten Stufen darstellen. Die Klassifizierung muss sich auf die Bewertung der folgenden Parameter stützen:

    a. die potenziellen Auswirkungen unter Berücksichtigung der gemäß Artikel 26 Absatz 4 Buchstabe c ermittelten exponierten Vermögenswerte und Perimeter und

    b. die Schwere des Cyberangriffs.

9. Bis zum 13 Juni 2026 führt ENTSO-E in Zusammenarbeit mit der EU-VNBO eine Machbarkeitsstudie hinsichtlich der Möglichkeit durch, ein gemeinsames Instrument zu entwickeln, das es allen Einrichtungen ermöglicht, Informationen mit den zuständigen nationalen Behörden auszutauschen, und prüft die damit verbundenen finanziellen Kosten.

10. In der Machbarkeitsstudie wird die Möglichkeit geprüft, ein solches gemeinsames Instrument

    a. zu nutzen, um Einrichtungen mit kritischen oder erheblichen Auswirkungen durch einschlägige sicherheitsrelevante Informationen für den Betrieb grenzüberschreitender Stromflüsse zu unterstützen, z. B. durch echtzeitnahe Berichterstattung über Cyberangriffe, Frühwarnungen im Zusammenhang mit Cybersicherheitsfragen und nicht offengelegten Schwachstellen von Geräten, die im Elektrizitätssystem eingesetzt werden;

    b. in einem geeigneten und äußerst vertrauenswürdigen Umfeld zu pflegen;

    c. zu nutzen, um Daten bei Einrichtungen mit kritischen oder erheblichen Auswirkungen zu erheben und die Entfernung vertraulicher Informationen und die Anonymisierung der Daten zu unterstützen und diese unverzüglich an Einrichtungen mit kritischen oder erheblichen Auswirkungen weiterzuleiten.

11. In Zusammenarbeit mit der EU-VNBO

a. konsultiert ENTSO-E bei der Machbarkeitsstudie die ENISA und die NIS-Kooperationsgruppe, die nationalen zentralen Anlaufstellen und die Vertreter der wichtigsten Interessenträger;

b. legt ENTSO-E die Ergebnisse der Machbarkeitsstudie der ACER und der NIS-Kooperationsgruppe vor

12. ENTSO-E kann in Zusammenarbeit mit der EU-VNBO Initiativen analysieren und unterstützen, die von Einrichtungen mit kritischen oder erheblichen Auswirkungen vorgeschlagen werden, um solche Instrumente für den Informationsaustausch zu bewerten und zu testen.

Artikel 37(1)

Erhält eine zuständige Behörde Informationen über einen meldepflichtigen Cyberangriff,

a. bewertet sie den Grad der Vertraulichkeit dieser Informationen und unterrichtet die Einrichtung unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Eingang der Informationen, über das Ergebnis ihrer Bewertung;

b. versucht sie, andere ähnliche Cyberangriffe in der Union zu ermitteln, die anderen zuständigen Behörden gemeldet wurden, um die zu dem meldepflichtigen Cyberangriff eingegangenen Informationen mit Informationen zu vergleichen, die zu anderen Cyberangriffen bereitgestellt wurden, und um vorhandene Informationen zu ergänzen sowie die Reaktion im Bereich der Cybersicherheit zu stärken und zu koordinieren;

c. ist sie für die Entfernung von Geschäftsgeheimnissen und die Anonymisierung der Informationen im Einklang mit den einschlägigen nationalen Vorschriften und Unionsvorschriften verantwortlich;

d. übermittelt sie die Informationen unverzüglich, spätestens jedoch 24 Stunden nach Eingang der Informationen über einen meldepflichtigen Cyberangriff, den nationalen zentralen Anlaufstellen, den CSIRTs und allen gemäß Artikel 4 benannten zuständigen Behörden anderer Mitgliedstaten und stellt diesen Behörden oder Stellen regelmäßig aktualisierte Informationen zur Verfügung;

e. übermittelt sie die Informationen über den Cyberangriff nach Anonymisierung und Entfernung von Geschäftsgeheimnissen gemäß Absatz 1 Buchstabe c unverzüglich, spätestens jedoch 24 Stunden nach Eingang der Informationen gemäß Absatz 1 Buchstabe a, den Einrichtungen mit kritischen oder erheblichen Auswirkungen in ihrem Mitgliedstaat und stellt regelmäßig aktualisierte Informationen bereit, um den Einrichtungen einen wirksamen Schutz zu ermöglichen;

f. kann sie die meldende Einrichtung mit erheblichen oder kritischen Auswirkungen auffordern, die meldepflichtigen Informationen über Cyberangriffe auf sichere Weise an andere möglicherweise betroffene Einrichtungen weiterzuleiten, um den Elektrizitätssektor für die Lage zu sensibilisieren und zu verhindern, dass ein Risiko eintritt, das dort zu einem grenzüberschreitenden Cybersicherheitsvorfall eskalieren könnte;

g. übermittelt sie der ENISA nach Anonymisierung und Entfernung von Geschäftsgeheimnissen einen zusammenfassenden Bericht mit den Informationen zu dem Cyberangriff.

Artikel 37(10)

In der Machbarkeitsstudie wird die Möglichkeit geprüft, ein solches gemeinsames Instrument

a. zu nutzen, um Einrichtungen mit kritischen oder erheblichen Auswirkungen durch einschlägige sicherheitsrelevante Informationen für den Betrieb grenzüberschreitender Stromflüsse zu unterstützen, z. B. durch echtzeitnahe Berichterstattung über Cyberangriffe, Frühwarnungen im Zusammenhang mit Cybersicherheitsfragen und nicht offengelegten Schwachstellen von Geräten, die im Elektrizitätssystem eingesetzt werden;

b. in einem geeigneten und äußerst vertrauenswürdigen Umfeld zu pflegen;

c. zu nutzen, um Daten bei Einrichtungen mit kritischen oder erheblichen Auswirkungen zu erheben und die Entfernung vertraulicher Informationen und die Anonymisierung der Daten zu unterstützen und diese unverzüglich an Einrichtungen mit kritischen oder erheblichen Auswirkungen weiterzuleiten.

Artikel 37(11)

In Zusammenarbeit mit der EU-VNBO

a. konsultiert ENTSO-E bei der Machbarkeitsstudie die ENISA und die NIS-Kooperationsgruppe, die nationalen zentralen Anlaufstellen und die Vertreter der wichtigsten Interessenträger;

b. legt ENTSO-E die Ergebnisse der Machbarkeitsstudie der ACER und der NIS-Kooperationsgruppe vor.

Artikel 37(12)

ENTSO-E kann in Zusammenarbeit mit der EU-VNBO Initiativen analysieren und unterstützen, die von Einrichtungen mit kritischen oder erheblichen Auswirkungen vorgeschlagen werden, um solche Instrumente für den Informationsaustausch zu bewerten und zu testen.

Artikel 37(2)

Erhält ein CSIRT Kenntnis von einer aktiv ausgenutzten Schwachstelle ohne Patch, so

a. teilt es diese der ENISA unverzüglich über einen geeigneten Kanal für den sicheren Informationsaustausch mit, sofern in anderen Rechtsvorschriften der Union nichts anderes bestimmt ist;

b. unterstützt es die betroffene Einrichtung dabei, vom Hersteller oder Anbieter eine wirksame, koordinierte und rasche Behandlung der aktiv ausgenutzten Schwachstelle ohne Patch oder wirksame und effiziente Abhilfemaßnahmen zu erhalten;

c. tauscht es die verfügbaren Informationen mit dem Verkäufer aus und fordert den Hersteller oder Anbieter auf, möglichst eine Liste der CSIRTs in den Mitgliedstaaten vorzulegen, die von der aktiv ausgenutzten Schwachstelle ohne Patch betroffen sind und informiert werden müssen;

d. tauscht es verfügbare Informationen nach dem Grundsatz „Kenntnis nur, wenn nötig" mit den unter obigem Buchstaben genannten CSIRTs aus;

e. stellt es Informationen über etwaige vorhandene Abhilfestrategien und -maßnahmen in Bezug auf die aktiv ausgenutzte Schwachstelle ohne Patch bereit.

Artikel 37(3)

Erhält eine zuständige Behörde Kenntnis von einer aktiv ausgenutzten Schwachstelle ohne Patch, so

a. informiert sie in Abstimmung mit den CSIRTs in ihrem Mitgliedstaat über etwaige vorhandene Abhilfestrategien und -maßnahmen in Bezug auf die aktiv ausgenutzte Schwachstelle ohne Patch;

b. übermittelt sie die Informationen an ein CSIRT in dem Mitgliedstaat, in dem die aktiv ausgenutzte Schwachstelle ohne Patch gemeldet wurde.

Artikel 37(4)

Erhält die zuständige Behörde Kenntnis von einer Schwachstelle ohne Patch, in Bezug auf die keine Beweise für eine aktive Ausnutzung vorliegen, stimmt sie sich unverzüglich mit dem CSIRT im Hinblick auf eine koordinierte Offenlegung von Schwachstellen gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 [73] ab.

Artikel 37(5)

Erhält ein CSIRT gemäß Artikel 38 Absatz 6 von einer oder mehreren Einrichtungen mit erheblichen oder kritischen Auswirkungen Informationen in Bezug auf Cyberbedrohungen, so leitet es diese oder andere Informationen, die für die Verhütung, Erkennung, Behandlung oder Minderung des damit verbundenen Risikos von Bedeutung sind, an die Einrichtungen mit kritischen oder erheblichen Auswirkungen in seinem Mitgliedstaat und gegebenenfalls an alle betroffenen CSIRTs und seine nationale zentralen Anlaufstelle unverzüglich, spätestens jedoch vier Stunden nach Eingang der Informationen, weiter.

Artikel 37(6)

[73] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_12

Erhält eine zuständige Behörde von einer oder mehreren Einrichtungen mit erheblichen oder kritischen Auswirkungen Informationen über Cyberbedrohungen, so leitet sie diese Informationen für die Zwecke des Absatzes 5 an das CSIRT weiter.

Artikel 37(7)

Die zuständigen Behörden können die Zuständigkeiten nach den Absätzen 3 und 4 in Bezug auf eine oder mehrere Einrichtungen mit erheblichen oder kritischen Auswirkungen, die in mehr als einem Mitgliedstaat tätig sind, ganz oder teilweise an eine andere zuständige Behörde in einem dieser Mitgliedstaaten delegieren, sofern sich die betroffenen zuständigen Behörden darauf geeinigt haben.

Artikel 37(8)

Die ÜNB entwickeln mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO bis zum 13 Juni 2025 eine Klassifizierungsmethode für Cyberangriffe. Die ÜNB können mit Unterstützung von ENTSO-E und der EU-VNBO die zuständigen Behörden ersuchen, die ENISA und ihre für Cybersicherheit zuständigen Behörden zur Unterstützung bei der Entwicklung einer solchen Klassifizierungsskala zu konsultieren. Die Methode muss fünf Stufen für die Schwere eines Cyberangriffs enthalten, wobei „erheblich“ und „kritisch“ die höchsten Stufen darstellen. Die Klassifizierung muss sich auf die Bewertung der folgenden Parameter stützen:

a. die potenziellen Auswirkungen unter Berücksichtigung der gemäß Artikel 26 Absatz 4 Buchstabe c ermittelten exponierten Vermögenswerte und Perimeter und
b. die Schwere des Cyberangriffs.

Artikel 37(9)

Bis zum 13 Juni 2026 führt ENTSO-E in Zusammenarbeit mit der EU-VNBO eine Machbarkeitsstudie hinsichtlich der Möglichkeit durch, ein gemeinsames Instrument zu entwickeln, das es allen Einrichtungen ermöglicht, Informationen mit den zuständigen nationalen Behörden auszutauschen, und prüft die damit verbundenen finanziellen Kosten.

Artikel 38

1. Jede Einrichtung mit erheblichen oder kritischen Auswirkungen
    a. richtet für alle Vermögenswerte innerhalb ihres gemäß Artikel 26 Absatz 4 Buchstabe c bestimmten Cybersicherheitsperimeters mindestens die CSOC-Kapazitäten ein, um
        i. sicherzustellen, dass die einschlägigen Netz- und Informationssysteme und -anwendungen Sicherheitsprotokolle für die Sicherheitsüberwachung umfassen, damit Anomalien erkannt und Informationen über Cyberangriffe erhoben werden können;

ii. die Sicherheitsüberwachung durchzuführen, einschließlich der Erkennung eines Eindringens und der Bewertung von Schwachstellen von Netz- und Informationssystemen;
iii. zu analysieren und erforderlichenfalls im Rahmen ihrer Zuständigkeit und Kapazitäten alle für den Schutz der Einrichtung erforderlichen Maßnahmen zu ergreifen;
iv. sich an der in diesem Artikel beschriebenen Erhebung und Weitergabe von Informationen zu beteiligen;

b. ist berechtigt, sich diese Kapazitäten gemäß Buchstabe a ganz oder teilweise über MSSP zu beschaffen. Einrichtungen mit kritischen oder erheblichen Auswirkungen bleiben für die MSSP verantwortlich und überwachen deren Bemühungen;

c. benennt für den Informationsaustausch eine zentrale Anlaufstelle auf Ebene der Einrichtung.

2. Die ENISA kann im Rahmen der in Artikel 6 Absatz 2 der Verordnung (EU) 2019/881 [74] festgelegten Aufgabe unverbindliche Leitlinien für die Einrichtung solcher Kapazitäten oder die Vergabe von Unteraufträgen an MSSP für die Erbringung des Dienstes herausgeben.

3. Jede Einrichtung mit kritischen oder erheblichen Auswirkungen teilt ihren CSIRTs und der für sie zuständigen Behörde relevante Informationen im Zusammenhang mit einem meldepflichtigen Cyberangriff unverzüglich, spätestens jedoch vier Stunden, nachdem ihr bekannt wurde, dass der Sicherheitsvorfall meldepflichtig ist, mit.

4. Informationen im Zusammenhang mit einem Cyberangriff gelten als meldepflichtig, wenn der Cyberangriff bei der Bewertung durch die betroffene Einrichtung nach der Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8 als „erheblich“ bis „kritisch“ eingestuft wird. Die gemäß Absatz 1 Buchstabe c benannte zentrale Anlaufstelle auf Ebene der Einrichtung teilt die Einstufung des Sicherheitsvorfalls mit.

5. Übermitteln Einrichtungen mit kritischen oder erheblichen Auswirkungen relevante Informationen zu aktiv ausgenutzten Schwachstellen ohne Patch an ein CSIRT, so kann dieses diese Informationen an die für das CSIRT zuständige Behörde weiterleiten. Je nach Sensibilität der gemeldeten Informationen kann das CSIRT die Informationen aus triftigen cybersicherheitsbezogenen Gründen zurückhalten oder zeitverzögert übermitteln.

6. Jede Einrichtung mit kritischen oder erheblichen Auswirkungen stellt ihren CSIRTs unverzüglich alle Informationen im Zusammenhang mit einer meldepflichtigen Cyberbedrohung bereit, die grenzüberschreitende Auswirkungen haben könnte. Informationen im Zusammenhang mit einer Cyberbedrohung gelten als meldepflichtig, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

a. Sie umfassen relevante Informationen für die Verhütung, Erkennung, Behandlung oder Minderung der Auswirkungen des Risikos durch andere Einrichtungen mit kritischen oder erheblichen Auswirkungen;

b. die ermittelten, im Zusammenhang mit einem Angriff genutzten Vorgehensweisen, Taktiken und Verfahren sind mit Informationen wie kompromittierten URL-Adressen oder IP-Adressen, Hashs oder anderen Attributen verbunden, die für die Kontextualisierung und Zuordnung des Angriffs nützlich sind;

[74] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

c. eine Cyberbedrohung kann weiter bewertet und mit zusätzlichen Informationen verknüpft werden, die von Dienstanbietern oder Dritten, die nicht dieser Verordnung unterliegen, bereitgestellt werden.

7. Jede Einrichtung mit kritischen oder erheblichen Auswirkungen gibt beim Austausch von Informationen gemäß diesem Artikel an,

   a. dass die Informationen gemäß dieser Verordnung übermittelt werden;
   b. ob die Informationen Folgendes betreffen:
      i. einen meldepflichtigen Cyberangriff gemäß Absatz 3;
      ii. nicht öffentlich bekannte aktiv ausgenutzte Schwachstellen ohne Patch gemäß Absatz 4;
      iii. eine meldepflichtige Cyberbedrohung gemäß Absatz 5;
   c. im Falle eines meldepflichtigen Cyberangriffs, welchen Grad der Cyberangriff nach der in Artikel 37 Absatz 8 genannten Klassifizierungsmethode für Cyberangriffe aufweist und welche Informationen zu dieser Einstufung geführt haben, einschließlich mindestens der Kritikalität des Cyberangriffs.

8. Meldet eine Einrichtung mit kritischen oder erheblichen Auswirkungen einen erheblichen Sicherheitsvorfall gemäß Artikel 23 der Richtlinie (EU) 2022/2555 [75] und enthält die Meldung des Sicherheitsvorfalls nach dem genannten Artikel einschlägige Informationen gemäß Absatz 3 des vorliegenden Artikels, so gilt die Meldung der Einrichtung nach Artikel 23 Absatz 1 der genannten Richtlinie auch als Meldung von Informationen gemäß Absatz 3 des vorliegenden Artikels.

