EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RAHMEN ZUR BEWERTUNG NATIONALER FÄHIGKEITEN

DEZEMBER 2020

ÜBER ENISA

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Die Agentur wurde im Jahr 2004 errichtet und durch den Rechtsakt zur Cybersicherheit in ihrem Mandat weiter gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von IKT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, kooperiert mit den Mitgliedstaaten und Organen und Einrichtungen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Kapazitätenaufbau und Sensibilisierung im Bereich der Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürgerinnen und Bürger Europas zu gewährleisten. Weitere Informationen sind zu finden auf www.enisa.europa.eu.

KONTAKTANGABEN

Wenn Sie mit den Autoren Kontakt aufnehmen möchten, wenden Sie sich bitte an team@enisa.europa.eu.
Medienanfragen zu dieser Veröffentlichung richten Sie bitte an press@enisa.europa.eu.

AUTOREN

Anna Sarri, Pinelopi Kyranoudi – Agentur der Europäischen Union für Cybersicherheit (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique – Wavestone

DANKSAGUNG

Die ENISA bedankt sich bei allen teilnehmenden Sachverständigen und würdigt sie für die wertvollen Beiträge für diesen Bericht und insbesondere für die folgenden Beiträge (in alphabetischer Reihenfolge):

Zentralstaatsbüro für die Entwicklung der digitalen Gesellschaft (Kroatien), Marin Ante Pivcevic

Zentrum für Cybersicherheit (Belgien)

CFCS – Center for Cybersikkerhed (Dänemark), Thomas Wulff

Europäisches Cybersicherheitszentrum – EC3, Alzofra Martinez Alvaro

Europäisches Cybersicherheitszentrum – EC3, Adrian-Ionut Bobeica

Bundesministerium des Innern (Deutschland), Sascha-Alexander Lettgen

Behörde für Informationssicherheit (Republik Slowenien), Marjan Kavčič

Italienische Regierung (Italien)

Agentur für Informationstechnologie in Malta (Malta), Katia Bonello und Martin Camilleri

Ministerium für Justiz und öffentliche Sicherheit (Norwegen), Robin Bakke

Ministerium für digitale Politik (Griechenland), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali und Sotiris Vasilos

Ministerium für wirtschaftliche Angelegenheiten und Kommunikation (Estland), Anna-Liisa Pärnalaas

Nationale Agentur für Cyber- und Informationssicherheit (Tschechische Republik), Veronika Netolická

Nationale Sicherheitsbehörde (Slowakei)

Nationale Sicherheitsbehörde (Spanien), Maria Mar Lopez Gil

NCTV, Ministerium für Justiz und Sicherheit (Niederlande)

Portugiesisches Nationales Cybersicherheitszentrum (Portugal), Alexandre Leite und Pedro Matos

Abteilung für Cybersicherheitspolitik, Ministerium für Umwelt, Klima und Kommunikation (Irland), James Caffrey

Universität Oxford – Global Cyber Security Capacity Centre (Zentrum für globale Cybersicherheitskapazitäten), Carolin Weisser Harris

Die ENISA möchte sich auch bei all denjenigen Sachverständigen, die Beiträge geleistet haben, aber lieber anonym bleiben, für ihren wertvollen Beitrag zu dieser Studie bedanken.

IMPRESSUM/RECHTLICHE HINWEISE

HINWEIS ZUM COPYRIGHT

ISBN: 978-92-9204-477-0

DOI: 10.2824/678327

KATALOG: TP-02-21-253-DE-N

1. INHALTSVERZEICHNIS

GLOSSAR

AKRONYM	DEFINITION
C2M2	Reifegradmodell für Cybersicherheitsfähigkeiten (Cybersecurity Capability Maturity Model)
CCRA	Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC (Common Criteria Recognition Arrangement)
CCSMM	Community-Reifegradmodell für Cybersicherheit (Community Cyber Security Maturity Model)
CII	Kritische Informationsinfrastruktur (Critical Information Infrastructure)
CMM	Reifegradmodell für Cybersicherheitskapazitäten für Nationen (Cybersecurity Capacity Maturity Model for Nations)
CMMC	Zertifizierung des Reifegradmodells für Cybersicherheit (Cybersecurity Maturity Model Certification)
CPI	Cyber Power Index
CSIRT	Computer-Notfallteams (Computer Security Incident Response Team)
CVD	Koordinierte Offenlegung von Sicherheitslücken (Coordinated Vulnerability Disclosure)
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
DSM	Digitaler Binnenmarkt (Digital Single Market)
DSMS	Datenschutz-Managementsystem (Privacy Information Management System, PIMS)
ECCG	Europäische Gruppe für die Cybersicherheitszertifizierung (European Cybersecurity Certification Group)
ECSM	Europäischer Monat der Cybersicherheit
ECSO	Europäische Cybersicherheitsorganisation
EFTA	Europäische Freihandelsassoziation
EQR	Europäischer Qualifikationsrahmen
EU	Europäische Union
F&E	Forschung und Entwicklung
GCI	Globaler Cybersicherheitsindex
GDS	Dienststelle für die digitale Transformation der britischen Regierung (Government Digital Service)
IA-CM	Modell für interne Auditstellen für den öffentlichen Sektor (Internal Audit Capability Model for the Public Sector)

IKT	Informations- und Kommunikationstechnologien
ISMM	Reifegradmodell für Informationssicherheit für das NIST-Cybersicherheitsregelwerk (Information Security Maturity Model for NIST Cybersecurity Framework)
ITU	Internationale Fernmeldeunion
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Unternehmen
LEA	Strafverfolgungsbehörde (Law Enforcement Agency)
MS	Mitgliedstaat
NCSS	Nationale Cybersicherheitsstrategien
NIS	Netz- und Informationssicherheit
NIST	Nationales Institut für Standards und Technologie
NLO	Nationale Verbindungsbeamte
OES	Betreiber wesentlicher Dienste (Operators of Essential Services)
OT	Betriebstechnik (Operations Technology)
PET	Technologien zum Schutz der Privatsphäre (Privacy Enhancing Technologies)
PPP	Öffentlich-private Partnerschaft
Q-C2M2	Reifegradmodell für Cybersicherheitsfähigkeiten von Katar (Qatar Cybersecurity Capability Maturity Model)
SOG-IS MRA	Abkommen über die gegenseitige Anerkennung des Beratenden Ausschusses für die Maßnahmen auf dem Gebiet der Sicherheit von Informationssystemen (Senior Officers Group for Information Systems' Security, Mutual Recognition Agreement)

ZUSAMMENFASSUNG

Da die derzeitige Cyberbedrohungslandschaft sich weiter ausdehnt und die Intensität und Anzahl der Cyberangriffe weiter zunimmt, müssen die EU-Mitgliedstaaten wirksam reagieren und ihre nationalen Cybersicherheitsstrategien (NCSS) weiterentwickeln und anpassen. Seit der Veröffentlichung der ersten Studien der ENISA zu NCSS im Jahr 2012 haben die EU-Mitgliedstaaten und die EFTA-Länder große Fortschritte bei der Entwicklung und Umsetzung ihrer Strategien erzielt.

In diesem Bericht werden die von der ENISA durchgeführten Arbeiten zum Aufbau eines Rahmens zur Bewertung nationaler Fähigkeiten (NCAF) vorgestellt.

Der Rahmen zielt darauf ab, den Mitgliedstaaten eine Selbstbewertung ihres Reifegrades durch Bewertung ihrer NCSS-Ziele zu ermöglichen, die ihnen helfen wird, die Cybersicherheitsfähigkeiten sowohl auf strategischer als auch auf operativer Ebene zu verbessern und auszubauen.

Er enthält eine einfache repräsentative Ansicht des Reifegrades der Cybersicherheit des Mitgliedstaats. Der NCAF ist ein Instrument, das die Mitgliedstaaten bei Folgendem unterstützt:

- Bereitstellung nützlicher Informationen zur Entwicklung einer langfristigen Strategie (z. B. bewährte Verfahren, Leitlinien);
- Hilfestellung bei der Ermittlung fehlender Elemente in der NCSS;
- Hilfestellung beim weiteren Ausbau der Cybersicherheitskapazitäten;
- Stärkung der Rechenschaftspflicht für politische Maßnahmen;
- Vermittlung von Glaubwürdigkeit gegenüber der Öffentlichkeit und internationalen Partnern;
- Unterstützung der Öffentlichkeitsarbeit und Verbesserung der öffentlichen Wahrnehmung als transparente Organisation;
- Hilfestellung bei der Antizipierung künftiger Probleme;
- Hilfestellung bei der Ermittlung der gewonnenen Erkenntnisse und bewährten Verfahren;
- Bereitstellung einer Basis für die Cybersicherheitskapazitäten in der gesamten EU, um Diskussionen zu erleichtern;
- Hilfestellung bei der Bewertung der nationalen Fähigkeiten in Bezug auf Cybersicherheit.

Dieser Rahmen wurde mit Unterstützung von ENISA-Fachleuten und Vertretern aus 19 Mitgliedstaaten und den EFTA-Ländern entworfen.[1] Die Zielgruppe dieses Berichts sind politische Entscheidungsträger, Sachverständige und Staatsbeamte, die für die Entwicklung, Implementierung und Bewertung einer NCSS und auf einer breiteren Ebene für Cybersicherheitsfähigkeiten verantwortlich sind oder daran beteiligt sind.

Der Rahmen zur Bewertung nationaler Fähigkeiten umfasst 17 strategische Ziele und gliedert sich in vier Hauptcluster:

- Cluster Nr. 1: Governance und Standards im Bereich der Cybersicherheit
  1. Entwicklung eines nationalen Cybernotfallplans
  2. Festlegung grundlegender Sicherheitsvorkehrungen
  3. Sicherung der digitalen Identität und Aufbau von Vertrauen in digitale öffentliche Dienste

- Cluster Nr. 2: Kapazitätenaufbau und Sensibilisierung
  4. Organisation von Cybersicherheitsübungen
  5. Einrichtung einer Kapazität zur Reaktion auf Sicherheitsvorfälle
  6. Sensibilisierung der Benutzer
  7. Stärkung von Schulungs-, Ausbildungs- und Bildungsprogrammen
  8. Förderung von F&E
  9. Schaffung von Anreizen für den Privatsektor, in Sicherheitsvorkehrungen zu investieren
  10. Verbesserung der Cybersicherheit der Lieferkette

- Cluster Nr. 3: Gesetze und Bestimmungen
  11. Schutz der kritischen Informationsinfrastruktur, OES und DSP
  12. Bekämpfung der Cyberkriminalität
  13. Einrichtung von Mechanismen zur Meldung von Vorfällen
  14. Stärkung des Schutzes der Privatsphäre und des Datenschutzes

- Cluster Nr. 4: Zusammenarbeit
  15. Aufbau einer öffentlich-privaten Partnerschaft
  16. Institutionalisierung der Zusammenarbeit zwischen öffentlichen Stellen
  17. Internationale Zusammenarbeit

[1] Befragt wurden Vertreter aus folgenden Mitgliedstaaten und EFTA-Ländern: Belgien, Dänemark, Deutschland, Estland, Griechenland, Irland, Italien, Kroatien, Liechtenstein, Malta, Niederlande, Norwegen, Portugal, Slowakei, Slowenien, Spanien, Schweden, Tschechische Republik, Ungarn..