9. Jede Einrichtung mit kritischen oder erheblichen Auswirkungen erstattet der für sie zuständigen Behörde oder dem CSIRT Bericht, wobei sie klar angibt, welche Informationen nur an die zuständige Behörde oder das CSIRT übermittelt werden dürfen, wenn der Informationsaustausch die Quelle eines Cyberangriffs sein könnte. Jede Einrichtung mit kritischen oder erheblichen Auswirkungen hat das Recht, dem zuständigen CSIRT eine nichtvertrauliche Fassung der Informationen zur Verfügung zu stellen.

Artikel 38(1)

Jede Einrichtung mit erheblichen oder kritischen Auswirkungen

a. richtet für alle Vermögenswerte innerhalb ihres gemäß Artikel 26 Absatz 4 Buchstabe c bestimmten Cybersicherheitsperimeters mindestens die CSOC-Kapazitäten ein, um

   i. sicherzustellen, dass die einschlägigen Netz- und Informationssysteme und -anwendungen Sicherheitsprotokolle für die Sicherheitsüberwachung umfassen, damit Anomalien erkannt und Informationen über Cyberangriffe erhoben werden können;
   ii. die Sicherheitsüberwachung durchzuführen, einschließlich der Erkennung eines Eindringens und der Bewertung von Schwachstellen von Netz- und Informationssystemen;

[75] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#tit_1

iii. zu analysieren und erforderlichenfalls im Rahmen ihrer Zuständigkeit und Kapazitäten alle für den Schutz der Einrichtung erforderlichen Maßnahmen zu ergreifen;

iv. sich an der in diesem Artikel beschriebenen Erhebung und Weitergabe von Informationen zu beteiligen;

b. ist berechtigt, sich diese Kapazitäten gemäß Buchstabe a ganz oder teilweise über MSSP zu beschaffen. Einrichtungen mit kritischen oder erheblichen Auswirkungen bleiben für die MSSP verantwortlich und überwachen deren Bemühungen;

c. benennt für den Informationsaustausch eine zentrale Anlaufstelle auf Ebene der Einrichtung.

Artikel 38(2)

Die ENISA kann im Rahmen der in Artikel 6 Absatz 2 der Verordnung (EU) 2019/881 [76] festgelegten Aufgabe unverbindliche Leitlinien für die Einrichtung solcher Kapazitäten oder die Vergabe von Unteraufträgen an MSSP für die Erbringung des Dienstes herausgeben.

Artikel 38(3)

Jede Einrichtung mit kritischen oder erheblichen Auswirkungen teilt ihren CSIRTs und der für sie zuständigen Behörde relevante Informationen im Zusammenhang mit einem meldepflichtigen Cyberangriff unverzüglich, spätestens jedoch vier Stunden, nachdem ihr bekannt wurde, dass der Sicherheitsvorfall meldepflichtig ist, mit.

Artikel 38(4)

Informationen im Zusammenhang mit einem Cyberangriff gelten als meldepflichtig, wenn der Cyberangriff bei der Bewertung durch die betroffene Einrichtung nach der Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8 als „erheblich“ bis „kritisch“ eingestuft wird. Die gemäß Absatz 1 Buchstabe c benannte zentrale Anlaufstelle auf Ebene der Einrichtung teilt die Einstufung des Sicherheitsvorfalls mit.

Artikel 38(5)

Übermitteln Einrichtungen mit kritischen oder erheblichen Auswirkungen relevante Informationen zu aktiv ausgenutzten Schwachstellen ohne Patch an ein CSIRT, so kann dieses diese Informationen an die für das CSIRT zuständige Behörde weiterleiten. Je nach Sensibilität der gemeldeten Informationen kann das CSIRT die Informationen aus triftigen cybersicherheitsbezogenen Gründen zurückhalten oder zeitverzögert übermitteln.

Artikel 38(6)

[76] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Jede Einrichtung mit kritischen oder erheblichen Auswirkungen stellt ihren CSIRTs unverzüglich alle Informationen im Zusammenhang mit einer meldepflichtigen Cyberbedrohung bereit, die grenzüberschreitende Auswirkungen haben könnte. Informationen im Zusammenhang mit einer Cyberbedrohung gelten als meldepflichtig, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

a. Sie umfassen relevante Informationen für die Verhütung, Erkennung, Behandlung oder Minderung der Auswirkungen des Risikos durch andere Einrichtungen mit kritischen oder erheblichen Auswirkungen;

b. die ermittelten, im Zusammenhang mit einem Angriff genutzten Vorgehensweisen, Taktiken und Verfahren sind mit Informationen wie kompromittierten URL-Adressen oder IP-Adressen, Hashs oder anderen Attributen verbunden, die für die Kontextualisierung und Zuordnung des Angriffs nützlich sind;

c. eine Cyberbedrohung kann weiter bewertet und mit zusätzlichen Informationen verknüpft werden, die von Dienstanbietern oder Dritten, die nicht dieser Verordnung unterliegen, bereitgestellt werden.

Artikel 38(7)

Jede Einrichtung mit kritischen oder erheblichen Auswirkungen gibt beim Austausch von Informationen gemäß diesem Artikel an,

a. dass die Informationen gemäß dieser Verordnung übermittelt werden;

b. ob die Informationen Folgendes betreffen:

   i. einen meldepflichtigen Cyberangriff gemäß Absatz 3;

   ii. nicht öffentlich bekannte aktiv ausgenutzte Schwachstellen ohne Patch gemäß Absatz 4;

   iii. eine meldepflichtige Cyberbedrohung gemäß Absatz 5;

c. im Falle eines meldepflichtigen Cyberangriffs, welchen Grad der Cyberangriff nach der in Artikel 37 Absatz 8 genannten Klassifizierungsmethode für Cyberangriffe aufweist und welche Informationen zu dieser Einstufung geführt haben, einschließlich mindestens der Kritikalität des Cyberangriffs.

Artikel 38(8)

Meldet eine Einrichtung mit kritischen oder erheblichen Auswirkungen einen erheblichen Sicherheitsvorfall gemäß Artikel 23 der Richtlinie (EU) 2022/2555 [77] und enthält die Meldung des Sicherheitsvorfalls nach dem genannten Artikel einschlägige Informationen gemäß Absatz 3 des

[77] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#tit_1

vorliegenden Artikels, so gilt die Meldung der Einrichtung nach Artikel 23 Absatz 1 der genannten Richtlinie auch als Meldung von Informationen gemäß Absatz 3 des vorliegenden Artikels.

Artikel 38(9)

Jede Einrichtung mit kritischen oder erheblichen Auswirkungen erstattet der für sie zuständigen Behörde oder dem CSIRT Bericht, wobei sie klar angibt, welche Informationen nur an die zuständige Behörde oder das CSIRT übermittelt werden dürfen, wenn der Informationsaustausch die Quelle eines Cyberangriffs sein könnte. Jede Einrichtung mit kritischen oder erheblichen Auswirkungen hat das Recht, dem zuständigen CSIRT eine nichtvertrauliche Fassung der Informationen zur Verfügung zu stellen.

Artikel 39

1. Einrichtungen mit erheblichen oder kritischen Auswirkungen entwickeln mit der erforderlichen Unterstützung der jeweils zuständigen Behörde, von ENTSO-E und der EU-VNBO die erforderlichen Kapazitäten für den Umgang mit entdeckten Cyberangriffen. Einrichtungen mit kritischen oder erheblichen Auswirkungen können von dem CSIRT unterstützt werden, das in ihrem jeweiligen Mitgliedstaat im Rahmen der den CSIRTs gemäß Artikel 11 Absatz 5 Buchstabe a der Richtlinie (EU) 2022/2555 [78] übertragenen Aufgabe benannt wurde.
2. Hat ein Cyberangriff Auswirkungen auf grenzüberschreitende Stromflüsse, so arbeiten die zentralen Anlaufstellen auf Ebene der betroffenen Einrichtungen mit kritischen oder erheblichen Auswirkungen zusammen, um Informationen untereinander auszutauschen, wobei sie von der zuständigen Behörde des Mitgliedstaats, in dem der Cyberangriff zuerst gemeldet wurde, koordiniert werden.
3. Einrichtungen mit kritischen oder erheblichen Auswirkungen
    a. stellen sicher, dass ihre eigene zentrale Anlaufstelle auf Ebene der Einrichtung nach dem Grundsatz „Kenntnis nur, wenn nötig“ Zugang zu den Informationen hat, die sie von der nationalen zentralen Anlaufstelle über ihre zuständige Behörde erhalten hat;
    b. übermitteln, sofern dies nicht bereits gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2022/2555 geschehen ist, der zuständigen Behörde des Mitgliedstaats, in dem sie niedergelassen sind, und der nationalen zentralen Anlaufstelle eine Liste ihrer für die Cybersicherheit zuständigen zentralen Anlaufstellen,
        i. von denen die zuständige Behörde und die nationale zentrale Anlaufstelle Informationen über meldepflichtige Cyberangriffe erhalten könnte;
        ii. an die die zuständigen Behörden und die nationalen zentralen Anlaufstellen gegebenenfalls Informationen übermitteln müssen;
    c. richten auf der Grundlage der beobachtbaren Entwicklung des Cyberangriffs innerhalb der Perimeter mit kritischen oder erheblichen Auswirkungen Verfahren zur Bewältigung von Cyberangriffen ein, einschließlich Rollen und Zuständigkeiten, Aufgaben und Reaktionen;

[78] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_11

d. testen mindestens einmal jährlich alle Verfahren zur Bewältigung von Cyberangriffen, wobei sie mindestens ein Szenario testen, das sich direkt oder indirekt auf grenzüberschreitende Stromflüsse auswirkt. Dieser jährliche Test kann von Einrichtungen mit kritischen oder erheblichen Auswirkungen während der regelmäßigen Übungen gemäß Artikel 43 durchgeführt werden. Jede Live-Reaktionsmaßnahme auf einen Cyberangriff mit einer Folge, die gemäß der in Artikel 37 Absatz 8 genannten Klassifizierungsmethode für Cyberangriffe mindestens in die Stufe 2 eingestuft wird und der eine Cybersicherheitsursache zugrunde liegt, kann als jährlicher Test des Plans für die Reaktion auf Cyberangriffe betrachtet werden.

4. Die in Absatz 1 aufgeführten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 der Verordnung (EU) 2019/943 [79] auch an die regionalen Koordinierungszentren delegiert werden.

Artikel 39(1)

Einrichtungen mit erheblichen oder kritischen Auswirkungen entwickeln mit der erforderlichen Unterstützung der jeweils zuständigen Behörde, von ENTSO-E und der EU-VNBO die erforderlichen Kapazitäten für den Umgang mit entdeckten Cyberangriffen. Einrichtungen mit kritischen oder erheblichen Auswirkungen können von dem CSIRT unterstützt werden, das in ihrem jeweiligen Mitgliedstaat im Rahmen der den CSIRTs gemäß Artikel 11 Absatz 5 Buchstabe a der Richtlinie (EU) 2022/2555 [80] übertragenen Aufgabe benannt wurde.

Einrichtungen mit kritischen oder erheblichen Auswirkungen setzen wirksame Verfahren zur Ermittlung, Klassifizierung und Bewältigung von Cyberangriffen ein, die sich auf grenzüberschreitende Stromflüsse auswirken oder auswirken könnten, um deren Auswirkungen möglichst gering zu halten.

Artikel 39(2)

Hat ein Cyberangriff Auswirkungen auf grenzüberschreitende Stromflüsse, so arbeiten die zentralen Anlaufstellen auf Ebene der betroffenen Einrichtungen mit kritischen oder erheblichen Auswirkungen zusammen, um Informationen untereinander auszutauschen, wobei sie von der zuständigen Behörde des Mitgliedstaats, in dem der Cyberangriff zuerst gemeldet wurde, koordiniert werden.

Artikel 39(3)

Einrichtungen mit kritischen oder erheblichen Auswirkungen

a. stellen sicher, dass ihre eigene zentrale Anlaufstelle auf Ebene der Einrichtung nach dem Grundsatz „Kenntnis nur, wenn nötig“ Zugang zu den Informationen hat, die sie von der nationalen zentralen Anlaufstelle über ihre zuständige Behörde erhalten hat;

[79] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1
[80] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_11

b. übermitteln, sofern dies nicht bereits gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2022/2555 geschehen ist, der zuständigen Behörde des Mitgliedstaats, in dem sie niedergelassen sind, und der nationalen zentralen Anlaufstelle eine Liste ihrer für die Cybersicherheit zuständigen zentralen Anlaufstellen,

   i. von denen die zuständige Behörde und die nationale zentrale Anlaufstelle Informationen über meldepflichtige Cyberangriffe erhalten könnte;

   ii. an die die zuständigen Behörden und die nationalen zentralen Anlaufstellen gegebenenfalls Informationen übermitteln müssen;

c. richten auf der Grundlage der beobachtbaren Entwicklung des Cyberangriffs innerhalb der Perimeter mit kritischen oder erheblichen Auswirkungen Verfahren zur Bewältigung von Cyberangriffen ein, einschließlich Rollen und Zuständigkeiten, Aufgaben und Reaktionen;

d. testen mindestens einmal jährlich alle Verfahren zur Bewältigung von Cyberangriffen, wobei sie mindestens ein Szenario testen, das sich direkt oder indirekt auf grenzüberschreitende Stromflüsse auswirkt. Dieser jährliche Test kann von Einrichtungen mit kritischen oder erheblichen Auswirkungen während der regelmäßigen Übungen gemäß Artikel 43 durchgeführt werden. Jede Live-Reaktionsmaßnahme auf einen Cyberangriff mit einer Folge, die gemäß der in Artikel 37 Absatz 8 genannten Klassifizierungsmethode für Cyberangriffe mindestens in die Stufe 2 eingestuft wird und der eine Cybersicherheitsursache zugrunde liegt, kann als jährlicher Test des Plans für die Reaktion auf Cyberangriffe betrachtet werden.

Artikel 39(4)

Die in Absatz 1 aufgeführten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 der Verordnung (EU) 2019/943 [81] auch an die regionalen Koordinierungszentren delegiert werden.

Artikel 4

1. So bald wie möglich, in jedem Fall aber bis zum 13 Dezember 2024, benennt jeder Mitgliedstaat eine nationale Regierungs- oder Regulierungsbehörde, die für die Wahrnehmung der ihr in dieser Verordnung übertragenen Aufgaben zuständig ist (im Folgenden „zuständige Behörde“). Bis die Aufgaben im Rahmen dieser Verordnung auf die zuständige Behörde übertragen wurden, nimmt die von jedem Mitgliedstaat gemäß Artikel 57 Absatz 1 der Richtlinie (EU) 2019/944 [82] benannte Regulierungsbehörde die Aufgaben der zuständigen Behörde im Einklang mit dieser Verordnung wahr.

2. Die Mitgliedstaaten unterrichten die Kommission, die ACER, die ENISA, die gemäß Artikel 14 der Richtlinie (EU) 2022/2555 [83] eingesetzte NIS-Kooperationsgruppe und die gemäß Artikel

[81] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1
[82] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02019L0944-20240716#art_57
[83] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_14

1 des Beschlusses der Kommission vom 15. November 2012 [84] eingesetzte Koordinierungsgruppe „Strom“ unverzüglich und teilen ihnen den Namen und die Kontaktdaten ihrer gemäß Absatz 1 des vorliegenden Artikels benannten zuständigen Behörde sowie etwaige spätere Änderungen in Bezug auf diese Behörde mit.

3. Die Mitgliedstaaten können ihrer zuständigen Behörde gestatten, Aufgaben, die ihr in dieser Verordnung übertragen wurden, an andere nationale Behörden zu delegieren, mit Ausnahme der in Artikel 5 aufgeführten Aufgaben. Jede zuständige Behörde überwacht die Anwendung dieser Verordnung durch die Behörden, an die sie Aufgaben delegiert hat. Die zuständige Behörde teilt der Kommission, der ACER, der Koordinierungsgruppe „Strom“, der ENISA und der NISKooperationsgruppe den Namen der Behörden, an die sie Aufgaben delegiert hat, deren Kontaktdaten, die ihnen übertragenen Aufgaben sowie etwaige spätere Änderungen mit.

Artikel 4(1)

So bald wie möglich, in jedem Fall aber bis zum 13 Dezember 2024, benennt jeder Mitgliedstaat eine nationale Regierungs- oder Regulierungsbehörde, die für die Wahrnehmung der ihr in dieser Verordnung übertragenen Aufgaben zuständig ist (im Folgenden „zuständige Behörde“). Bis die Aufgaben im Rahmen dieser Verordnung auf die zuständige Behörde übertragen wurden, nimmt die von jedem Mitgliedstaat gemäß Artikel 57 Absatz 1 der Richtlinie (EU) 2019/944 [85] benannte Regulierungsbehörde die Aufgaben der zuständigen Behörde im Einklang mit dieser Verordnung wahr.