1. EINFÜHRUNG

Nach der im Juli 2016 veröffentlichten Richtlinie zur Netz- und Informationssicherheit (NIS) müssen die EU-Mitgliedstaaten gemäß Artikel 1 und 7 eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festlegen, die auch als NCSS (National Cyber Security Strategy) bezeichnet wird. In diesem Zusammenhang wird eine NCSS als Rahmen definiert, der strategische Grundsätze, Leitlinien, strategische Ziele, Prioritäten, angemessene Politik- und Regulierungsmaßnahmen festlegt. Das vorgesehene Ziel einer NCSS besteht darin, ein hohes Maß an Netzwerk- und Systemsicherheit zu erreichen und aufrechtzuerhalten, damit die Mitgliedstaaten potenzielle Bedrohungen mindern können. Darüber hinaus kann eine NCSS auch ein Katalysator für die wirtschaftliche Entwicklung sowie den wirtschaftlichen und sozialen Fortschritt sein.

Der EU-Rechtsakt zur Cybersicherheit sieht vor, dass die ENISA die Verbreitung bewährter Verfahren bei der Definition und Umsetzung einer NCSS fördert, indem sie die Mitgliedstaaten bei der Annahme der NIS-Richtlinie unterstützt und wertvolle Rückmeldungen zu ihren Erfahrungen sammelt. Zu diesem Zweck hat die ENISA verschiedene Instrumente entwickelt, um die Mitgliedstaaten bei der Entwicklung, Umsetzung und Bewertung ihrer nationalen Cybersicherheitsstrategien (NCSS) zu unterstützen.

Im Rahmen ihres Mandats zielt die ENISA darauf ab, einen Rahmen für die Selbstbewertung nationaler Fähigkeiten zu entwickeln, um den Reifegrad der verschiedenen NCSS zu messen. Ziel dieses Berichts ist es, die in der Definition des Selbstbewertungsrahmens durchgeführte Studie vorzustellen.

1.1 STUDIENUMFANG UND ZIELE

Das Hauptziel dieser Studie ist die Schaffung eines Rahmens zur Selbstbewertung nationaler Fähigkeiten, nachfolgend als NCAF bezeichnet, um den Reifegrad der Cybersicherheitsfähigkeiten der Mitgliedstaaten zu messen. Insbesondere sollte der Rahmen die Mitgliedstaaten zu Folgendem befähigen:

- Durchführung der Bewertung ihrer nationalen Cybersicherheitsfähigkeiten;
- Sensibilisierung für den Reifegrad des Landes;
- Identifizierung von Verbesserungspotentialen;
- Aufbau von Cybersicherheitsfähigkeiten.

Dieser Rahmen sollte den Mitgliedstaaten und insbesondere den nationalen politischen Entscheidungsträgern helfen, eine Selbstbewertung durchzuführen, um die nationalen Cybersicherheitsfähigkeiten zu verbessern.

1.2 METHODOLOGISCHER WEG

Der methodologische Weg zur Entwicklung des Rahmens zur Selbstbewertung nationaler Kapazitäten beruht auf vier Hauptschritten:

1. **Schreibtischstudie**: Der erste Schritt besteht in der Durchführung einer umfassenden Literaturprüfung, um bewährte Verfahren für die Entwicklung eines Rahmens zur Bewertung der Reife für nationale Cybersicherheitsstrategien zu sammeln. Die Schreibtischstudie konzentriert sich auf eine systematische Analyse relevanter Dokumente zum Aufbau von Cybersicherheitskapazitäten und zur Strategiedefinition, auf bestehende NCCS der Mitgliedstaaten und auf einen Vergleich bestehender

Reifegradmodelle zur Cybersicherheit. Ein Benchmark-Test zu bestehenden Reifegradmodellen wurde durchgeführt, indem ein für den Zweck dieser Studie entwickelter Analyserahmen entwickelt wurde. Der Analyserahmen baut auf der Becker[2]-Methodik für die Entwicklung von Reifegradmodellen auf, die ein generisches und konsolidiertes Verfahrensmodell für die Gestaltung von Reifegradmodellen festlegt und klare Anforderungen für die Entwicklung von Reifegradmodellen liefert. Der Analyserahmen wurde weiter angepasst, um die Anforderungen dieser Studie zu erfüllen.

2. **Zusammentragung von Meinungen von Fachleuten und Interessenträgern:** Basierend auf den Daten, die im Rahmen der Schreibtischstudie gesammelt wurden, und den damit verbundenen vorläufigen Ergebnissen der Analyse umfasste diese Phase die Ermittlung von Fachleuten, die Erfahrung in der Entwicklung und Implementierung einer NCSS oder von Reifegradmodellen haben, sowie deren Einladung zur Befragung. ENISA wandte sich an die Sachverständigengruppe für die nationale Cybersicherheitsstrategie und die nationalen Verbindungsbeamten (NLO), um die relevanten Fachleute in jedem Mitgliedstaat zu finden. Zusätzlich wurden einige Fachleute befragt, die an der Entwicklung von Reifegradmodellen beteiligt waren. Insgesamt wurden 22 Befragungen durchgeführt, von denen 19 mit Vertretern von Cybersicherheitsagenturen in verschiedenen Mitgliedstaaten (und EFTA-Ländern) durchgeführt wurden.
3. **Analyse der Bestandsaufnahme:** Die durch die Schreibtischstudie und durch Befragungen gesammelten Daten wurden anschließend analysiert, um bewährte Verfahren bei der Gestaltung eines Selbstbewertungsrahmens zu ermitteln, um die Reife der NCSS zu messen, die Bedürfnisse der Mitgliedstaaten zu verstehen und zu bestimmen, welche Daten in den verschiedenen europäischen Ländern[3] gesammelt werden können. Diese Analyse ermöglichte es, das in den vorherigen Schritten entwickelte vorläufige Modell zu optimieren und die im Modell enthaltenen Indikatoren, den Reifegrad und seine Dimensionen zu verfeinern.
4. **Endgültige Formgebung des Modells:** Anschließend wurde eine aktualisierte Version des Selbstbewertungsrahmens für nationale Fähigkeiten von den Fachleuten der ENISA überprüft und danach von weiteren Sachverständigen in einem Workshop im Oktober 2020 vor der Veröffentlichung weiter validiert.

1.3 ZIELGRUPPE

Die Zielgruppe dieses Berichts sind politische Entscheidungsträger, Fachleute und Beamte, die für die Entwicklung, Implementierung und Bewertung einer NCSS und auf einer breiteren Ebene für Cybersicherheitsfähigkeiten zuständig oder daran beteiligt sind. Darüber hinaus können die in diesem Dokument formalisierten Ergebnisse für Fachleute und Forscher im Bereich Cybersicherheitspolitik auf nationaler oder europäischer Ebene von Wert sein.

[2] J. Becker, R. Knackstedt, and J. Pöppelbuß, „Developing Maturity Models for IT Management: A Procedure Model and its Application“, Business & Information Systems Engineering, Band 1, Nr. 3, S. 213-222, Juni 2009.
[3] Für die Zwecke dieser Studie gehören zu den in diesem Bericht genannten „europäischen Ländern“ die 27 EU-Mitgliedstaaten.

2. HINTERGRUND

2.1 FRÜHERE ARBEITEN ZUM NCSS-LEBENSZYKLUS

Wie im EU-Rechtsakt zur Cybersicherheit festgelegt, besteht eines der Hauptziele der ENISA darin, die Mitgliedstaaten bei der Entwicklung nationaler Strategien zur Sicherheit von Netzwerk- und Informationssystemen zu unterstützen, die Verbreitung dieser Strategien zu fördern und deren Implementierung zu überwachen. Im Rahmen ihres Mandats hat die ENISA mehrere Dokumente zu diesem Thema erstellt, um den Austausch bewährter Verfahren zu fördern und die Implementierung von NCSS in der gesamten EU zu unterstützen:

- ein Praxisleitfaden zur Entwicklungs- und Ausführungsphase von NCSS[4], veröffentlicht 2012,
- ein Dokument zur Kursausrichtung für nationale Bemühungen zur Stärkung der Sicherheit im Cyberspace[5] (2012),
- ein erster ENISA-Rahmen zur Bewertung der NCSS eines Mitgliedstaats[6] (2014),
- eine interaktive Online-Karte zu NCSS[7] (2014),
- ein NCSS-Leitfaden über bewährte Verfahren[8] (2016),
- das nationale Cybersicherheitsstrategie-Bewertungsinstrument[9] (2018),
- Bewährte Verfahren bei Innovationen für Cybersicherheit im Rahmen der NCSS („Good practices in innovation on Cybersecurity under the NCSS“)[10] (2019),

ANHANG A bietet eine kurze Zusammenfassung der wichtigsten Veröffentlichungen der ENISA zu diesem Thema.

Die oben genannten Leitfäden und Dokumente wurden im Rahmen der Schreibtischstudie untersucht. Insbesondere ist das „Nationale Cybersicherheitsstrategie-Bewertungsinstrument“[11] ein grundlegendes Element des NCAF. Der NCAF baut auf den Zielen des Online-Bewertungsinstruments für NCSS auf.

[4] NCSS: Practical Guide on Development and Execution (ENISA, 2012).
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012).
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] An evaluation framework for NCSS (ENISA, 2014).
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] National Cybersecurity Strategies - Interactive Map (ENISA 2014, aktualisiert 2019).
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Dieses Dokument ersetzt den Leitfaden von 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016).
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] National Cybersecurity Strategies Evaluation Tool (2018).
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] National Cybersecurity Strategies Evaluation Tool (2018).
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

2.2 GEMEINSAME ZIELE INNERHALB DER EUROPÄISCHEN NCSS FESTGELEGT

Die Ungleichheit zwischen den verschiedenen Mitgliedstaaten macht es schwierig, gemeinsame Aktivitäten oder Aktionspläne in verschiedenen nationalen Kontexten, rechtlichen Rahmenbedingungen und der politischen Agenda zu ermitteln. Die NCSS der Mitgliedstaaten verfolgen jedoch häufig strategische Ziele, die sich auf dieselben Themen beziehen. Auf der Grundlage der früheren Arbeiten der ENISA und der Analyse der NCSS der Mitgliedstaaten wurden 22 strategische Ziele ermittelt. 15 dieser strategischen Ziele wurden bereits in früheren Arbeiten der ENISA festgelegt, zwei wurden in dieser Studie neu hinzugefügt und fünf Ziele wurden festgelegt, um sie in der Zukunft in Erwägung zu ziehen.

2.2.1 Gemeinsame strategische Ziele der Mitgliedstaaten

Basierend auf den früheren Arbeiten der ENISA, nämlich dem Nationalen Cybersicherheitsstrategie-Bewertungsinstrument[12], zeigt die folgende Tabelle die oben genannten 15 strategischen Ziele, die üblicherweise in den NCSS der Mitgliedstaaten behandelt werden. Die Ziele umreißen den Kern der allgemeinen „nationalen Philosophie“ zu diesem Thema. Weitere Informationen zu den unten beschriebenen Zielen finden Sie im ENISA-Bericht zum NCSS-Leitfaden für bewährte Verfahren[13].