Artikel 4(2)

Die Mitgliedstaaten unterrichten die Kommission, die ACER, die ENISA, die gemäß Artikel 14 der Richtlinie (EU) 2022/2555 [86] eingesetzte NIS-Kooperationsgruppe und die gemäß Artikel 1 des Beschlusses der Kommission vom 15. November 2012 [87] eingesetzte Koordinierungsgruppe „Strom“ unverzüglich und teilen ihnen den Namen und die Kontaktdaten ihrer gemäß Absatz 1 des vorliegenden Artikels benannten zuständigen Behörde sowie etwaige spätere Änderungen in Bezug auf diese Behörde mit.

Artikel 4(3)

Die Mitgliedstaaten können ihrer zuständigen Behörde gestatten, Aufgaben, die ihr in dieser Verordnung übertragen wurden, an andere nationale Behörden zu delegieren, mit Ausnahme der in Artikel 5 aufgeführten Aufgaben. Jede zuständige Behörde überwacht die Anwendung dieser Verordnung durch die Behörden, an die sie Aufgaben delegiert hat.

Die zuständige Behörde teilt der Kommission, der ACER, der Koordinierungsgruppe „Strom“, der

[84] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32012D1117(01)
[85] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02019L0944-20240716#art_57
[86] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_14
[87] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32012D1117(01)

ENISA und der NISKooperationsgruppe den Namen der Behörden, an die sie Aufgaben delegiert hat, deren Kontaktdaten, die ihnen übertragenen Aufgaben sowie etwaige spätere Änderungen mit.

Artikel 40

1. Stellt die zuständige Behörde fest, dass eine Stromversorgungskrise im Zusammenhang mit einem Cyberangriff steht, der Auswirkungen auf mehr als einen Mitgliedstaat hat, setzen die zuständigen Behörden der betroffenen Mitgliedstaaten, die CS-NCA, die RP-NCA und die NIS-Behörden für das Cyberkrisenmanagement der betroffenen Mitgliedstaaten gemeinsam eine Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen ein.
2. Die Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen
   a. koordiniert eine effiziente Einholung aller relevanten Cybersicherheitsinformationen und deren weitere Übermittlung an die am Krisenmanagementprozess beteiligten Einrichtungen;
   b. organisiert die Kommunikation zwischen allen von der Krise betroffenen Einrichtungen und den zuständigen Behörden, um Überschneidungen zu verringern und die Effizienz der Analysen und technischen Reaktionen zur Bewältigung zeitgleich auftretender Stromversorgungskrisen, denen eine Cybersicherheitsursache zugrunde liegt, zu erhöhen;
   c. stellt in Zusammenarbeit mit den zuständigen CSIRTs das erforderliche Fachwissen bereit, einschließlich operativer Beratung bei der Umsetzung möglicher Abhilfemaßnahmen für die von dem Sicherheitsvorfall betroffenen Einrichtungen;
   d. unterrichtet die Kommission und die Koordinierungsgruppe „Strom“ im Einklang mit den in Artikel 46 festgelegten Schutzprinzipien über den Stand des Sicherheitsvorfalls und aktualisiert diese Informationen regelmäßig;
   e. holt Rat bei den zuständigen Behörden, Agenturen oder Einrichtungen ein, die zur Bewältigung der Stromversorgungskrise beitragen könnten.
3. Gilt der Cyberangriff als Cybersicherheitsvorfall großen Ausmaßes oder wird dies erwartet, unterrichtet die Ad-hocKoordinierungsgruppe für grenzüberschreitende Krisen unverzüglich die nationalen Behörden für das Cyberkrisenmanagement gemäß Artikel 9 Absatz 1 [88] der Richtlinie (EU) 2022/2555 in den von dem Sicherheitsvorfall betroffenen Mitgliedstaaten sowie die Kommission und das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe). In einer solchen Situation unterstützt die Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen das EU-CyCLONe in Bezug auf sektorale Besonderheiten.
4. Einrichtungen mit kritischen oder erheblichen Auswirkungen müssen Kapazitäten, interne Leitlinien, Vorsorgepläne und Personal, das an der Aufdeckung und Eindämmung grenzüberschreitender Krisen mitwirkt, vorsehen und darüber verfügen. Die von einer zeitgleich auftretenden Stromversorgungskrise betroffene Einrichtung mit kritischen oder erheblichen Auswirkungen untersucht die zugrunde liegende Ursache dieser Krise in Zusammenarbeit mit der für sie zuständigen Behörde, um festzustellen, inwieweit die Krise mit einem Cyberangriff in Verbindung steht.

[88] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9

5. Die in Absatz 4 genannten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 [89] der Verordnung (EU) 2019/943 auch an die regionalen Koordinierungszentren delegiert werden.

Artikel 40(1)

Stellt die zuständige Behörde fest, dass eine Stromversorgungskrise im Zusammenhang mit einem Cyberangriff steht, der Auswirkungen auf mehr als einen Mitgliedstaat hat, setzen die zuständigen Behörden der betroffenen Mitgliedstaaten, die CS-NCA, die RP-NCA und die NIS-Behörden für das Cyberkrisenmanagement der betroffenen Mitgliedstaaten gemeinsam eine Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen ein.

Artikel 40(2)

Die Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen

a. koordiniert eine effiziente Einholung aller relevanten Cybersicherheitsinformationen und deren weitere Übermittlung an die am Krisenmanagementprozess beteiligten Einrichtungen;
b. organisiert die Kommunikation zwischen allen von der Krise betroffenen Einrichtungen und den zuständigen Behörden, um Überschneidungen zu verringern und die Effizienz der Analysen und technischen Reaktionen zur Bewältigung zeitgleich auftretender Stromversorgungskrisen, denen eine Cybersicherheitsursache zugrunde liegt, zu erhöhen;
c. stellt in Zusammenarbeit mit den zuständigen CSIRTs das erforderliche Fachwissen bereit, einschließlich operativer Beratung bei der Umsetzung möglicher Abhilfemaßnahmen für die von dem Sicherheitsvorfall betroffenen Einrichtungen;
d. unterrichtet die Kommission und die Koordinierungsgruppe „Strom“ im Einklang mit den in Artikel 46 festgelegten Schutzprinzipien über den Stand des Sicherheitsvorfalls und aktualisiert diese Informationen regelmäßig;
e. holt Rat bei den zuständigen Behörden, Agenturen oder Einrichtungen ein, die zur Bewältigung der Stromversorgungskrise beitragen könnten.

Artikel 40(3)

Gilt der Cyberangriff als Cybersicherheitsvorfall großen Ausmaßes oder wird dies erwartet, unterrichtet die Ad-hocKoordinierungsgruppe für grenzüberschreitende Krisen unverzüglich die nationalen Behörden für das Cyberkrisenmanagement gemäß Artikel 9 Absatz 1 [90] der Richtlinie

[89] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1
[90] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9

(EU) 2022/2555 in den von dem Sicherheitsvorfall betroffenen Mitgliedstaaten sowie die Kommission und das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe). In einer solchen Situation unterstützt die Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen das EU-CyCLONe in Bezug auf sektorale Besonderheiten.

Artikel 40(4)

Einrichtungen mit kritischen oder erheblichen Auswirkungen müssen Kapazitäten, interne Leitlinien, Vorsorgepläne und Personal, das an der Aufdeckung und Eindämmung grenzüberschreitender Krisen mitwirkt, vorsehen und darüber verfügen. Die von einer zeitgleich auftretenden Stromversorgungskrise betroffene Einrichtung mit kritischen oder erheblichen Auswirkungen untersucht die zugrunde liegende Ursache dieser Krise in Zusammenarbeit mit der für sie zuständigen Behörde, um festzustellen, inwieweit die Krise mit einem Cyberangriff in Verbindung steht.

Artikel 40(5)

Die in Absatz 4 genannten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 [91] der Verordnung (EU) 2019/943 auch an die regionalen Koordinierungszentren delegiert werden.

Artikel 41

1. Innerhalb von 24 Monaten nach der Übermittlung des Berichts über die unionsweite Risikobewertung an die ACER entwickelt diese in enger Zusammenarbeit mit der ENISA, ENTSO-E, der EU-VNBO, den CS-NCA, den zuständigen Behörden, den RP-NCA, den NRB und den nationalen NIS-Behörden für das Cyberkrisenmanagement einen unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplan für den Elektrizitätssektor.
2. Innerhalb von 12 Monaten nach der Ausarbeitung des unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplans für den Elektrizitätssektor gemäß Absatz 1 durch die ACER erstellt jede zuständige Behörde einen nationalen Cybersicherheitskrisenmanagement- und -reaktionsplan für grenzüberschreitende Stromflüsse unter Berücksichtigung des unionsweiten Cybersicherheitskrisenmanagem und -reaktionsplans für den Elektrizitätssektor und des gemäß Artikel 10 der Verordnung (EU) 2019/941 [92] erstellten nationalen Risikovorsorgeplans. Dieser Plan muss mit dem Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gemäß Artikel 9 Absatz 4 der Richtlinie (EU) 2022/2555 [93] im Einklang stehen. Die zuständige Behörde stimmt sich mit den Einrichtungen mit kritischen oder erheblichen Auswirkungen sowie mit der RP-NCA in ihrem Mitgliedstaat ab.
3. Der gemäß Artikel 9 Absatz 4 der Richtlinie (EU) 2022/2555 [94] erforderliche nationale Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gilt als nationaler

[91] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1
[92] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e928-1-1
[93] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9
[94] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9

Plan für das Cybersicherheitskrisenmanagement im Sinne dieses Artikels, wenn er Bestimmungen für das Krisenmanagement und die Krisenreaktion in Bezug auf grenzüberschreitende Stromflüsse enthält.

4. Die in den Absätzen 1 und 2 aufgeführten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 [95] der Verordnung (EU) 2019/943 auch an die regionalen Koordinierungszentren delegiert werden.

5. Einrichtungen mit kritischen oder erheblichen Auswirkungen stellen sicher, dass ihre Krisenmanagementprozesse im Bereich der Cybersicherheit

   a. kompatible Verfahren für die grenzüberschreitende Bewältigung von Cybersicherheitsvorfällen gemäß Artikel 6 Nummer 8 der Richtlinie (EU) 2022/2555 [96] umfassen, die förmlich in ihren Krisenmanagementpläne enthalten sind;

   b. Teil der allgemeinen Krisenmanagementmaßnahmen sind.

6. Innerhalb von 12 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre erstellen Einrichtungen mit kritischen oder erheblichen Auswirkungen auf Ebene der Einrichtung einen Krisenmanagementplan für Cybersicherheitskrisen, der in ihre allgemeinen Krisenmanagementpläne aufgenommen wird. Dieser Plan muss mindestens Folgendes umfassen:

   a. Regeln für die Erklärung einer Krise gemäß Artikel 14 Absätze 2 und 3 der Verordnung (EU) 2019/941; [97]

   b. klare Aufgaben und Zuständigkeiten für das Krisenmanagement, einschließlich der Rolle anderer relevanter Einrichtungen mit kritischen oder erheblichen Auswirkungen;

   c. aktuelle Kontaktinformationen sowie Regeln für die Kommunikation und den Informationsaustausch während einer Krisensituation, einschließlich der Verbindung zu den CSIRTs.

7. Die Maßnahmen für das Krisenmanagement gemäß Artikel 21 Absatz 2 [98] Buchstabe c der Richtlinie (EU) 2022/2555 gelten als Krisenmanagementplan auf Ebene der Einrichtung für den Elektrizitätssektor im Sinne dieses Artikels, wenn sie alle in Absatz 6 aufgeführten Anforderungen erfüllen.

8. Die Krisenmanagementpläne werden in den Cybersicherheitsübungen gemäß den Artikeln 43, 44 und 45 getestet.

9. In Bezug auf Prozesse mit kritischen oder erheblichen Auswirkungen nehmen Einrichtungen mit kritischen oder erheblichen Auswirkungen ihre Krisenmanagementpläne auf Ebene der Einrichtung in ihre Pläne zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity) auf. Die Krisenmanagementpläne auf Ebene der Einrichtung müssen Folgendes umfassen:

   a. Prozesse, die von der Verfügbarkeit, Integrität und Zuverlässigkeit von IT-Diensten abhängen;

   b. alle Standorte für die Aufrechterhaltung des Geschäftsbetriebs, einschließlich der Standorte für Hardware und Software;

[95] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1
[96] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_6
[97] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e1185-1-1
[98] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_21

c. alle internen Aufgaben und Zuständigkeiten im Zusammenhang mit den Verfahren zur Aufrechterhaltung des Geschäftsbetriebs.

10. Einrichtungen mit kritischen oder erheblichen Auswirkungen aktualisieren ihre Krisenmanagementpläne auf Ebene der Einrichtung mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.

11. Die ACER aktualisiert den gemäß Absatz 1 erstellten unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplan für den Elektrizitätssektor mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.

12. Jede zuständige Behörde aktualisiert den gemäß Absatz 2 erstellten nationalen Cybersicherheitskrisenmanagementund -reaktionsplan für grenzüberschreitende Stromflüsse mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.

13. Einrichtungen mit kritischen oder erheblichen Auswirkungen testen ihre Pläne zur Aufrechterhaltung des Geschäftsbetriebs mindestens einmal alle drei Jahre oder nach größeren Änderungen in einem Prozess mit kritischen Auswirkungen. Die Ergebnisse der Tests der Pläne zur Aufrechterhaltung des Geschäftsbetriebs werden dokumentiert. Einrichtungen mit kritischen oder erheblichen Auswirkungen können den Test ihres Plans zur Aufrechterhaltung des Geschäftsbetriebs in die Cybersicherheitsübungen einbeziehen.

14. Einrichtungen mit kritischen oder erheblichen Auswirkungen aktualisieren ihren Plan zur Aufrechterhaltung des Geschäftsbetriebs immer bei Bedarf und mindestens einmal alle drei Jahre unter Berücksichtigung der Ergebnisse des Tests.

15. Werden bei einem Test Mängel im Plan zur Aufrechterhaltung des Geschäftsbetriebs festgestellt, behebt die Einrichtung mit kritischen oder erheblichen Auswirkungen diese Mängel innerhalb von 180 Kalendertagen nach dem Test und führt einen neuen Test durch, um nachzuweisen, dass die Korrekturmaßnahmen wirksam sind.

16. Kann eine Einrichtung mit kritischen oder erheblichen Auswirkungen die Mängel nicht innerhalb von 180 Kalendertagen beheben, nimmt sie die Gründe in den Bericht auf, der der für sie zuständigen Behörde gemäß Artikel 27 vorzulegen ist.

Artikel 41(1)

Innerhalb von 24 Monaten nach der Übermittlung des Berichts über die unionsweite Risikobewertung an die ACER entwickelt diese in enger Zusammenarbeit mit der ENISA, ENTSO-E, der EU-VNBO, den CS-NCA, den zuständigen Behörden, den RP-NCA, den NRB und den nationalen NIS-Behörden für das Cyberkrisenmanagement einen unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplan für den Elektrizitätssektor.

Artikel 41(10)

Einrichtungen mit kritischen oder erheblichen Auswirkungen aktualisieren ihre Krisenmanagementpläne auf Ebene der Einrichtung mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.

Artikel 41(11)

Die ACER aktualisiert den gemäß Absatz 1 erstellten unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplan für den Elektrizitätssektor mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.

Artikel 41(12)

Jede zuständige Behörde aktualisiert den gemäß Absatz 2 erstellten nationalen Cybersicherheitskrisenmanagementund -reaktionsplan für grenzüberschreitende Stromflüsse mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.

Artikel 41(13)

Einrichtungen mit kritischen oder erheblichen Auswirkungen testen ihre Pläne zur Aufrechterhaltung des Geschäftsbetriebs mindestens einmal alle drei Jahre oder nach größeren Änderungen in einem Prozess mit kritischen Auswirkungen. Die Ergebnisse der Tests der Pläne zur Aufrechterhaltung des Geschäftsbetriebs werden dokumentiert. Einrichtungen mit kritischen oder erheblichen Auswirkungen können den Test ihres Plans zur Aufrechterhaltung des Geschäftsbetriebs in die Cybersicherheitsübungen einbeziehen.

Artikel 41(14)

Einrichtungen mit kritischen oder erheblichen Auswirkungen aktualisieren ihren Plan zur Aufrechterhaltung des Geschäftsbetriebs immer bei Bedarf und mindestens einmal alle drei Jahre unter Berücksichtigung der Ergebnisse des Tests.

Artikel 41(15)

Werden bei einem Test Mängel im Plan zur Aufrechterhaltung des Geschäftsbetriebs festgestellt, behebt die Einrichtung mit kritischen oder erheblichen Auswirkungen diese Mängel innerhalb von 180 Kalendertagen nach dem Test und führt einen neuen Test durch, um nachzuweisen, dass die Korrekturmaßnahmen wirksam sind.

Artikel 41(16)

Kann eine Einrichtung mit kritischen oder erheblichen Auswirkungen die Mängel nicht innerhalb von 180 Kalendertagen beheben, nimmt sie die Gründe in den Bericht auf, der der für sie zuständigen Behörde gemäß Artikel 27 vorzulegen ist.