Tabelle 1: Gemeinsame strategische Ziele der Mitgliedstaaten in ihren NCSS

ID	Strategische Ziele der NCSS	Ziele
1	**Entwicklung von nationalen Cybernotfallplänen**	▶ Präsentation und Erläuterung der Kriterien, anhand derer eine Situation als Krise definiert werden sollte ▶ Definition wichtiger Prozesse und Maßnahmen zur Bewältigung der Krise ▶ Klare Definition der Rollen und Verantwortlichkeiten verschiedener Interessenträger während einer Cyberkrise ▶ Präsentation und Erläuterung der Kriterien für das Ende einer Krise und/oder wer die Befugnis hat, sie als beendet zu erklären
2	**Festlegung grundlegender Sicherheitsvorkehrungen**	▶ Harmonisierung der unterschiedlichen Verfahren der Organisationen im öffentlichen und im privaten Sektor ▶ Schaffung einer gemeinsamen Sprache zwischen den zuständigen Behörden und den Organisationen und Öffnung sicherer Kommunikationskanäle ▶ Befähigung verschiedener Interessenträger, ihre Cybersicherheitsfähigkeiten zu überprüfen und zu vergleichen ▶ Austausch von Informationen über bewährte Verfahren für Cybersicherheit in allen Branchen ▶ Hilfestellung für die Interessenträger, ihre Investitionen in die Sicherheit zu priorisieren
3	**Organisation von Cybersicherheitsübungen**	▶ Ermittlung, was getestet werden muss (Pläne und Prozesse, Personen, Infrastruktur, Reaktionsfähigkeiten, Kooperationsfähigkeiten, Kommunikation usw.) ▶ Einrichtung eines nationalen Planungsteams für Cyberübungen mit einem klaren Auftrag ▶ Integration von Cyberübungen in den Lebenszyklus der nationalen Cybersicherheitsstrategie oder des nationalen Cybernotfallplans

[12] National Cybersecurity Strategies Evaluation Tool (2018).
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Dieses Dokument ersetzt den Leitfaden von 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016).
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

ID	Strategische Ziele der NCSS	Ziele
4	Einrichtung einer Kapazität zur Reaktion auf Sicherheitsvorfälle	▶ Auftrag – bezieht sich auf die Befugnisse, Rollen und Verantwortlichkeiten, die dem Team von der jeweiligen staatlichen Stelle zugewiesen werden müssen ▶ Dienstleistungsportfolio – umfasst die Dienstleistungen, die ein Team für seinen Kundenkreis erbringt oder für sein eigenes internes Funktionieren nutzt ▶ Operative Fähigkeiten – betrifft die technischen und operativen Anforderungen, die ein Team erfüllen muss ▶ Kooperationsfähigkeiten – umfassen Anforderungen hinsichtlich des Informationsaustauschs mit anderen Teams, die nicht durch die vorherigen drei Kategorien abgedeckt sind, z. B. politische Entscheidungsträger, Militär, Aufsichtsbehörden, Betreiber (kritischer Informationsinfrastrukturen) und Strafverfolgungsbehörden
5	Sensibilisierung der Benutzer	▶ Ermittlung von Wissenslücken in Bezug auf Cybersicherheit oder Informationssicherheit ▶ Schließen der Lücken durch Schärfen des Bewusstseins oder Entwicklung/Stärkung der Wissensgrundlagen
6	Stärkung von Schulungs-, Ausbildungs- und Bildungsprogrammen	▶ Verbesserung der operativen Fähigkeiten der vorhandenen Mitarbeiter für Informationssicherheit ▶ Ermutigung von Lernenden, sich anzuschließen, und ihre Vorbereitung zum Eintritt den Bereich der Cybersicherheit ▶ Förderung und Bewerbung von Beziehungen zwischen dem akademischen Umfeld der Informationssicherheit und der Informationssicherheitsbranche ▶ Ausrichtung der Cybersicherheitsschulung an Unternehmensanforderungen
7	Förderung von F&E	▶ Ermittlung der tatsächlichen Ursachen von Sicherheitsanfälligkeiten, anstatt nur deren Auswirkungen zu beheben ▶ Zusammenbringen von Wissenschaftlern aus verschiedenen Disziplinen, um Lösungen für mehrdimensionale und komplexe Probleme wie physische Cyberbedrohungen zu finden ▶ Zusammenführung der Bedürfnisse der Wirtschaft und der Forschungsergebnisse, um den Übergang von der Theorie zur Praxis zu erleichtern ▶ Finden von Wegen, um die Cybersicherheit von Produkten und Dienstleistungen, die vorhandene Cyberinfrastrukturen unterstützen, nicht nur aufrechtzuerhalten, sondern auch zu erhöhen
8	Schaffung von Anreizen für den Privatsektor, in Sicherheitsvorkehrungen zu investieren	▶ Ermittlung möglicher Anreize für private Unternehmen, in Sicherheitsvorkehrungen zu investieren ▶ Anreize für Unternehmen, Sicherheitsinvestitionen zu fördern
9	Schutz der kritischen Informationsinfrastruktur, OES und DSP (CII)	▶ Ermittlung von kritischer Informationsinfrastruktur ▶ Ermittlung und Minderung relevanter Risiken für CII
10	Bekämpfung der Cyberkriminalität	▶ Schaffung von Gesetzen im Bereich der Cyberkriminalität ▶ Steigerung der Leistungsfähigkeit von Strafverfolgungsbehörden
11	Einrichtung von Mechanismen zur Meldung von Vorfällen	▶ Erlangung von Kenntnissen über die gesamte Bedrohungsumgebung ▶ Bewertung der Auswirkungen von Vorfällen (z. B. Sicherheitsverletzungen, Netzwerkausfälle, Dienstunterbrechungen) ▶ Erlangung von Kenntnissen über bestehende und neue Schwachstellen und Arten von Angriffen ▶ Entsprechende Aktualisierung der Sicherheitsvorkehrungen ▶ Umsetzung der Bestimmungen der NIS-Richtlinie zur Meldung von Vorfällen
12	Stärkung des Schutzes der Privatsphäre und des Datenschutzes	▶ Beitrag zur Stärkung der Grundrechte auf Privatsphäre und Datenschutz.
13	Aufbau einer öffentlich-privaten Partnerschaft (PPP)	▶ Abschrecken (um Angreifer abzuschrecken) ▶ Schützen (nutzt die Erforschung neuer Sicherheitsbedrohungen)