Artikel 41(2)

Innerhalb von 12 Monaten nach der Ausarbeitung des unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplans für den Elektrizitätssektor gemäß Absatz 1 durch die ACER erstellt jede zuständige Behörde einen nationalen Cybersicherheitskrisenmanagement- und -reaktionsplan für grenzüberschreitende Stromflüsse unter Berücksichtigung des unionsweiten Cybersicherheitskrisenmanagement und -reaktionsplans für den Elektrizitätssektor und des gemäß Artikel 10 der Verordnung (EU) 2019/941 [99] erstellten nationalen Risikovorsorgeplans. Dieser Plan muss mit dem Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gemäß Artikel 9 Absatz 4 der Richtlinie (EU) 2022/2555 [100] im Einklang stehen. Die zuständige Behörde stimmt sich mit den Einrichtungen mit kritischen oder erheblichen Auswirkungen sowie mit der RP-NCA in ihrem Mitgliedstaat ab.

Artikel 41(3)

Der gemäß Artikel 9 Absatz 4 der Richtlinie (EU) 2022/2555 [101] erforderliche nationale Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gilt als nationaler Plan für das Cybersicherheitskrisenmanagement im Sinne dieses Artikels, wenn er Bestimmungen für das Krisenmanagement und die Krisenreaktion in Bezug auf grenzüberschreitende Stromflüsse enthält.

Artikel 41(4)

Die in den Absätzen 1 und 2 aufgeführten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 [102] der Verordnung (EU) 2019/943 auch an die regionalen Koordinierungszentren delegiert werden.

Artikel 41(5)

Einrichtungen mit kritischen oder erheblichen Auswirkungen stellen sicher, dass ihre Krisenmanagementprozesse im Bereich der Cybersicherheit

a. kompatible Verfahren für die grenzüberschreitende Bewältigung von Cybersicherheitsvorfällen gemäß Artikel 6 Nummer 8 der Richtlinie (EU) 2022/2555 [103] umfassen, die förmlich in ihren Krisenmanagementpläne enthalten sind;
b. Teil der allgemeinen Krisenmanagementmaßnahmen sind.

Artikel 41(6)

Innerhalb von 12 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kri-

[99] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e928-1-1
[100] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9
[101] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9
[102] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1
[103] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_6

tischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre erstellen Einrichtungen mit kritischen oder erheblichen Auswirkungen auf Ebene der Einrichtung einen Krisenmanagementplan für Cybersicherheitskrisen, der in ihre allgemeinen Krisenmanagementpläne aufgenommen wird. Dieser Plan muss mindestens Folgendes umfassen:

a. Regeln für die Erklärung einer Krise gemäß Artikel 14 Absätze 2 und 3 der Verordnung (EU) 2019/941; [104]
b. klare Aufgaben und Zuständigkeiten für das Krisenmanagement, einschließlich der Rolle anderer relevanter Einrichtungen mit kritischen oder erheblichen Auswirkungen;
c. aktuelle Kontaktinformationen sowie Regeln für die Kommunikation und den Informationsaustausch während einer Krisensituation, einschließlich der Verbindung zu den CSIRTs.

Artikel 41(7)

Die Maßnahmen für das Krisenmanagement gemäß Artikel 21 Absatz 2 [105] Buchstabe c der Richtlinie (EU) 2022/2555 gelten als Krisenmanagementplan auf Ebene der Einrichtung für den Elektrizitätssektor im Sinne dieses Artikels, wenn sie alle in Absatz 6 aufgeführten Anforderungen erfüllen.

Artikel 41(8)

Die Krisenmanagementpläne werden in den Cybersicherheitsübungen gemäß den Artikeln 43, 44 und 45 getestet.

Artikel 41(9)

In Bezug auf Prozesse mit kritischen oder erheblichen Auswirkungen nehmen Einrichtungen mit kritischen oder erheblichen Auswirkungen ihre Krisenmanagementpläne auf Ebene der Einrichtung in ihre Pläne zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity) auf. Die Krisenmanagementpläne auf Ebene der Einrichtung müssen Folgendes umfassen:

a. Prozesse, die von der Verfügbarkeit, Integrität und Zuverlässigkeit von IT-Diensten abhängen;
b. alle Standorte für die Aufrechterhaltung des Geschäftsbetriebs, einschließlich der Standorte für Hardware und Software;
c. alle internen Aufgaben und Zuständigkeiten im Zusammenhang mit den Verfahren zur Aufrechterhaltung des Geschäftsbetriebs.

Artikel 42

[104] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#d1e1185-1-1
[105] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_21

1. Die zuständigen Behörden arbeiten mit der ENISA zusammen, um im Rahmen der Unterstützung für die Mitgliedstaaten gemäß Artikel 6 Absätze 2 und 7 der Verordnung (EU) 2019/881 [106] Frühwarnkapazitäten für die Cybersicherheit im Elektrizitätsbereich (Electricity Cybersecurity Early Alert Capabilities, ECEAC) zu entwickeln.

2. Die ECEAC müssen es der ENISA bei der Wahrnehmung der in Artikel 7 Absatz 7 der Verordnung (EU) 2019/881aufgeführten Aufgaben ermöglichen,

   a. freiwillig ausgetauschte Informationen einzuholen bei:

      i. CSIRTs, zuständigen Behörden;
      ii. den in Artikel 2 der vorliegenden Verordnung aufgeführten Einrichtungen;
      iii. jeder anderen Einrichtung, die relevante Informationen auf freiwilliger Basis weitergeben möchte;

   b. die eingeholten Informationen zu bewerten und zu klassifizieren;

   c. die Informationen zu bewerten, zu denen die ENISA Zugang hat, um Risikobedingungen für die Cybersicherheit und relevante Indikatoren für Aspekte grenzüberschreitender Stromflüsse zu ermitteln;

   d. Bedingungen und Indikatoren zu ermitteln, die häufig mit Cyberangriffen im Elektrizitätssektor korrelieren;

   e. anhand der Bewertung und Ermittlung von Risikofaktoren festzulegen, ob weitere Analysen vorzunehmen und Präventivmaßnahmen zu ergreifen sind;

   f. die zuständigen Behörden über die ermittelten Risiken und empfohlene Präventionsmaßnahmen für die betreffenden Einrichtungen zu unterrichten;

   g. alle in Artikel 2 aufgeführten relevanten Einrichtungen über die Ergebnisse der gemäß den Buchstaben b, c und d dieses Absatzes bewerteten Informationen zu unterrichten;

   h. die einschlägigen Informationen regelmäßig in den gemäß Artikel 7 Absatz 6 der Verordnung (EU) 2019/881 [107] erstellten EU-Cybersicherheitslagebericht aufnehmen;

   i. soweit möglich, aus den erhobenen Informationen anwendbare Daten abzuleiten, die darauf hindeuten, dass ein potenzieller Sicherheitsverstoß oder Cyberangriff („Kompromittierungsindikatoren“) vorliegt.

3. Die CSIRTs leiten die von der ENISA bereitgestellten Informationen im Rahmen ihrer in Artikel 11 Absatz 3 Buchstabe b der Richtlinie (EU) 2022/2555 [108] festgelegten Aufgaben unverzüglich an die betreffenden Einrichtungen weiter.

4. Die ACER überwacht die Wirksamkeit der ECEAC. Die ENISA unterstützt die ACER durch Bereitstellung aller erforderlichen Informationen gemäß Artikel 6 Absatz 2 und Artikel 7 Absatz 1 der Verordnung (EU) 2019/881. Die Analyse dieser Überwachungstätigkeit ist Teil der Überwachung gemäß Artikel 12 [109] der vorliegenden Verordnung.

Artikel 42(1)

[106] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1
[107] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1
[108] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_11
[109] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Die zuständigen Behörden arbeiten mit der ENISA zusammen, um im Rahmen der Unterstützung für die Mitgliedstaaten gemäß Artikel 6 Absätze 2 und 7 der Verordnung (EU) 2019/881 [110] Frühwarnkapazitäten für die Cybersicherheit im Elektrizitätsbereich (Electricity Cybersecurity Early Alert Capabilities, ECEAC) zu entwickeln.

Artikel 42(2)

Die ECEAC müssen es der ENISA bei der Wahrnehmung der in Artikel 7 Absatz 7 der Verordnung (EU) 2019/881aufgeführten Aufgaben ermöglichen,

a. freiwillig ausgetauschte Informationen einzuholen bei:
   i. CSIRTs, zuständigen Behörden;
   ii. den in Artikel 2 der vorliegenden Verordnung aufgeführten Einrichtungen;
   iii. jeder anderen Einrichtung, die relevante Informationen auf freiwilliger Basis weitergeben möchte;
b. die eingeholten Informationen zu bewerten und zu klassifizieren;
c. die Informationen zu bewerten, zu denen die ENISA Zugang hat, um Risikobedingungen für die Cybersicherheit und relevante Indikatoren für Aspekte grenzüberschreitender Stromflüsse zu ermitteln;
d. Bedingungen und Indikatoren zu ermitteln, die häufig mit Cyberangriffen im Elektrizitätssektor korrelieren;
e. anhand der Bewertung und Ermittlung von Risikofaktoren festzulegen, ob weitere Analysen vorzunehmen und Präventivmaßnahmen zu ergreifen sind;
f. die zuständigen Behörden über die ermittelten Risiken und empfohlene Präventionsmaßnahmen für die betreffenden Einrichtungen zu unterrichten;
g. alle in Artikel 2 aufgeführten relevanten Einrichtungen über die Ergebnisse der gemäß den Buchstaben b, c und d dieses Absatzes bewerteten Informationen zu unterrichten;
h. die einschlägigen Informationen regelmäßig in den gemäß Artikel 7 Absatz 6 der Verordnung (EU) 2019/881 [111] erstellten EU-Cybersicherheitslagebericht aufnehmen;
i. soweit möglich, aus den erhobenen Informationen anwendbare Daten abzuleiten, die darauf hindeuten, dass ein potenzieller Sicherheitsverstoß oder Cyberangriff („Kompromittierungsindikatoren“) vorliegt.

Artikel 42(3)

[110] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1
[111] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Die CSIRTs leiten die von der ENISA bereitgestellten Informationen im Rahmen ihrer in Artikel 11 Absatz 3 Buchstabe b der Richtlinie (EU) 2022/2555 [112] festgelegten Aufgaben unverzüglich an die betreffenden Einrichtungen weiter.

Artikel 42(4)

Die ACER überwacht die Wirksamkeit der ECEAC. Die ENISA unterstützt die ACER durch Bereitstellung aller erforderlichen Informationen gemäß Artikel 6 Absatz 2 und Artikel 7 Absatz 1 der Verordnung (EU) 2019/881.

Die Analyse dieser Überwachungstätigkeit ist Teil der Überwachung gemäß Artikel 12 [113] der vorliegenden Verordnung.

Artikel 43

1. Bis zum 31. Dezember des Jahres nach der Unterrichtung der Einrichtungen mit kritischen Auswirkungen und danach alle drei Jahre führt jede Einrichtung mit kritischen Auswirkungen eine Cybersicherheitsübung durch, die ein oder mehrere Szenarien mit Cyberangriffen umfasst, die sich direkt oder indirekt auf grenzüberschreitende Stromflüsse auswirken und mit den gemäß den Artikeln 20 und 27 bei den Cybersicherheitsrisikobewertungen auf Ebene der Mitgliedstaaten und Einrichtungen ermittelten Risiken im Zusammenhang stehen.
2. Abweichend von Absatz 1 kann die RP-NCA nach Konsultation der zuständigen Behörde und der gemäß Artikel 9 der Richtlinie (EU) 2022/2555 [114] benannten oder eingerichteten zuständigen Behörde für das Cyberkrisenmanagement beschließen, anstelle der Cybersicherheitsübung auf Ebene der Einrichtung eine Cybersicherheitsübung gemäß Absatz 1 auf Ebene des Mitgliedstaats durchzuführen. In diesem Zusammenhang unterrichtet die zuständige Behörde
   a. alle Einrichtungen mit kritischen Auswirkungen ihres Mitgliedstaats, die NRB, die CSIRTs und die CS-NCA bis spätestens 30. Juni des Jahres, das der Cybersicherheitsübung auf Ebene der Einrichtungen vorausgeht;
   b. jede Einrichtung, die an der Cybersicherheitsübung auf Ebene des Mitgliedstaats teilnehmen muss, spätestens sechs Monate vor der Übung.
3. Die RP-NCA organisiert mit technischer Unterstützung ihrer CSIRTs die in Absatz 2 beschriebene Cybersicherheitsübung auf Ebene des Mitgliedstaats getrennt oder zusammen mit einer anderen Cybersicherheitsübung in diesem Mitgliedstaat. Um diese Übungen zusammenfassen zu können, kann die RP-NCA die in Absatz 1 genannte Cybersicherheitsübung auf Ebene des Mitgliedstaats um ein Jahr verschieben
4. Die Cybersicherheitsübungen auf Ebene der Einrichtungen und der Mitgliedstaaten müssen mit den nationalen Rahmen für das Cybersicherheitskrisenmanagement gemäß Artikel 9 Absatz 4 Buchstabe d der Richtlinie (EU) 2022/2555 [115] im Einklang stehen.

[112] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_11
[113] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1
[114] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9
[115] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9

5. Bis zum 31 Dezember 2026 und danach alle drei Jahre stellt ENTSO-E in Zusammenarbeit mit der EU-VNBO ein Muster für das Übungsszenario für die Durchführung der in Absatz 1 genannten Cybersicherheitsübungen auf Ebene der Einrichtungen und der Mitgliedstaaten bereit. Das Muster muss den Ergebnissen der jüngsten Bewertung des Cybersicherheitsrisikos auf Ebene der Einrichtungen und der Mitgliedstaaten Rechnung tragen und zentrale Leistungskriterien enthalten. ENTSO-E und die EU-VNBO beziehen die ACER und die ENISA bei der Entwicklung dieses Musters ein.

Artikel 43(1)

Bis zum 31. Dezember des Jahres nach der Unterrichtung der Einrichtungen mit kritischen Auswirkungen und danach alle drei Jahre führt jede Einrichtung mit kritischen Auswirkungen eine Cybersicherheitsübung durch, die ein oder mehrere Szenarien mit Cyberangriffen umfasst, die sich direkt oder indirekt auf grenzüberschreitende Stromflüsse auswirken und mit den gemäß den Artikeln 20 und 27 bei den Cybersicherheitsrisikobewertungen auf Ebene der Mitgliedstaaten und Einrichtungen ermittelten Risiken im Zusammenhang stehen.

Artikel 43(2)

Abweichend von Absatz 1 kann die RP-NCA nach Konsultation der zuständigen Behörde und der gemäß Artikel 9 der Richtlinie (EU) 2022/2555 [116] benannten oder eingerichteten zuständigen Behörde für das Cyberkrisenmanagement beschließen, anstelle der Cybersicherheitsübung auf Ebene der Einrichtung eine Cybersicherheitsübung gemäß Absatz 1 auf Ebene des Mitgliedstaats durchzuführen. In diesem Zusammenhang unterrichtet die zuständige Behörde

a. alle Einrichtungen mit kritischen Auswirkungen ihres Mitgliedstaats, die NRB, die CSIRTs und die CS-NCA bis spätestens 30. Juni des Jahres, das der Cybersicherheitsübung auf Ebene der Einrichtungen vorausgeht;

b. jede Einrichtung, die an der Cybersicherheitsübung auf Ebene des Mitgliedstaats teilnehmen muss, spätestens sechs Monate vor der Übung.

Artikel 43(3)

Die RP-NCA organisiert mit technischer Unterstützung ihrer CSIRTs die in Absatz 2 beschriebene Cybersicherheitsübung auf Ebene des Mitgliedstaats getrennt oder zusammen mit einer anderen Cybersicherheitsübung in diesem Mitgliedstaat. Um diese Übungen zusammenfassen zu können, kann die RP-NCA die in Absatz 1 genannte Cybersicherheitsübung auf Ebene des Mitgliedstaats um ein Jahr verschieben

Artikel 43(4)

[116] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9

Die Cybersicherheitsübungen auf Ebene der Einrichtungen und der Mitgliedstaaten müssen mit den nationalen Rahmen für das Cybersicherheitskrisenmanagement gemäß Artikel 9 Absatz 4 Buchstabe d der Richtlinie (EU) 2022/2555 [117] im Einklang stehen.

Artikel 43(5)

Bis zum 31 Dezember 2026 und danach alle drei Jahre stellt ENTSO-E in Zusammenarbeit mit der EU-VNBO ein Muster für das Übungsszenario für die Durchführung der in Absatz 1 genannten Cybersicherheitsübungen auf Ebene der Einrichtungen und der Mitgliedstaaten bereit. Das Muster muss den Ergebnissen der jüngsten Bewertung des Cybersicherheitsrisikos auf Ebene der Einrichtungen und der Mitgliedstaaten Rechnung tragen und zentrale Leistungskriterien enthalten. ENTSO-E und die EU-VNBO beziehen die ACER und die ENISA bei der Entwicklung dieses Musters ein.

Artikel 44

1. Bis zum 31 Dezember 2029 und danach alle drei Jahre organisiert ENTSO-E in Zusammenarbeit mit der EU-VNBO in jeder Netzbetriebsregion eine regionale Cybersicherheitsübung. An der regionalen Cybersicherheitsübung nehmen die Einrichtungen mit kritischen Auswirkungen teil. ENTSO-E kann in Zusammenarbeit mit der EU-VNBO innerhalb desselben Zeitrahmens anstelle einer regionalen Cybersicherheitsübung eine überregionale Cybersicherheitsübung in mehr als einer Netzbetriebsregion organisieren. Bei der Übung sollten andere vorhandene Risikobewertungen und Szenarien für die Cybersicherheit, die auf Unionsebene entwickelt wurden, berücksichtigt werden.
2. Die ENISA unterstützt ENTSO-E und die EU-VNBO bei der Vorbereitung und Organisation der Cybersicherheitsübung auf regionaler oder überregionaler Ebene.
3. ENTSO-E unterrichtet in Abstimmung mit der EU-VNBO die Einrichtungen mit kritischen Auswirkungen, die an der regionalen oder überregionalen Cybersicherheitsübung teilnehmen müssen, sechs Monate vor der Übung.
4. Der Organisator einer regelmäßigen Cybersicherheitsübung auf Unionsebene gemäß Artikel 7 Absatz 5 der Verordnung (EU) 2019/881 [118] oder einer obligatorischen Cybersicherheitsübung in Bezug auf den Elektrizitätssektor innerhalb desselben geografischen Perimeters kann ENTSO-E und die EU-VNBO zur Teilnahme einladen. In diesen Fällen gilt die Verpflichtung nach Absatz 1 nicht, sofern alle Einrichtungen mit kritischen Auswirkungen in der Netzbetriebsregion an derselben Übung teilnehmen.
5. Nehmen ENTSO-E und die EU-VNBO an einer Cybersicherheitsübung gemäß Absatz 4 teil, so können sie die in Absatz 1 genannte regionale oder überregionale Cybersicherheitsübung um ein Jahr verschieben.
6. Bis zum 31 Dezember 2027 und danach alle drei Jahre stellt ENTSO-E in Abstimmung mit der EU-VNBO ein Muster für die Durchführung der regionalen und überregionalen Cybersicher-

[117] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_9
[118] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

heitsübungen bereit. Das Muster muss den Ergebnissen der jüngsten Bewertung des Cybersicherheitsrisikos auf regionaler Ebene Rechnung tragen und zentrale Leistungskriterien enthalten. In Bezug auf die Organisation und Durchführung der regionalen und überregionalen Cybersicherheitsübungen konsultiert ENTSO-E die Kommission und kann den Rat der ACER, der ENISA und der Gemeinsamen Forschungsstelle einholen.

Artikel 44(1)

Bis zum 31 Dezember 2029 und danach alle drei Jahre organisiert ENTSO-E in Zusammenarbeit mit der EU-VNBO in jeder Netzbetriebsregion eine regionale Cybersicherheitsübung. An der regionalen Cybersicherheitsübung nehmen die Einrichtungen mit kritischen Auswirkungen teil. ENTSO-E kann in Zusammenarbeit mit der EU-VNBO innerhalb desselben Zeitrahmens anstelle einer regionalen Cybersicherheitsübung eine überregionale Cybersicherheitsübung in mehr als einer Netzbetriebsregion organisieren. Bei der Übung sollten andere vorhandene Risikobewertungen und Szenarien für die Cybersicherheit, die auf Unionsebene entwickelt wurden, berücksichtigt werden.

Artikel 44(2)

Die ENISA unterstützt ENTSO-E und die EU-VNBO bei der Vorbereitung und Organisation der Cybersicherheitsübung auf regionaler oder überregionaler Ebene.

Artikel 44(3)

ENTSO-E unterrichtet in Abstimmung mit der EU-VNBO die Einrichtungen mit kritischen Auswirkungen, die an der regionalen oder überregionalen Cybersicherheitsübung teilnehmen müssen, sechs Monate vor der Übung.

Artikel 44(4)

Der Organisator einer regelmäßigen Cybersicherheitsübung auf Unionsebene gemäß Artikel 7 Absatz 5 der Verordnung (EU) 2019/881 [119] oder einer obligatorischen Cybersicherheitsübung in Bezug auf den Elektrizitätssektor innerhalb desselben geografischen Perimeters kann ENTSO-E und die EU-VNBO zur Teilnahme einladen. In diesen Fällen gilt die Verpflichtung nach Absatz 1 nicht, sofern alle Einrichtungen mit kritischen Auswirkungen in der Netzbetriebsregion an derselben Übung teilnehmen.

Artikel 44(5)

Nehmen ENTSO-E und die EU-VNBO an einer Cybersicherheitsübung gemäß Absatz 4 teil, so

[119] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

können sie die in Absatz 1 genannte regionale oder überregionale Cybersicherheitsübung um ein Jahr verschieben.

Artikel 44(6)

Bis zum 31 Dezember 2027 und danach alle drei Jahre stellt ENTSO-E in Abstimmung mit der EU-VNBO ein Muster für die Durchführung der regionalen und überregionalen Cybersicherheitsübungen bereit. Das Muster muss den Ergebnissen der jüngsten Bewertung des Cybersicherheitsrisikos auf regionaler Ebene Rechnung tragen und zentrale Leistungskriterien enthalten. In Bezug auf die Organisation und Durchführung der regionalen und überregionalen Cybersicherheitsübungen konsultiert ENTSO-E die Kommission und kann den Rat der ACER, der ENISA und der Gemeinsamen Forschungsstelle einholen.

Artikel 45

1. Auf Ersuchen einer Einrichtung mit kritischen Auswirkungen nehmen die Anbieter kritischer Dienste an den in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen teil, wenn sie Dienste für die Einrichtung mit kritischen Auswirkungen in dem Bereich erbringen, der dem Anwendungsbereich der betreffenden Cybersicherheitsübung entspricht.
2. Die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen analysieren und beenden die einschlägigen Cybersicherheitsübungen mit einem an alle Teilnehmer gerichteten Bericht, in dem die gewonnenen Erkenntnisse zusammengefasst werden, wobei sie bei der ENISA gemäß Artikel 7 Absatz 5 der Verordnung (EU) 2019/881 [120] Rat einholen können. Der Bericht muss Folgendes enthalten:
   a. die Übungsszenarien, Sitzungsberichte, wichtigsten Standpunkte, Erfolge und Erkenntnisse auf allen Ebenen der Elektrizitätswertschöpfungskette;
   b. die Angabe, ob die wichtigsten Leistungskriterien erfüllt wurden;
   c. eine Liste von Empfehlungen für Einrichtungen, die an der einschlägigen Cybersicherheitsübung teilnehmen, in Bezug auf eine Korrektur, Anpassung oder Änderung von cybersicherheitskrisenprozessen, -verfahren, zugehörigen Governance-Modellen und etwaigen bestehenden vertraglichen Verpflichtungen mit Anbietern kritischer Dienste.
3. Auf Ersuchen des CSIRTs-Netzes, der NIS-Kooperationsgruppe oder des EU-CyCLONe leiten die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen die Ergebnisse der einschlägigen Cybersicherheitsübung weiter. Die Organisatoren teilen jeder an den Übungen teilnehmenden Einrichtung die in Absatz 2 Buchstaben a und b dieses Artikels genannten Informationen mit. Die Organisatoren übermitteln die Liste der in Absatz 2 Buchstabe c genannten Empfehlungen ausschließlich an die Einrichtungen, an die sich die Empfehlungen richten.
4. Die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen treffen mit den an den Übungen teilnehmenden Einrichtungen regelmäßig

[120] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Folgemaßnahmen in Bezug auf die Umsetzung der Empfehlungen gemäß Absatz 2 Buchstabe c des vorliegenden Artikels.

Artikel 45(1)

Auf Ersuchen einer Einrichtung mit kritischen Auswirkungen nehmen die Anbieter kritischer Dienste an den in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen teil, wenn sie Dienste für die Einrichtung mit kritischen Auswirkungen in dem Bereich erbringen, der dem Anwendungsbereich der betreffenden Cybersicherheitsübung entspricht.

Artikel 45(2)

Die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen analysieren und beenden die einschlägigen Cybersicherheitsübungen mit einem an alle Teilnehmer gerichteten Bericht, in dem die gewonnenen Erkenntnisse zusammengefasst werden, wobei sie bei der ENISA gemäß Artikel 7 Absatz 5 der Verordnung (EU) 2019/881 [121] Rat einholen können. Der Bericht muss Folgendes enthalten:

a. die Übungsszenarien, Sitzungsberichte, wichtigsten Standpunkte, Erfolge und Erkenntnisse auf allen Ebenen der Elektrizitätswertschöpfungskette;
b. die Angabe, ob die wichtigsten Leistungskriterien erfüllt wurden;
c. eine Liste von Empfehlungen für Einrichtungen, die an der einschlägigen Cybersicherheitsübung teilnehmen, in Bezug auf eine Korrektur, Anpassung oder Änderung von cybersicherheitskrisenprozessen, -verfahren, zugehörigen Governance-Modellen und etwaigen bestehenden vertraglichen Verpflichtungen mit Anbietern kritischer Dienste.

Artikel 45(3)

Auf Ersuchen des CSIRTs-Netzes, der NIS-Kooperationsgruppe oder des EU-CyCLONe leiten die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen die Ergebnisse der einschlägigen Cybersicherheitsübung weiter. Die Organisatoren teilen jeder an den Übungen teilnehmenden Einrichtung die in Absatz 2 Buchstaben a und b dieses Artikels genannten Informationen mit. Die Organisatoren übermitteln die Liste der in Absatz 2 Buchstabe c genannten Empfehlungen ausschließlich an die Einrichtungen, an die sich die Empfehlungen richten.

Artikel 45(4)

Die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen treffen mit den an den Übungen teilnehmenden Einrichtungen regelmäßig

[121] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Folgemaßnahmen in Bezug auf die Umsetzung der Empfehlungen gemäß Absatz 2 Buchstabe c des vorliegenden Artikels.

Artikel 46

1. Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass die im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen nur nach dem Grundsatz „Kenntnis nur, wenn nötig" und im Einklang mit den einschlägigen Vorschriften der Union und der Mitgliedstaaten über die Informationssicherheit zugänglich sind.

2. Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass die im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen während des gesamten Lebenszyklus dieser Informationen entsprechend behandelt und nachverfolgt werden und dass sie am Ende ihres Lebenszyklus erst dann freigegeben werden, wenn sie anonymisiert wurden.

3. Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass alle erforderlichen Schutzmaßnahmen organisatorischer und technischer Art getroffen werden, um die Vertraulichkeit, Integrität, Verfügbarkeit und Nichtabstreitbarkeit der im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen, unabhängig von den dabei genutzten Mitteln, zu wahren und zu schützen. Die Schutzmaßnahmen müssen

   a. verhältnismäßig sein;

   b. Cybersicherheitsrisiken im Zusammenhang mit bekannten früheren und sich abzeichnenden Bedrohungen Rechnung tragen, denen die Informationen im Zusammenhang mit dieser Verordnung ausgesetzt sein könnten;

   c. soweit möglich auf nationalen, europäischen oder internationalen Normen und bewährten Verfahren beruhen;

   d. dokumentiert werden.

4. Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass jede Person, der Zugang zu den im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen gewährt wird, über die auf Ebene der Einrichtungen geltenden Sicherheitsvorschriften sowie über die für den Schutz von Informationen relevanten Maßnahmen und Verfahren unterrichtet wird. Die Einrichtungen stellen sicher, dass die betroffene Person die Zuständigkeit anerkennt, die Informationen nach den in der Unterrichtung erteilten Anweisungen zu schützen.

5. Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass der Zugang zu den im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen auf Personen beschränkt wird,

   a. die aufgrund ihrer Funktionen, und beschränkt auf die Ausführung der ihnen übertragenen Aufgaben, zum Zugang zu diesen Informationen berechtigt sind;

b. in Bezug auf die die Einrichtung ethische Grundsätze und Integritätsgrundsätze prüfen konnte und für die es keine Hinweise auf ein negatives Ergebnis einer Zuverlässigkeitsüberprüfung gibt, mit der die Zuverlässigkeit der Person im Einklang mit bewährten Verfahren und den Standardsicherheitsanforderungen der Einrichtung und erforderlichenfalls mit den nationalen Gesetzen und Vorschriften bewertet wurde.

6. Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen bedürfen der schriftlichen Zustimmung der natürlichen oder juristischen Person, die die Informationen ursprünglich erstellt oder bereitgestellt hat, bevor sie diese Informationen an Dritte weitergeben, die nicht in den Anwendungsbereich dieser Verordnung fallen.

7. Eine in Artikel 2 Absatz 1 aufgeführte Einrichtung kann der Ansicht sein, dass diese Informationen ohne Einhaltung der Absätze 1 und 4 des vorliegenden Artikels weitergegeben werden müssen, um eine zeitgleich auftretende Stromversorgungskrise mit einer zugrunde liegenden Cybersicherheitsursache oder eine grenzüberschreitende Krise innerhalb der Union in einem anderen Sektor zu verhindern. In diesem Fall

   a. konsultiert sie die zuständige Behörde und kann von ihr zur Weitergabe dieser Informationen ermächtigt werden;

   b. anonymisiert sie diese Informationen, ohne dass die Elemente verloren gehen, die erforderlich sind, um die Öffentlichkeit über ein unmittelbares und ernstes Risiko für grenzüberschreitende Stromflüsse und mögliche Abhilfemaßnahmen zu informieren;

   c. schützt sie die Identität des Urhebers und der Einrichtungen, die diese Informationen im Rahmen dieser Verordnung verarbeitet haben.

8. Abweichend von Absatz 6 des vorliegenden Artikels können die zuständigen Behörden Informationen, die im Rahmen dieser Verordnung bereitgestellt, empfangen, ausgetauscht oder übermittelt werden, einem nicht in Artikel 2 Absatz 1 aufgeführten Dritten bereitstellen, ohne dass der Urheber der Informationen schriftlich zugestimmt hat, müssen diesen jedoch so bald wie möglich davon in Kenntnis setzen. Bevor die betreffende zuständige Behörde Informationen, die im Rahmen dieser Verordnung bereitgestellt, empfangen, ausgetauscht oder übermittelt wurden, einem nicht in Artikel 2 Absatz 1 aufgeführten Dritten offenlegt, muss sie in angemessenem Umfang sicherstellen, dass der betreffende Dritte Kenntnis von den geltenden Sicherheitsvorschriften hat, und hinreichende Gewähr dafür erhalten, dass der betreffende Dritte die empfangenen Informationen gemäß den Absätzen 1 bis 5 des vorliegenden Artikels schützen kann. Die zuständige Behörde anonymisiert diese Informationen, ohne dass die Elemente verloren gehen, die erforderlich sind, um die Öffentlichkeit über ein unmittelbares und ernstes Risiko für grenzüberschreitende Stromflüsse und mögliche Abhilfemaßnahmen zu informieren, und schützt die Identität des Urhebers der Informationen. In diesem Fall schützt der nicht in Artikel 2 Absatz 1 aufgeführte Dritte die empfangenen Informationen gemäß den auf Ebene der Einrichtung bereits geltenden Bestimmungen oder, wenn dies nicht möglich ist, nach den Bestimmungen und Anweisungen der jeweils zuständigen Behörde.

9. Dieser Artikel gilt nicht für Einrichtungen, die nicht in Artikel 2 Absatz 1 aufgeführt sind, wenn sie Informationen gemäß Absatz 6 des vorliegenden Artikels erhalten. In diesem Fall ist Absatz 7 anzuwenden, oder die zuständige Behörde kann dieser Einrichtung schriftliche Bestimmungen bereitstellen, die in Fällen anzuwenden sind, in denen Informationen gemäß dieser Verordnung eingehen.

Artikel 46(1)

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass die im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen nur nach dem Grundsatz „Kenntnis nur, wenn nötig“ und im Einklang mit den einschlägigen Vorschriften der Union und der Mitgliedstaaten über die Informationssicherheit zugänglich sind.

Artikel 46(2)

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass die im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen während des gesamten Lebenszyklus dieser Informationen entsprechend behandelt und nachverfolgt werden und dass sie am Ende ihres Lebenszyklus erst dann freigegeben werden, wenn sie anonymisiert wurden.

Artikel 46(3)

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass alle erforderlichen Schutzmaßnahmen organisatorischer und technischer Art getroffen werden, um die Vertraulichkeit, Integrität, Verfügbarkeit und Nichtabstreitbarkeit der im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen, unabhängig von den dabei genutzten Mitteln, zu wahren und zu schützen. Die Schutzmaßnahmen müssen

a. verhältnismäßig sein;

b. Cybersicherheitsrisiken im Zusammenhang mit bekannten früheren und sich abzeichnenden Bedrohungen Rechnung tragen, denen die Informationen im Zusammenhang mit dieser Verordnung ausgesetzt sein könnten;

c. soweit möglich auf nationalen, europäischen oder internationalen Normen und bewährten Verfahren beruhen;

d. dokumentiert werden.

Artikel 46(4)

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass jede Person, der Zugang zu den im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen gewährt wird, über die auf Ebene der Einrichtungen geltenden Sicherheitsvorschriften sowie über die für den Schutz von Informationen relevanten Maßnahmen und Verfahren unterrichtet wird. Die Einrichtungen stellen sicher, dass die betroffene Person die Zuständigkeit anerkennt, die Informationen nach den in der Unterrichtung erteilten Anweisungen zu schützen.