ID	Strategische Ziele der NCSS	Ziele
		▶ Erkennen (verwendet den Informationsaustausch, um neuen Bedrohungen zu begegnen) ▶ Reagieren (um die Fähigkeit zu liefern, mit den anfänglichen Auswirkungen eines Vorfalls fertig zu werden) ▶ Wiederherstellung (um die Fähigkeit zu liefern, die schlussendlichen Auswirkungen eines Vorfalls zu beheben)
14	**Institutionalisierung der Zusammenarbeit zwischen öffentlichen Stellen**	▶ Intensivierung der Zusammenarbeit zwischen öffentlichen Stellen mit Verantwortlichkeiten und Kompetenzen im Zusammenhang mit der Cybersicherheit ▶ Vermeidung einer Überschneidung von Kompetenzen und Ressourcen zwischen öffentlichen Stellen ▶ Verbesserung und Institutionalisierung der Zusammenarbeit zwischen öffentlichen Stellen in verschiedenen Bereichen der Cybersicherheit
15	**Internationale Zusammenarbeit (nicht nur mit EU-Mitgliedstaaten)**	▶ Nutzung des Vorteils der Schaffung einer gemeinsamen Wissensbasis zwischen den EU-Mitgliedstaaten ▶ Schaffung von Synergieeffekten zwischen den nationalen Cybersicherheitsbehörden ▶ Ermöglichen und Verstärken des Kampfes gegen grenzüberschreitende Kriminalität

2.2.2 Zusätzliche strategischen Ziele

Basierend auf den durchgeführten Schreibtischstudien und den von der ENISA durchgeführten Befragungen wurden zusätzliche strategische Ziele ermittelt. Die Mitgliedstaaten befassen sich zunehmend mit diesen Themen in ihren NCSS oder definieren Aktionspläne zu demselben Thema. Beispiele für von den Mitgliedstaaten durchgeführte Aktivitäten werden ebenfalls genannt. Wenn ein Beispiel aus einer öffentlich zugänglichen Quelle stammt, wird ein Quellenverweis angegeben. In Fällen, in denen Beispiele auf vertraulichen Befragungen von Beamten der EU-Mitgliedstaaten beruhen, werden keine Verweise angegeben.

Folgende zusätzliche strategische Ziele wurden ermittelt:

- Verbesserung der Cybersicherheit der Lieferkette
- Sicherung der digitalen Identität und Aufbau von Vertrauen in digitale öffentliche Dienste

Verbesserung der Cybersicherheit der Lieferkette

Kleine und mittlere Unternehmen (KMU) sind das Rückgrat der Wirtschaft Europas. Sie repräsentieren 99 % aller Unternehmen in der EU.[14] Schätzungen zufolge haben KMU im Jahr 2015 rund 85 % der neuen Arbeitsplätze geschaffen und zwei Drittel der gesamten Beschäftigung des Privatsektors in der EU bereitgestellt. Da KMU Dienstleistungen für große Unternehmen erbringen und zunehmend mit öffentlichen Verwaltungen zusammenarbeiten[15], muss außerdem beachtet werden, dass KMU im heutigen Verbundnetz in Bezug auf Cyberangriffe das schwache Glied darstellen. KMU sind am stärksten Cyberangriffen ausgesetzt, können es sich jedoch häufig nicht leisten, angemessen in Cybersicherheit zu investieren.[16] Die Verbesserung der Cybersicherheit der Lieferkette sollte daher mit Schwerpunkt auf KMU erfolgen.

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16] https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study

Zusätzlich zu diesem systemischen Ansatz können die Mitgliedstaaten auch die Bemühungen um die Cybersicherheit bestimmter IKT-Dienste und -Produkte erhöhen, die als wesentlich angesehen werden: IKT-Technologien für kritische Informationsinfrastrukturen, im Telekommunikationssektor erzwungene Sicherheitsmechanismen (Kontrollen auf ISP-Ebene usw.), Vertrauensdienste gemäß Definition in der eIDAS-Verordnung und Cloud-Diensteanbieter. Beispielsweise hat sich Polen in seiner nationalen Cybersicherheitsstrategie von 2019-2024[17] verpflichtet, ein nationales Bewertungs- und Zertifizierungssystem für Cybersicherheit als Mechanismus zur Qualitätssicherung in der Lieferkette zu entwickeln. Dieses Zertifizierungssystem wird an den EU-Zertifizierungsrahmen für digitale IKT-Produkte, -Dienstleistungen und -Prozesse angepasst, der im EU-Rechtsakt zur Cybersicherheit (2019/881) festgelegt ist.

Die Verbesserung der Cybersicherheit der Lieferkette ist daher von größter Bedeutung. Dies kann erreicht werden, indem unter anderem klare Leitlinien zur Förderung von KMU festgelegt, Leitlinien für Cybersicherheitsanforderungen in Beschaffungsverfahren der öffentlichen Verwaltung bereitgestellt, die Zusammenarbeit im Privatsektor gefördert, PPP aufgebaut, Mechanismen zur koordinierten Offenlegung von Sicherheitslücken (CVD)[18] gefördert und Produktzertifizierungssysteme, einschließlich Cybersicherheitskomponenten bei digitalen Initiativen für KMU, und Finanzierungkompetenzen entwickelt werden.