Artikel 46(5)

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass der Zugang zu den im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen auf Personen beschränkt wird,

a. die aufgrund ihrer Funktionen, und beschränkt auf die Ausführung der ihnen übertragenen Aufgaben, zum Zugang zu diesen Informationen berechtigt sind;

b. in Bezug auf die die Einrichtung ethische Grundsätze und Integritätsgrundsätze prüfen konnte und für die es keine Hinweise auf ein negatives Ergebnis einer Zuverlässigkeitsüberprüfung gibt, mit der die Zuverlässigkeit der Person im Einklang mit bewährten Verfahren und den Standardsicherheitsanforderungen der Einrichtung und erforderlichenfalls mit den nationalen Gesetzen und Vorschriften bewertet wurde.

Artikel 46(6)

Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen bedürfen der schriftlichen Zustimmung der natürlichen oder juristischen Person, die die Informationen ursprünglich erstellt oder bereitgestellt hat, bevor sie diese Informationen an Dritte weitergeben, die nicht in den Anwendungsbereich dieser Verordnung fallen.

Artikel 46(7)

Eine in Artikel 2 Absatz 1 aufgeführte Einrichtung kann der Ansicht sein, dass diese Informationen ohne Einhaltung der Absätze 1 und 4 des vorliegenden Artikels weitergegeben werden müssen, um eine zeitgleich auftretende Stromversorgungskrise mit einer zugrunde liegenden Cybersicherheitsursache oder eine grenzüberschreitende Krise innerhalb der Union in einem anderen Sektor zu verhindern. In diesem Fall

a. konsultiert sie die zuständige Behörde und kann von ihr zur Weitergabe dieser Informationen ermächtigt werden;

b. anonymisiert sie diese Informationen, ohne dass die Elemente verloren gehen, die erforderlich sind, um die Öffentlichkeit über ein unmittelbares und ernstes Risiko für grenzüberschreitende Stromflüsse und mögliche Abhilfemaßnahmen zu informieren;

c. schützt sie die Identität des Urhebers und der Einrichtungen, die diese Informationen im Rahmen dieser Verordnung verarbeitet haben.

Artikel 46(8)

Abweichend von Absatz 6 des vorliegenden Artikels können die zuständigen Behörden Informationen, die im Rahmen dieser Verordnung bereitgestellt, empfangen, ausgetauscht oder über-

mittelt werden, einem nicht in Artikel 2 Absatz 1 aufgeführten Dritten bereitstellen, ohne dass der Urheber der Informationen schriftlich zugestimmt hat, müssen diesen jedoch so bald wie möglich davon in Kenntnis setzen. Bevor die betreffende zuständige Behörde Informationen, die im Rahmen dieser Verordnung bereitgestellt, empfangen, ausgetauscht oder übermittelt wurden, einem nicht in Artikel 2 Absatz 1 aufgeführten Dritten offenlegt, muss sie in angemessenem Umfang sicherstellen, dass der betreffende Dritte Kenntnis von den geltenden Sicherheitsvorschriften hat, und hinreichende Gewähr dafür erhalten, dass der betreffende Dritte die empfangenen Informationen gemäß den Absätzen 1 bis 5 des vorliegenden Artikels schützen kann. Die zuständige Behörde anonymisiert diese Informationen, ohne dass die Elemente verloren gehen, die erforderlich sind, um die Öffentlichkeit über ein unmittelbares und ernstes Risiko für grenzüberschreitende Stromflüsse und mögliche Abhilfemaßnahmen zu informieren, und schützt die Identität des Urhebers der Informationen. In diesem Fall schützt der nicht in Artikel 2 Absatz 1 aufgeführte Dritte die empfangenen Informationen gemäß den auf Ebene der Einrichtung bereits geltenden Bestimmungen oder, wenn dies nicht möglich ist, nach den Bestimmungen und Anweisungen der jeweils zuständigen Behörde.

Artikel 46(9)

Dieser Artikel gilt nicht für Einrichtungen, die nicht in Artikel 2 Absatz 1 aufgeführt sind, wenn sie Informationen gemäß Absatz 6 des vorliegenden Artikels erhalten. In diesem Fall ist Absatz 7 anzuwenden, oder die zuständige Behörde kann dieser Einrichtung schriftliche Bestimmungen bereitstellen, die in Fällen anzuwenden sind, in denen Informationen gemäß dieser Verordnung eingehen.

Artikel 47

1. Alle gemäß dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen unterliegen dem Berufsgeheimnis gemäß den Absätzen 2 bis 5 dieses Artikels sowie den Anforderungen aus Artikel 65 der Verordnung (EU) 2019/943. [122] Alle von den in Artikel 2 dieser Verordnung aufgeführten Einrichtungen für die Zwecke der Durchführung dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen werden unter Berücksichtigung des vom Urheber angewandten Vertraulichkeitsgrads der Informationen geschützt.
2. Die in Artikel 2 aufgeführten Einrichtungen unterliegen der Verpflichtung zur Wahrung des Berufsgeheimnisses.
3. Die CS-NCAs, die NRB, die RP-NCA und die CSIRTs tauschen alle für die Wahrnehmung ihrer Aufgaben erforderlichen Informationen aus.
4. Alle von den in Artikel 2 Absatz 1 aufgeführten Einrichtungen für die Zwecke der Durchführung von Artikel 23 empfangenen, ausgetauschten oder übermittelten Informationen werden anonymisiert und aggregiert.
5. Informationen, die eine dieser Verordnung unterliegende Einrichtung oder Behörde im Rahmen der Erfüllung ihrer Pflichten erhält, dürfen an keine andere Einrichtung oder Behörde

[122] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e5115-54-1

weitergegeben werden; davon unberührt bleiben Fälle, die unter das nationale Recht, andere Bestimmungen dieser Verordnung oder andere einschlägige Unionsvorschriften fallen.

6. Unbeschadet des nationalen Rechts und des Unionsrechts dürfen Behörden, Einrichtungen oder natürliche Personen, die Informationen gemäß dieser Verordnung erhalten, diese für keinen anderen Zweck als für die Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung verwenden.

7. Die ACER gibt nach Konsultation der ENISA, aller zuständigen Behörden, von ENTSO-E und der EU-VNBO bis zum 13 Juni 2025 Leitlinien für alle in Artikel 2 Absatz 1 aufgeführten Einrichtungen zu Mechanismen für den Austausch von Informationen und insbesondere zu den geplanten Kommunikationsflüssen und Methoden zur Anonymisierung und Aggregierung von Informationen für die Zwecke der Durchführung des vorliegenden Artikels heraus.

8. Nach nationalem Recht oder Unionsrecht vertrauliche Informationen werden nur dann mit der Kommission und anderen zuständigen Behörden ausgetauscht, wenn ein solcher Austausch für die Anwendung dieser Verordnung erforderlich ist. Die auszutauschenden Informationen werden auf den für den Zweck dieses Informationsaustauschs erforderlichen und verhältnismäßigen Umfang beschränkt. Beim Informationsaustausch wird die Vertraulichkeit der Informationen gewahrt und die Sicherheit sowie die geschäftlichen Interessen von Einrichtungen mit kritischen oder erheblichen Auswirkungen werden geschützt.

Artikel 47(1)

Alle gemäß dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen unterliegen dem Berufsgeheimnis gemäß den Absätzen 2 bis 5 dieses Artikels sowie den Anforderungen aus Artikel 65 der Verordnung (EU) 2019/943. [123] Alle von den in Artikel 2 dieser Verordnung aufgeführten Einrichtungen für die Zwecke der Durchführung dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen werden unter Berücksichtigung des vom Urheber angewandten Vertraulichkeitsgrads der Informationen geschützt.

Artikel 47(2)

Die in Artikel 2 aufgeführten Einrichtungen unterliegen der Verpflichtung zur Wahrung des Berufsgeheimnisses.

Artikel 47(3)

Die CS-NCAs, die NRB, die RP-NCA und die CSIRTs tauschen alle für die Wahrnehmung ihrer Aufgaben erforderlichen Informationen aus.

Artikel 47(4)

[123] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943#d1e5115-54-1

Alle von den in Artikel 2 Absatz 1 aufgeführten Einrichtungen für die Zwecke der Durchführung von Artikel 23 empfangenen, ausgetauschten oder übermittelten Informationen werden anonymisiert und aggregiert.

Artikel 47(5)

Informationen, die eine dieser Verordnung unterliegende Einrichtung oder Behörde im Rahmen der Erfüllung ihrer Pflichten erhält, dürfen an keine andere Einrichtung oder Behörde weitergegeben werden; davon unberührt bleiben Fälle, die unter das nationale Recht, andere Bestimmungen dieser Verordnung oder andere einschlägige Unionsvorschriften fallen.

Artikel 47(6)

Unbeschadet des nationalen Rechts und des Unionsrechts dürfen Behörden, Einrichtungen oder natürliche Personen, die Informationen gemäß dieser Verordnung erhalten, diese für keinen anderen Zweck als für die Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung verwenden.

Artikel 47(7)

Die ACER gibt nach Konsultation der ENISA, aller zuständigen Behörden, von ENTSO-E und der EU-VNBO bis zum 13 Juni 2025 Leitlinien für alle in Artikel 2 Absatz 1 aufgeführten Einrichtungen zu Mechanismen für den Austausch von Informationen und insbesondere zu den geplanten Kommunikationsflüssen und Methoden zur Anonymisierung und Aggregierung von Informationen für die Zwecke der Durchführung des vorliegenden Artikels heraus.

Artikel 47(8)

Nach nationalem Recht oder Unionsrecht vertrauliche Informationen werden nur dann mit der Kommission und anderen zuständigen Behörden ausgetauscht, wenn ein solcher Austausch für die Anwendung dieser Verordnung erforderlich ist. Die auszutauschenden Informationen werden auf den für den Zweck dieses Informationsaustauschs erforderlichen und verhältnismäßigen Umfang beschränkt. Beim Informationsaustausch wird die Vertraulichkeit der Informationen gewahrt und die Sicherheit sowie die geschäftlichen Interessen von Einrichtungen mit kritischen oder erheblichen Auswirkungen werden geschützt.

Artikel 48

1. Bis zur Genehmigung der Modalitäten oder Methoden gemäß Artikel 6 Absatz 2 oder der Pläne gemäß Artikel 6 Absatz 3 erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO unverbindliche Leitlinien zu folgenden Themen:

   a. einem vorläufigen Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssek-

tor (im Folgenden „ECII“) gemäß Absatz 2;

b. einer vorläufigen Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen gemäß Absatz 4 sowie

c. einer vorläufigen Liste europäischer und internationaler Normen und Kontrollen gemäß Absatz 6, die nach nationalen Rechtsvorschriften erforderlich und für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.

2. Bis zum 13 Oktober 2024 erarbeitet ENTSO-E in Zusammenarbeit mit der EU-VNBO eine Empfehlung für einen vorläufigen ECII. ENTSO-E teilt den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO den empfohlenen vorläufigen ECII mit.

3. Vier Monate nach Erhalt des empfohlenen vorläufigen ECII oder bis spätestens 13 Februar 2025 ermitteln die zuständigen Behörden auf der Grundlage des empfohlenen ECII Einrichtungen, die als Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat in Betracht kommen, und erstellen eine vorläufige Liste von Einrichtungen mit erheblichen oder kritischen Auswirkungen. Die in der vorläufigen Liste aufgeführten Einrichtungen mit erheblichen oder kritischen Auswirkungen können ihren in dieser Verordnung festgelegten Verpflichtungen nach dem Vorsorgeprinzip freiwillig nachkommen. Bis zum 13 März 2025 teilen die zuständigen Behörden den in der vorläufigen Liste aufgeführten Einrichtungen mit, dass sie als Einrichtung mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

4. Bis zum 13 Dezember 2024 erarbeitet ENTSO-E in Zusammenarbeit mit der EU-VNBO eine vorläufige Liste von unionsweiten Prozessen mit erheblichen oder kritischen Auswirkungen. Die gemäß Absatz 3 unterrichteten Einrichtungen, die freiwillig beschließen, ihre in dieser Verordnung festgelegten Verpflichtungen nach dem Vorsorgeprinzip zu erfüllen, nutzen die vorläufige Liste von unionsweiten Prozessen mit erheblichen oder kritischen Auswirkungen, um vorläufige Perimeter mit erheblichen oder kritischen Auswirkungen zu bestimmen und um zu ermitteln, welche Vermögenswerte in die erste Bewertung des Cybersicherheitsrisikos auf Ebene der Einrichtung einzubeziehen sind.

5. Bis zum 13 September 2024 übermittelt jede gemäß Artikel 4 Absatz 1 zuständige Behörde ENTSO-E und der EU-VNBO eine Liste ihrer nationalen Rechtsvorschriften, die für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.

6. Bis zum 13 Juni 2025 erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO unter Berücksichtigung der von den zuständigen Behörden bereitgestellten Informationen eine vorläufige Liste der nach nationalem Recht vorgeschriebenen europäischen und internationalen Normen und Kontrollen, die für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.

7. Die vorläufige Liste der europäischen und internationalen Normen und Kontrollen muss Folgendes enthalten:

a. europäische und internationale Normen und nationale Rechtsvorschriften, die Leitlinien für Methoden für das Risikomanagement im Bereich der Cybersicherheit auf Ebene der Einrichtungen enthalten, und

b. Cybersicherheitskontrollen, die denjenigen gleichwertig sind, die voraussichtlich Teil der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen sein werden.

8. ENTSO-E und die EU-VNBO berücksichtigen bei der Fertigstellung der vorläufigen Liste von Normen die Stellungnahmen der ENISA und der ACER. ENTSO-E und die EU-VNBO veröffentlichen die vorläufige Liste der europäischen und internationalen Normen und Kontrollen auf ihren Websites.
9. ENTSO-E und die EU-VNBO konsultieren die ENISA und die ACER zu den gemäß Absatz 1 erstellten Vorschlägen für unverbindliche Leitlinien.
10. Bis die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen gemäß Artikel 29 entwickelt und gemäß Artikel 8 angenommen sind, bemühen sich alle in Artikel 2 Absatz 1 aufgeführten Einrichtungen, die gemäß Absatz 1 des vorliegenden Artikels erstellten unverbindlichen Leitlinien nach und nach anzuwenden.

Artikel 48(1)

Bis zur Genehmigung der Modalitäten oder Methoden gemäß Artikel 6 Absatz 2 oder der Pläne gemäß Artikel 6 Absatz 3 erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO unverbindliche Leitlinien zu folgenden Themen:

a. einem vorläufigen Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor (im Folgenden „ECII“) gemäß Absatz 2;
b. einer vorläufigen Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen gemäß Absatz 4 sowie
c. einer vorläufigen Liste europäischer und internationaler Normen und Kontrollen gemäß Absatz 6, die nach nationalen Rechtsvorschriften erforderlich und für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.

Artikel 48(10)

Bis die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen gemäß Artikel 29 entwickelt und gemäß Artikel 8 angenommen sind, bemühen sich alle in Artikel 2 Absatz 1 aufgeführten Einrichtungen, die gemäß Absatz 1 des vorliegenden Artikels erstellten unverbindlichen Leitlinien nach und nach anzuwenden.

Artikel 48(2)

Bis zum 13 Oktober 2024 erarbeitet ENTSO-E in Zusammenarbeit mit der EU-VNBO eine Empfehlung für einen vorläufigen ECII. ENTSO-E teilt den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO den empfohlenen vorläufigen ECII mit.

Artikel 48(3)

Vier Monate nach Erhalt des empfohlenen vorläufigen ECII oder bis spätestens 13 Februar 2025 ermitteln die zuständigen Behörden auf der Grundlage des empfohlenen ECII Einrichtungen, die als Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat in Betracht kommen, und erstellen eine vorläufige Liste von Einrichtungen mit erheblichen oder kritischen Auswirkungen.

Die in der vorläufigen Liste aufgeführten Einrichtungen mit erheblichen oder kritischen Auswirkungen können ihren in dieser Verordnung festgelegten Verpflichtungen nach dem Vorsorgeprinzip freiwillig nachkommen. Bis zum 13 März 2025 teilen die zuständigen Behörden den in der vorläufigen Liste aufgeführten Einrichtungen mit, dass sie als Einrichtung mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

Artikel 48(4)

Bis zum 13 Dezember 2024 erarbeitet ENTSO-E in Zusammenarbeit mit der EU-VNBO eine vorläufige Liste von unionsweiten Prozessen mit erheblichen oder kritischen Auswirkungen.

Die gemäß Absatz 3 unterrichteten Einrichtungen, die freiwillig beschließen, ihre in dieser Verordnung festgelegten Verpflichtungen nach dem Vorsorgeprinzip zu erfüllen, nutzen die vorläufige Liste von unionsweiten Prozessen mit erheblichen oder kritischen Auswirkungen, um vorläufige Perimeter mit erheblichen oder kritischen Auswirkungen zu bestimmen und um zu ermitteln, welche Vermögenswerte in die erste Bewertung des Cybersicherheitsrisikos auf Ebene der Einrichtung einzubeziehen sind.

Artikel 48(5)

Bis zum 13 September 2024 übermittelt jede gemäß Artikel 4 Absatz 1 zuständige Behörde ENTSO-E und der EU-VNBO eine Liste ihrer nationalen Rechtsvorschriften, die für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.

Artikel 48(6)

Bis zum 13 Juni 2025 erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO unter Berücksichtigung der von den zuständigen Behörden bereitgestellten Informationen eine vorläufige Liste der nach nationalem Recht vorgeschriebenen europäischen und internationalen Normen und Kontrollen, die für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.

Artikel 48(7)

Die vorläufige Liste der europäischen und internationalen Normen und Kontrollen muss Folgendes enthalten:

a. europäische und internationale Normen und nationale Rechtsvorschriften, die Leitlinien für Methoden für das Risikomanagement im Bereich der Cybersicherheit auf Ebene der Einrich-

tungen enthalten, und

b. Cybersicherheitskontrollen, die denjenigen gleichwertig sind, die voraussichtlich Teil der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen sein werden.

Artikel 48(8)

ENTSO-E und die EU-VNBO berücksichtigen bei der Fertigstellung der vorläufigen Liste von Normen die Stellungnahmen der ENISA und der ACER. ENTSO-E und die EU-VNBO veröffentlichen die vorläufige Liste der europäischen und internationalen Normen und Kontrollen auf ihren Websites.

Artikel 48(9)

ENTSO-E und die EU-VNBO konsultieren die ENISA und die ACER zu den gemäß Absatz 1 erstellten Vorschlägen für unverbindliche Leitlinien.

Artikel 5

Die zuständigen Behörden koordinieren und gewährleisten eine angemessene Zusammenarbeit zwischen den für Cybersicherheit zuständigen Behörden, den Behörden für das Cyberkrisenmanagement, den NRB, den für die Risikovorsorge zuständigen Behörden und den CSIRTs im Hinblick auf die Erfüllung der in dieser Verordnung festgelegten einschlägigen Verpflichtungen. Zudem stimmen sich die zuständigen Behörden mit anderen von den einzelnen Mitgliedstaaten bestimmten Stellen oder Behörden ab, um effiziente Verfahren sicherzustellen und Überschneidungen von Aufgaben und Pflichten zu vermeiden. Die zuständigen Behörden können die jeweiligen NRB anweisen, die ACER gemäß Artikel 8 Absatz 3 um eine Stellungnahme zu ersuchen.

Artikel 5

Die zuständigen Behörden koordinieren und gewährleisten eine angemessene Zusammenarbeit zwischen den für Cybersicherheit zuständigen Behörden, den Behörden für das Cyberkrisenmanagement, den NRB, den für die Risikovorsorge zuständigen Behörden und den CSIRTs im Hinblick auf die Erfüllung der in dieser Verordnung festgelegten einschlägigen Verpflichtungen. Zudem stimmen sich die zuständigen Behörden mit anderen von den einzelnen Mitgliedstaaten bestimmten Stellen oder Behörden ab, um effiziente Verfahren sicherzustellen und Überschneidungen von Aufgaben und Pflichten zu vermeiden. Die zuständigen Behörden können die jeweiligen NRB anweisen, die ACER gemäß Artikel 8 Absatz 3 um eine Stellungnahme zu ersuchen.

Artikel 6

1. Die ÜNB entwickeln in Zusammenarbeit mit der EU-VNBO Vorschläge für die Modalitäten

oder Methoden gemäß Absatz 2 bzw. für Pläne gemäß Absatz 3.

2. Die folgenden Modalitäten oder Methoden und etwaige Änderungen dieser Modalitäten oder Methoden bedürfen der Genehmigung aller zuständigen Behörden:

   a. die Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 18 Absatz 1;
   b. der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23;
   c. die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen gemäß Artikel 29, der Vergleich der Cybersicherheitskontrollen im Elektrizitätssektor anhand von Normen gemäß Artikel 34, einschließlich Mindest-Cybersicherheitskontrollen und erweiterter Cybersicherheitskontrollen in der Lieferkette gemäß Artikel 33;
   d. eine Empfehlung für die Cybersicherheit bei der Auftragsvergabe gemäß Artikel 35;
   e. die Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8.

3. Die Vorschläge für die regionalen Pläne zur Minderung des Cybersicherheitsrisikos gemäß Artikel 22 bedürfen der Genehmigung aller zuständigen Behörden der betreffenden Netzbetriebsregion.

4. Die Vorschläge für Modalitäten oder Methoden gemäß Absatz 2 bzw. für Pläne gemäß Absatz 3 müssen einen Vorschlag für den Zeitplan für ihre Umsetzung und eine Beschreibung ihrer erwarteten Auswirkungen auf die Ziele dieser Verordnung enthalten.

5. Die EU-VNBO kann den betreffenden ÜNB bis zu drei Wochen vor Ablauf der Frist für die Übermittlung des Vorschlags für Modalitäten, Methoden oder Pläne an die zuständigen Behörden eine mit Gründen versehene Stellungnahme übermitteln. Die für den Vorschlag für Modalitäten, Methoden oder Pläne zuständigen ÜNB berücksichtigen die mit Gründen versehene Stellungnahme der EU-VNBO, bevor sie den Vorschlag den zuständigen Behörden zur Genehmigung vorlegen. Wenn die ÜNB die Stellungnahme der EU-VNBO nicht berücksichtigen, begründen sie dies.

6. Bei der gemeinsamen Entwicklung von Modalitäten, Methoden und Plänen arbeiten die teilnehmenden ÜNB eng zusammen. Die ÜNB unterrichten die zuständigen Behörden und die ACER mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO regelmäßig über die Fortschritte bei der Entwicklung der Modalitäten, Methoden oder Pläne.

Artikel 6(1)

Die ÜNB entwickeln in Zusammenarbeit mit der EU-VNBO Vorschläge für die Modalitäten oder Methoden gemäß Absatz 2 bzw. für Pläne gemäß Absatz 3.

Artikel 6(2)

Die folgenden Modalitäten oder Methoden und etwaige Änderungen dieser Modalitäten oder Methoden bedürfen der Genehmigung aller zuständigen Behörden:

a. die Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 18 Absatz 1;

b. der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23;

c. die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen gemäß Artikel 29, der Vergleich der Cybersicherheitskontrollen im Elektrizitätssektor anhand von Normen gemäß Artikel 34, einschließlich Mindest-Cybersicherheitskontrollen und erweiterter Cybersicherheitskontrollen in der Lieferkette gemäß Artikel 33;

d. eine Empfehlung für die Cybersicherheit bei der Auftragsvergabe gemäß Artikel 35;

e. die Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8.

Artikel 6(3)

Die Vorschläge für die regionalen Pläne zur Minderung des Cybersicherheitsrisikos gemäß Artikel 22 bedürfen der Genehmigung aller zuständigen Behörden der betreffenden Netzbetriebsregion.

Artikel 6(4)

Die Vorschläge für Modalitäten oder Methoden gemäß Absatz 2 bzw. für Pläne gemäß Absatz 3 müssen einen Vorschlag für den Zeitplan für ihre Umsetzung und eine Beschreibung ihrer erwarteten Auswirkungen auf die Ziele dieser Verordnung enthalten.

Artikel 6(5)

Die EU-VNBO kann den betreffenden ÜNB bis zu drei Wochen vor Ablauf der Frist für die Übermittlung des Vorschlags für Modalitäten, Methoden oder Pläne an die zuständigen Behörden eine mit Gründen versehene Stellungnahme übermitteln.

Die für den Vorschlag für Modalitäten, Methoden oder Pläne zuständigen ÜNB berücksichtigen die mit Gründen versehene Stellungnahme der EU-VNBO, bevor sie den Vorschlag den zuständigen Behörden zur Genehmigung vorlegen. Wenn die ÜNB die Stellungnahme der EU-VNBO nicht berücksichtigen, begründen sie dies.

Artikel 6(6)

Bei der gemeinsamen Entwicklung von Modalitäten, Methoden und Plänen arbeiten die teilnehmenden ÜNB eng zusammen. Die ÜNB unterrichten die zuständigen Behörden und die ACER mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO regelmäßig über die Fortschritte bei der Entwicklung der Modalitäten, Methoden oder Pläne.

Artikel 7

1. Können ÜNB bei der Entscheidung über Vorschläge für Modalitäten oder Methoden keine Einigung erzielen, so entscheiden sie mit qualifizierter Mehrheit. Die qualifizierte Mehrheit für diese Vorschläge wird wie folgt berechnet:

   a. ÜNB, die mindestens 55 % der Mitgliedstaaten vertreten, und

   b. ÜNB, die Mitgliedstaaten vertreten, die mindestens 65 % der Bevölkerung der Union umfassen.

2. Eine Sperrminorität bei Entscheidungen über Vorschläge für in Artikel 6 Absatz 2 aufgeführte Modalitäten oder Methoden ist mit ÜNB erreicht, die mindestens vier Mitgliedstaaten vertreten; andernfalls gilt die qualifizierte Mehrheit als erreicht.

3. Können ÜNB einer Netzbetriebsregion bei der Entscheidung über Vorschläge für die in Artikel 6 Absatz 2 genannten Pläne keine Einigung erzielen und besteht die betreffende Netzbetriebsregion aus mehr als fünf Mitgliedstaaten, so entscheiden die ÜNB mit qualifizierter Mehrheit. Bei Vorschlägen gemäß Artikel 6 Absatz 2 ist für eine qualifizierte Mehrheit folgende Mehrheit erforderlich:

   a. ÜNB, die mindestens 72 % der betroffenen Mitgliedstaaten vertreten, und

   b. ÜNB, die Mitgliedstaaten vertreten, die mindestens 65 % der Bevölkerung der betroffenen Region umfassen.

4. Eine Sperrminorität für Entscheidungen über Vorschläge für die Pläne muss eine Mindestanzahl von ÜNB umfassen, die mehr als 35 % der Bevölkerung der teilnehmenden Mitgliedstaaten vertreten, zuzüglich ÜNB, die mindestens einen weiteren betroffenen Mitgliedstaat vertreten; ansonsten gilt die qualifizierte Mehrheit als erreicht.

5. Bei Entscheidungen der ÜNB über Vorschläge für in Artikel 6 Absatz 2 aufgeführte Modalitäten oder Methoden erhält jeder Mitgliedstaat eine Stimme. Gibt es im Hoheitsgebiet eines Mitgliedstaats mehr als einen ÜNB, teilt der Mitgliedstaat die Stimmrechte unter den ÜNB auf.

6. Legen ÜNB den jeweils zuständigen Behörden nicht innerhalb der in dieser Verordnung festgelegten Fristen in Zusammenarbeit mit der EU-VNBO einen ersten oder geänderten Vorschlag für Modalitäten oder Methoden oder für Pläne vor, so übermitteln sie den jeweils zuständigen Behörden und der ACER entsprechende Entwürfe der Modalitäten oder Methoden bzw. der Pläne. Sie erläutern, warum keine Einigung erzielt wurde. Die zuständigen Behörden treffen gemeinsam geeignete Maßnahmen für die Annahme der erforderlichen Modalitäten oder Methoden bzw. der erforderlichen Pläne. Dies kann z. B. durch Ersuchen um Änderungen der Entwürfe gemäß diesem Absatz, durch Überarbeitung und Vervollständigung dieser Entwürfe oder, falls keine Entwürfe vorgelegt wurden, durch Festlegung und Genehmigung der erforderlichen Modalitäten, Methoden oder Pläne erfolgen.

Artikel 7(1)

Können ÜNB bei der Entscheidung über Vorschläge für Modalitäten oder Methoden keine Einigung erzielen, so entscheiden sie mit qualifizierter Mehrheit. Die qualifizierte Mehrheit für diese Vorschläge wird wie folgt berechnet:

a. ÜNB, die mindestens 55 % der Mitgliedstaaten vertreten, und

b. ÜNB, die Mitgliedstaaten vertreten, die mindestens 65 % der Bevölkerung der Union umfassen.

Artikel 7(2)

Eine Sperrminorität bei Entscheidungen über Vorschläge für in Artikel 6 Absatz 2 aufgeführte Modalitäten oder Methoden ist mit ÜNB erreicht, die mindestens vier Mitgliedstaaten vertreten; andernfalls gilt die qualifizierte Mehrheit als erreicht.

Artikel 7(3)

Können ÜNB einer Netzbetriebsregion bei der Entscheidung über Vorschläge für die in Artikel 6 Absatz 2 genannten Pläne keine Einigung erzielen und besteht die betreffende Netzbetriebsregion aus mehr als fünf Mitgliedstaaten, so entscheiden die ÜNB mit qualifizierter Mehrheit. Bei Vorschlägen gemäß Artikel 6 Absatz 2 ist für eine qualifizierte Mehrheit folgende Mehrheit erforderlich:

a. ÜNB, die mindestens 72 % der betroffenen Mitgliedstaaten vertreten, und

b. ÜNB, die Mitgliedstaaten vertreten, die mindestens 65 % der Bevölkerung der betroffenen Region umfassen.

Artikel 7(4)

Eine Sperrminorität für Entscheidungen über Vorschläge für die Pläne muss eine Mindestanzahl von ÜNB umfassen, die mehr als 35 % der Bevölkerung der teilnehmenden Mitgliedstaaten vertreten, zuzüglich ÜNB, die mindestens einen weiteren betroffenen Mitgliedstaat vertreten; ansonsten gilt die qualifizierte Mehrheit als erreicht.

Artikel 7(5)

Bei Entscheidungen der ÜNB über Vorschläge für in Artikel 6 Absatz 2 aufgeführte Modalitäten oder Methoden erhält jeder Mitgliedstaat eine Stimme. Gibt es im Hoheitsgebiet eines Mitgliedstaats mehr als einen ÜNB, teilt der Mitgliedstaat die Stimmrechte unter den ÜNB auf.

Artikel 7(6)

Legen ÜNB den jeweils zuständigen Behörden nicht innerhalb der in dieser Verordnung festgelegten Fristen in Zusammenarbeit mit der EU-VNBO einen ersten oder geänderten Vorschlag

für Modalitäten oder Methoden oder für Pläne vor, so übermitteln sie den jeweils zuständigen Behörden und der ACER entsprechende Entwürfe der Modalitäten oder Methoden bzw. der Pläne. Sie erläutern, warum keine Einigung erzielt wurde.

Die zuständigen Behörden treffen gemeinsam geeignete Maßnahmen für die Annahme der erforderlichen Modalitäten oder Methoden bzw. der erforderlichen Pläne. Dies kann z. B. durch Ersuchen um Änderungen der Entwürfe gemäß diesem Absatz, durch Überarbeitung und Vervollständigung dieser Entwürfe oder, falls keine Entwürfe vorgelegt wurden, durch Festlegung und Genehmigung der erforderlichen Modalitäten, Methoden oder Pläne erfolgen.

Artikel 8

1. Die ÜNB legen den jeweils zuständigen Behörden innerhalb der in den Artikeln 18, 23, 29, 33, 34, 35 und 37 festgelegten Fristen die Vorschläge für Modalitäten oder Methoden bzw. für Pläne zur Genehmigung vor. Die zuständigen Behörden können diese Fristen in Ausnahmefällen gemeinsam verlängern, insbesondere wenn eine Frist aufgrund von Umständen außerhalb des Verantwortungsbereichs der ÜNB oder der EU-VNBO nicht eingehalten werden kann.

2. Vorschläge für Modalitäten, Methoden oder bzw. Pläne gemäß Absatz 1 werden zeitgleich mit der Übermittlung an die zuständigen Behörden auch der ACER zur Information vorgelegt.

3. Auf gemeinsames Ersuchen der NRB gibt die ACER innerhalb von sechs Monaten nach Eingang des Vorschlags für Modalitäten oder Methoden oder für die Pläne eine Stellungnahme zu dem Vorschlag ab und übermittelt sie den NRB und den zuständigen Behörden. Die NRB, die CS-NCA und alle anderen als zuständige Behörden benannten Behörden stimmen sich untereinander ab, bevor die NRB die ACER um eine Stellungnahme ersuchen. Die ACER kann in dieser Stellungnahme Empfehlungen abgeben. Die ACER konsultiert die ENISA, bevor sie eine Stellungnahme zu den in Artikel 6 Absatz 2 aufgeführten Vorschlägen abgibt.

4. Die zuständigen Behörden konsultieren einander, arbeiten eng zusammen und stimmen sich untereinander ab, um zu einer Einigung über die vorgeschlagenen Modalitäten, Methoden oder Pläne zu gelangen. Vor der Genehmigung der Modalitäten oder Methoden oder der Pläne überarbeiten und ergänzen sie die Vorschläge nach Konsultation von ENTSO-E und der EU-VNBO erforderlichenfalls, um sicherzustellen, dass die Vorschläge mit dieser Verordnung im Einklang stehen und zu einem hohen gemeinsamen Cybersicherheitsniveau in der gesamten Union beitragen.

5. Die zuständigen Behörden entscheiden über die Modalitäten oder Methoden oder die Pläne innerhalb von sechs Monaten nach Eingang der Modalitäten oder Methoden bzw. der Pläne bei der jeweils zuständigen Behörde oder gegebenenfalls bei der letzten betroffenen zuständigen Behörde.

6. Gibt die ACER eine Stellungnahme ab, so tragen die jeweils zuständigen Behörden dieser Stellungnahme Rechnung und treffen ihre Entscheidungen innerhalb von sechs Monaten nach Eingang der Stellungnahme.