Sicherung der digitalen Identität und Aufbau von Vertrauen in digitale öffentliche Dienste

Im Februar 2020 hat die Kommission ihre Vision für die digitale Transformation der EU in der Mitteilung „Gestaltung der digitalen Zukunft Europas“[19] mit dem Ziel dargelegt, integrative Technologien bereitzustellen, die für die Menschen funktionieren und die Grundwerte der EU respektieren. In der Mitteilung heißt es insbesondere, dass die Förderung der digitalen Transformation öffentlicher Verwaltungen in ganz Europa von entscheidender Bedeutung ist. In diesem Sinne ist es von größter Bedeutung, Vertrauen in den Staat in Bezug auf die digitale Identität und öffentliche Dienstleistungen aufzubauen. Dies ist umso wichtiger, wenn man bedenkt, dass Transaktionen und Datenaustausch im öffentlichen Sektor häufig sensibler Natur sind.

Viele Länder haben ihre Absicht zum Ausdruck gebracht, dieses Thema in ihrer NCSS anzusprechen, wie zum Beispiel: Dänemark, Estland, Frankreich, Luxemburg, Malta, die Niederlande, Spanien und das Vereinigte Königreich. Einige dieser Länder haben auch zum Ausdruck gebracht, dass dieses strategische Ziel als Teil eines umfassenderen Plans angegangen werden könnte:

- Estland verknüpft den dazugehörigen Aktionsplan zum Thema „Sicherheit der elektronischen Identität und Fähigkeit zur elektronischen Authentifizierung“ mit der umfassenderen digitalen Agenda 2020 für Estland.
- In der französischen NCSS heißt es, dass der für digitale Technologie zuständige Außenminister die Erstellung eines Fahrplans überwacht, um das digitale Leben, die Privatsphäre und die personenbezogenen Daten des französischen Volkes zu schützen.
- In der niederländischen NCSS heißt es, dass die Cybersicherheit in öffentlichen Verwaltungen sowie bei öffentlichen Dienstleistungen für Bürger und Unternehmen in der umfassenden digitalen Agenda der Regierung ausführlicher erörtert wird.

[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Gestaltung der digitalen Zukunft Europas, COM(2020) 67 final: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_de.pdf

- Da die britische Regierung weiterhin verstärkt ihre Dienste online stellt, hat sie eine Regierungsdienststelle für Digitalisierung (Government Digital Service, GDS) eingerichtet, um sicherzustellen, dass alle neuen digitalen Dienste, die von staatlicher Seite erstellt oder bereitgestellt werden, mit Unterstützung des Britischen Nationalen Cybersicherheitszentrums (NCSC) „sicher durch Voreinstellungen“ sind.

2.2.3 Berücksichtigung anderer strategischer Ziele

Während der Phase der Schreibtischstudie im Rahmen der von der ENISA durchgeführten Befragungen wurden weitere strategische Ziele untersucht. Es wurde jedoch beschlossen, dass diese Ziele nicht Teil des Selbstbewertungsrahmens sind. ANHANG C – Weitere untersuchte Ziele

bietet Definitionen für jedes dieser Ziele, die verwendet werden können, um zukünftige Diskussionen über mögliche NCSS-Verbesserungen anzuregen.

Die folgenden strategischen Ziele wurden untersucht, um in der Zukunft in Erwägung gezogen zu werden:

- Entwicklung branchenspezifischer Cybersicherheitsstrategien
- Kampf gegen Desinformationskampagnen
- Sichere Spitzentechnologien (5G, KI, Quanteninformatik usw.)
- Sicherstellung der Datensouveränität
- Schaffung von Anreizen für die Entwicklung der Cyber-Versicherungsbranche.

2.3 WICHTIGE ERKENNTNISSE AUS DER BENCHMARK-ÜBUNG

Die Schreibtischstudie zu bestehenden Reifegradmodellen im Zusammenhang mit Cybersicherheit wurde mit dem Ziel durchgeführt, Informationen und Nachweise zu sammeln, um die Gestaltung des Rahmens zur Selbstbewertung nationaler Fähigkeiten im Bereich NCSS zu unterstützen. In diesem Zusammenhang wurde eine umfassende Literaturrecherche bestehender Modelle durchgeführt, um die Ergebnisse der ersten in den Abschnitten 2.1 und 2.2 entwickelten Rahmenuntersuchungen zu Reifegradmodellen für Cybersicherheit und der bestehenden NCSS zu ergänzen. Diese systematische Überprüfung unterstützt die Auswahl und Begründung des Reifegrads des Bewertungsrahmens sowie die Definition der verschiedenen Dimensionen und Indikatoren.

Im Rahmen der systematischen Überprüfung von Reifegradmodellen wurden 10 Modelle auf der Grundlage ihrer Hauptmerkmale ausgewählt und analysiert. Der allgemeine Überblick über die Hauptmerkmale für jedes im Rahmen dieser Studie überprüfte Modell ist in Tabelle 2: Übersicht über die analysierten Reifegradmodelleverfügbar, und eine detailliertere Analyse finden Sie in ANHANG A.