7. Verlangen die zuständigen Behörden für ihre Genehmigung gemeinsam eine Änderung der vorgeschlagenen Modalitäten oder Methoden oder der Pläne, so entwickeln die ÜNB in Zusammenarbeit mit der EU-VNBO einen Vorschlag für eine solche Änderung der Modalitäten oder

Methoden bzw. der Pläne. Die ÜNB legen den zuständigen Behörden den geänderten Vorschlag innerhalb von zwei Monaten nach deren Aufforderung zur Genehmigung vor. Die zuständigen Behörden entscheiden über die geänderten Modalitäten oder Methoden oder Pläne innerhalb von zwei Monaten nach deren Vorlage.

8. Konnten die zuständigen Behörden innerhalb der in Absatz 5 oder Absatz 7 genannten Frist keine Einigung erzielen, so unterrichten sie die Kommission. Die Kommission kann geeignete Maßnahmen ergreifen, um die Annahme der erforderlichen Modalitäten, Methoden oder Pläne zu ermöglichen.

9. Die ÜNB veröffentlichen mit Unterstützung von ENTSO-E und der EU-VNBO die Modalitäten oder Methoden oder die Pläne nach der Genehmigung durch die jeweils zuständigen Behörden auf ihren Websites, soweit diese Informationen nicht gemäß Artikel 47 als vertraulich betrachtet werden.

10. Die zuständigen Behörden können von den ÜNB und der EU-VNBO gemeinsam Vorschläge für Änderungen der genehmigten Modalitäten oder Methoden oder der genehmigten Pläne anfordern und eine Frist für die Einreichung dieser Vorschläge festlegen. Die ÜNB können den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO auch auf eigene Initiative Änderungen vorschlagen. Die Vorschläge zur Änderung der Modalitäten oder Methoden bzw. zur Änderung der Pläne werden nach dem Verfahren dieses Artikels entwickelt und genehmigt.

11. Mindestens alle drei Jahre nach der ersten Annahme der jeweiligen Modalitäten oder Methoden bzw. der Annahme der jeweiligen Pläne überprüfen die ÜNB in Zusammenarbeit mit der EU-VNBO die Wirksamkeit der angenommenen Modalitäten oder Methoden bzw. der angenommenen Pläne und teilen den zuständigen Behörden und der ACER die Ergebnisse der Überprüfung unverzüglich mit.

Artikel 8(1)

Die ÜNB legen den jeweils zuständigen Behörden innerhalb der in den Artikeln 18, 23, 29, 33, 34, 35 und 37 festgelegten Fristen die Vorschläge für Modalitäten oder Methoden bzw. für Pläne zur Genehmigung vor.

Die zuständigen Behörden können diese Fristen in Ausnahmefällen gemeinsam verlängern, insbesondere wenn eine Frist aufgrund von Umständen außerhalb des Verantwortungsbereichs der ÜNB oder der EU-VNBO nicht eingehalten werden kann.

Artikel 8(10)

Die zuständigen Behörden können von den ÜNB und der EU-VNBO gemeinsam Vorschläge für Änderungen der genehmigten Modalitäten oder Methoden oder der genehmigten Pläne anfordern und eine Frist für die Einreichung dieser Vorschläge festlegen.

Die ÜNB können den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO auch auf eigene Initiative Änderungen vorschlagen. Die Vorschläge zur Änderung der Modalitäten oder Metho-

den bzw. zur Änderung der Pläne werden nach dem Verfahren dieses Artikels entwickelt und genehmigt.

Artikel 8(11)

Mindestens alle drei Jahre nach der ersten Annahme der jeweiligen Modalitäten oder Methoden bzw. der Annahme der jeweiligen Pläne überprüfen die ÜNB in Zusammenarbeit mit der EU-VNBO die Wirksamkeit der angenommenen Modalitäten oder Methoden bzw. der angenommenen Pläne und teilen den zuständigen Behörden und der ACER die Ergebnisse der Überprüfung unverzüglich mit.

Artikel 8(2)

Vorschläge für Modalitäten, Methoden oder bzw. Pläne gemäß Absatz 1 werden zeitgleich mit der Übermittlung an die zuständigen Behörden auch der ACER zur Information vorgelegt.

Artikel 8(3)

Auf gemeinsames Ersuchen der NRB gibt die ACER innerhalb von sechs Monaten nach Eingang des Vorschlags für Modalitäten oder Methoden oder für die Pläne eine Stellungnahme zu dem Vorschlag ab und übermittelt sie den NRB und den zuständigen Behörden.

Die NRB, die CS-NCA und alle anderen als zuständige Behörden benannten Behörden stimmen sich untereinander ab, bevor die NRB die ACER um eine Stellungnahme ersuchen. Die ACER kann in dieser Stellungnahme Empfehlungen abgeben.

Die ACER konsultiert die ENISA, bevor sie eine Stellungnahme zu den in Artikel 6 Absatz 2 aufgeführten Vorschlägen abgibt.

Artikel 8(4)

Die zuständigen Behörden konsultieren einander, arbeiten eng zusammen und stimmen sich untereinander ab, um zu einer Einigung über die vorgeschlagenen Modalitäten, Methoden oder Pläne zu gelangen. Vor der Genehmigung der Modalitäten oder Methoden oder der Pläne überarbeiten und ergänzen sie die Vorschläge nach Konsultation von ENTSO-E und der EU-VNBO erforderlichenfalls, um sicherzustellen, dass die Vorschläge mit dieser Verordnung im Einklang stehen und zu einem hohen gemeinsamen Cybersicherheitsniveau in der gesamten Union beitragen.

Artikel 8(5)

Die zuständigen Behörden entscheiden über die Modalitäten oder Methoden oder die Pläne innerhalb von sechs Monaten nach Eingang der Modalitäten oder Methoden bzw. der Pläne bei

der jeweils zuständigen Behörde oder gegebenenfalls bei der letzten betroffenen zuständigen Behörde.

Artikel 8(6)

Gibt die ACER eine Stellungnahme ab, so tragen die jeweils zuständigen Behörden dieser Stellungnahme Rechnung und treffen ihre Entscheidungen innerhalb von sechs Monaten nach Eingang der Stellungnahme.

Artikel 8(7)

Verlangen die zuständigen Behörden für ihre Genehmigung gemeinsam eine Änderung der vorgeschlagenen Modalitäten oder Methoden oder der Pläne, so entwickeln die ÜNB in Zusammenarbeit mit der EU-VNBO einen Vorschlag für eine solche Änderung der Modalitäten oder Methoden bzw. der Pläne. Die ÜNB legen den zuständigen Behörden den geänderten Vorschlag innerhalb von zwei Monaten nach deren Aufforderung zur Genehmigung vor.

Die zuständigen Behörden entscheiden über die geänderten Modalitäten oder Methoden oder Pläne innerhalb von zwei Monaten nach deren Vorlage.

Artikel 8(8)

Konnten die zuständigen Behörden innerhalb der in Absatz 5 oder Absatz 7 genannten Frist keine Einigung erzielen, so unterrichten sie die Kommission.

Die Kommission kann geeignete Maßnahmen ergreifen, um die Annahme der erforderlichen Modalitäten, Methoden oder Pläne zu ermöglichen.

Artikel 8(9)

Die ÜNB veröffentlichen mit Unterstützung von ENTSO-E und der EU-VNBO die Modalitäten oder Methoden oder die Pläne nach der Genehmigung durch die jeweils zuständigen Behörden auf ihren Websites, soweit diese Informationen nicht gemäß Artikel 47 als vertraulich betrachtet werden.

Artikel 9

1. Die ÜNB konsultieren mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO die Interessenträger, einschließlich der ACER, der ENISA und der zuständigen Behörde jedes Mitgliedstaats, zu den Entwürfen von Vorschlägen für die in Artikel 6 Absatz 2 genannten Modalitäten oder Methoden und für die in Artikel 6 Absatz 3 genannten Pläne. Die Konsultation dauert mindestens einen Monat.

2. Die in Artikel 6 Absatz 2 genannten Vorschläge für Modalitäten oder Methoden, die von den ÜNB in Zusammenarbeit mit der EU-VNBO vorgelegt wurden, werden veröffentlicht und auf Unionsebene einer Konsultation unterzogen. Die von den relevanten ÜNB in Zusammenarbeit mit der EU-VNBO auf regionaler Ebene vorgelegten Vorschläge für Pläne gemäß Artikel 6 Absatz 3 werden mindestens auf regionaler Ebene einer Konsultation unterzogen.
3. Die ÜNB, unterstützt von ENTSO-E, und die für den Vorschlag für Modalitäten, Methoden oder Pläne zuständige EU-VNBO tragen den in den gemäß Absatz 1 durchgeführten Konsultationen geäußerten Ansichten der Interessenträger, gebührend Rechnung, bevor sie die Vorschläge zur regulatorischen Genehmigung vorlegen. In allen Fällen ist zusammen mit dem Vorschlag eine fundierte Begründung vorzulegen, weshalb die aus der Konsultation hervorgegangenen Stellungnahmen berücksichtigt bzw. nicht berücksichtigt wurden, und rechtzeitig — vor oder gleichzeitig mit dem Vorschlag für Modalitäten oder Methoden — zu veröffentlichen.

Artikel 9(1)

Die ÜNB konsultieren mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO die Interessenträger, einschließlich der ACER, der ENISA und der zuständigen Behörde jedes Mitgliedstaats, zu den Entwürfen von Vorschlägen für die in Artikel 6 Absatz 2 genannten Modalitäten oder Methoden und für die in Artikel 6 Absatz 3 genannten Pläne. Die Konsultation dauert mindestens einen Monat.

Artikel 9(2)

Die in Artikel 6 Absatz 2 genannten Vorschläge für Modalitäten oder Methoden, die von den ÜNB in Zusammenarbeit mit der EU-VNBO vorgelegt wurden, werden veröffentlicht und auf Unionsebene einer Konsultation unterzogen. Die von den relevanten ÜNB in Zusammenarbeit mit der EU-VNBO auf regionaler Ebene vorgelegten Vorschläge für Pläne gemäß Artikel 6 Absatz 3 werden mindestens auf regionaler Ebene einer Konsultation unterzogen.

Artikel 9(3)

Die ÜNB, unterstützt von ENTSO-E, und die für den Vorschlag für Modalitäten, Methoden oder Pläne zuständige EU-VNBO tragen den in den gemäß Absatz 1 durchgeführten Konsultationen geäußerten Ansichten der Interessenträger, gebührend Rechnung, bevor sie die Vorschläge zur regulatorischen Genehmigung vorlegen. In allen Fällen ist zusammen mit dem Vorschlag eine fundierte Begründung vorzulegen, weshalb die aus der Konsultation hervorgegangenen Stellungnahmen berücksichtigt bzw. nicht berücksichtigt wurden, und rechtzeitig — vor oder gleichzeitig mit dem Vorschlag für Modalitäten oder Methoden — zu veröffentlichen.

Benannter Strommarktbetreiber (NEMO)

Ein Marktteilnehmer, der von der zuständigen Behörde eines Mitgliedstaats benannt wurde, um

an der Kopplung des einheitlichen Day-Ahead-Markts oder des einheitlichen Intraday-Markts teilzunehmen.

Computer-Notfallteams (CSIRT)

Eine Organisation, die für das Management von Sicherheitsvorfällen in Netz- und Informationssystemen zuständig ist. RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [124]

Cybersicherheit zuständigen Behörden (CS NCA)

Die nationale zuständige Behörde für Cybersicherheit in einem bestimmten Mitgliedstaat.

DG CONNECT (Generaldirektion Kommunikationsnetze, Inhalte und Technologien der Europäischen Kommission)

Die Generaldirektion Kommunikationsnetze, Inhalte und Technologien (DG CONNECT) entwickelt und implementiert die politischen Maßnahmen der Europäischen Kommission.

DG ENER (Generaldirektion Energie der Europäischen Kommission)

Die Generaldirektion Energie der Europäischen Kommission ist für die Energiepolitik der EU verantwortlich.

Einrichtung mit erheblichen Auswirkungen (HIE)

Bezeichnet eine Einrichtung, die einen Prozess mit erheblichen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24 [125] ermittelt wird.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [126]

Einrichtung mit kritischen Auswirkungen (CIE)

Bezeichnet eine Einrichtung, die einen Prozess mit kritischen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24 [127] bestimmt wird.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [128]

[124] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[125] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_24
[126] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366
[127] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_24
[128] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

Elektrizitätskoordinierungsgruppe (ECG)

Ziel der Elektrizitätskoordinierungsgruppe ist es, Informationen über strompolitische Maßnahmen mit grenzüberschreitenden Auswirkungen auszutauschen und zu koordinieren und die Zusammenarbeit durch Wissens- und Erfahrungsaustausch zu erleichtern.

KOMMISSIONSENTSCHEIDUNG 2012/C 353/02 [129]

EU-VNBO (EU DSO)

Europäische Organisation der Verteilnetzbetreiber

Die EU-VNBO wurde von der Europäischen Union gegründet, um die Koordinierung und Entwicklung der Stromverteilungsnetze zu fördern. Sie spielt eine zentrale Rolle bei der Integration der Energiemärkte, der Einbindung erneuerbarer Energiequellen und der Unterstützung der Energiewende.

Die Aktivitäten der EU-VNBO werden durch das EU-Paket „Saubere Energie“ und die Strommarktverordnung (Verordnung (EU) 2019/943) geregelt.

https://eudsoentity.eu/ [130]

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [131]

Europäische Kommission (EC)

Die Europäische Kommission ist das Exekutivorgan der Europäischen Union und verantwortlich für die Umsetzung der EU-Rechtsvorschriften, die Entwicklung von Politiken und die Verwaltung des Haushalts.

Kooperationsgruppe für Netz- und Informationssysteme (NIS CG)

Kooperationsgruppe für Cybersicherheit

Die Kooperationsgruppe für Netz- und Informationssicherheit (NIS CG) koordiniert die Cybersicherheitszusammenarbeit in der EU. Die Aufgaben der NIS-Kooperationsgruppe sind in Artikel 11 der NIS-Richtlinie festgelegt.

DURCHFÜHRUNGSBESCHLUSS (EU) 2017/179 DER KOMMISSION [132]

Mitgliedstaat (MS)

[129] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32012D1117(01)
[130] https://eudsoentity.eu/
[131] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[132] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32017D0179

Bezeichnet ein Land, das Mitglied der Europäischen Union ist und das EU-Recht einhält.

Nationale Regulierungsbehörden (NRA)

Eine offizielle staatliche oder unabhängige Organisation, die für die Regulierung, Überwachung und Kontrolle bestimmter Bereiche innerhalb eines Landes oder einer Region zuständig ist.

Nationale zuständige Behörde (NCA)

Eine nationale zuständige Behörde ist eine offizielle Stelle oder Organisation, die durch Rechtsvorschriften befugt ist, einen bestimmten Sektor oder Bereich zu regeln, zu überwachen und zu kontrollieren. Diese Behörden stellen die Einhaltung nationaler und gegebenenfalls internationaler Gesetze und Standards sicher.

Regionale Koordinierungszentren (RCC)

Regionale Koordinierungszentren (RCC) haben eine beratende Rolle bei der Entwicklung regionaler Cybersicherheitsrisikobewertungen und -minderungspläne und koordinieren die Zusammenarbeit der Mitgliedstaaten im Bereich der Cybersicherheit.

Eingerichtet gemäß Artikel 35 der Verordnung (EU) 2019/943.

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [133]

Risikovorsorge zuständigen Behörden (RP-NCA)

Die RP-NCA ist für die Entwicklung und Umsetzung von Risikovorsorgeplänen zuständig.

Systembetreiber

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung eines Übertragungs- oder Verteilernetzes verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [134]

Übertragungsnetzbetreiber (TSO)

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung des Übertragungsnetzes in einem bestimmten Gebiet sowie dessen Verbindung

[133] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[134] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944

mit anderen Netzen und die langfristige Fähigkeit zur Deckung eines angemessenen Bedarfs an Stromübertragung verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [135]

Verband Europäischer Übertragungsnetzbetreiber (ENTSO-E)

Gemeinsame Organisation der europäischen Übertragungsnetzbetreiber. Sie spielt eine zentrale Rolle bei der Integration des europäischen Strommarktes und der Sicherstellung der Stabilität des Stromsystems.

Die Aktivitäten von ENTSO-E werden durch das EU-Paket „Saubere Energie“ und die Strommarktverordnung (Verordnung (EU) 2019/943) geregelt.

https://www.entsoe.eu/ [136]

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [137]

Verteilnetzbetreiber (DSO)

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung eines Verteilernetzes in einem bestimmten Gebiet sowie für die langfristige Fähigkeit zur Deckung gerechtfertigter Stromverteilungsanforderungen verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [138]

[135] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[136] https://www.entsoe.eu/
[137] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[138] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944

Resources

FILE 1

Vorläufige Liste unionsweiter Prozesse mit hohen und kritischen Auswirkungen (Englisch)

files/Provisional list of Union-wide high-impact and critical-impact processes.pdf

FILE 2

Begleitdokument zur vorläufigen Liste unionsweiter Prozesse mit hohen und kritischen Auswirkungen (Englisch)

files/Supporting document Provisional list of Union-wide high-impact and critical-impact processes.pdf

FILE 3

Vorläufiger Electricity Cybersecurity Impact Index (ECII) (Englisch)

files/Provisional ECII.pdf

FILE 4

Begleitdokument zum vorläufigen Electricity Cybersecurity Impact Index (ECII) (Englisch)

files/Supporting document provisional ECII.pdf