Tabelle 2: Übersicht über die analysierten Reifegradmodelle

Bezeichnung des Modells	Anzahl der Reifegrad stufen	Anzahl der qualitativen Merkmale	Bewertungsmethode	Ergebnisdarstell ung
Reifegradmodell für Cybersicherheitskapazitäten für Nationen (CMM)	5	5 Hauptdime nsionen	Zusammenarbeit mit einer lokalen Organisation zur Feinabstimmung des Modells, bevor es im nationalen Kontext angewendet wird	5-Stufen-Radar

Reifegradmodell für Cybersicherheitskapazitäten (C2M2)	4	10 Hauptbereiche	Selbstbewertungsmethode und -instrumentarium	Bewertungskarte mit Kreisdiagrammen
Rahmen zur Verbesserung der Cybersicherheit kritischer Infrastrukturen	Nicht zutreffend (4 Stufen)	5 Hauptfunktionen	Selbstbewertung	Nicht zutreffend
Reifegradmodell für Cybersicherheitskapazitäten von Katar (Q-C2M2)	5	5 Hauptbereiche	Nicht zutreffend	Nicht zutreffend
Zertifizierung des Reifegradmodells für Cybersicherheit (CMMC)	5	17 Hauptbereiche	Bewertung durch externe Prüfer	Nicht zutreffend
Das Community-Reifegradmodell für Cybersicherheit (CCSMM)	5	6 Hauptdimensionen	Bewertung innerhalb von Gemeinschaften mit Beiträgen von Strafverfolgungsbehörden der Bundesstaaten und des Bundes	Nicht zutreffend
Reifegradmodell für Informationssicherheit für das NIST-Cybersicherheitsregelwerk (ISMM)	5	23 bewertete Bereiche	Nicht zutreffend	Nicht zutreffend
Modell für interne Auditstellen (IA-CM) für den öffentlichen Sektor	5	6 Elemente	Selbstbewertung	Nicht zutreffend
Der Globale Cybersicherheitsindex (GCI)	Nicht zutreffend	5 Säulen	Selbstbewertung	Rangliste
Der Cyber Power Index (CPI)	Nicht zutreffend	4 Kategorien	Vergleich durch die Economist Intelligence Unit	Rangliste

Diese systematische Überprüfung ermöglichte es, Schlussfolgerungen zu bewährten Verfahren zu ziehen, die in bestehende Modelle übernommen wurden, um die Entwicklung des konzeptionellen Modells für das aktuelle Reifegradmodell zu unterstützen. Die Benchmark-Übung unterstützte insbesondere die Definition der Reifegrade, die Erstellung von Dimensionsclustern und die Auswahl von Indikatoren sowie eine geeignete Visualisierungsmethode für die Ergebnisse des Modells. Die relevantesten Ergebnisse für jedes dieser Elemente sind in Tabelle 3 aufgeführt.

Tabelle 3: Schlüsselerkenntnisse aus der Vergleichsübung

Merkmal	Schlüsselerkenntnis
Reifegrade	▶ Eine fünfstufige Reifegradskala für den Rahmen zur Bewertung von Cybersicherheitsfähigkeiten wird allgemein akzeptiert und kann detaillierte Bewertungsergebnisse liefern (siehe Tabelle 6 Vergleich der Reifegrade für eine ausführliche Ansicht der Definition der Reifegrade für jedes Modell; ▶ Alle Modelle bieten eine allgemeine Definition jedes Reifegrads, die dann an die verschiedenen Dimensionen oder Cluster von Dimensionen angepasst wird; ▶ Bei der Messung der Reife von Cybersicherheitsfähigkeiten werden in der Regel zwei Hauptaspekte bewertet: Die Reife von Strategien und die Reife von Prozessen, die zur Implementierung von Strategien eingerichtet wurden.
Qualitative Merkmale	▶ Die vergleichende Analyse der qualitativen Merkmale der vorhandenen Reifegradmodelle zeigt heterogene Ergebnisse mit einer durchschnittlichen Anzahl von qualitativen Merkmalen pro Modell zwischen vier und fünf;

	▶ Ein Modell, das auf etwa vier oder fünf qualitativen Merkmalen beruht, bietet den Ländern die richtige Datengranularität, indem relevante Dimensionen zusammengefasst und die Lesbarkeit der Ergebnisse sichergestellt werden. (Tabelle 7: Vergleich von Attributen/Dimensionen liefert eine Beschreibung der qualitativen Merkmale für jedes Modell); ▶ Das Schlüsselprinzip, das alle Modelle bei der Definition der Cluster anwenden, basiert auf der Konsistenz der in jedem Cluster gruppierten Elemente.
Bewertungsmethode	▶ Die Bewertungsmethoden, die in den verschiedenen analysierten Modellen verwendet werden, sind unterschiedlich; ▶ Die gebräuchlichste Bewertungsmethode basiert auf der Selbstbewertung.
Ergebnisdarstellung	▶ Es ist wichtig, die Ergebnisse auf verschiedenen Granularitätsstufen darzustellen; ▶ Die Visualisierungsmethode sollte selbsterklärend und leicht zu lesen sein.

Das konzeptionelle Modell wurde basierend auf dem Benchmarking der verschiedenen Reifegradmodelle sowie auf früheren Arbeiten der ENISA erstellt. Außerdem wurde beschlossen, auf dem *interaktiven Online-Tool der ENISA* aufzubauen, um Reifegradindikatoren zu entwickeln, die für jedes qualitative Merkmal verwendet werden.

2.4 HERAUSFORDERUNGEN DER NCSS-BEWERTUNG

Die Mitgliedstaaten stehen beim Aufbau von Cybersicherheitsfähigkeiten vor vielen Herausforderungen, insbesondere wenn sie sicherstellen wollen, dass ihre Fähigkeiten auf dem neuesten Stand der Entwicklung sind. Nachfolgend finden Sie eine Zusammenfassung der Herausforderungen, die von den Mitgliedstaaten im Rahmen dieser Studie ermittelt und mit ihnen erörtert wurden:

- **Schwierigkeiten bei der Koordinierung und Zusammenarbeit:** Die Koordinierung der Cybersicherheitsbemühungen auf nationaler Ebene, um eine effiziente Antwort auf Cybersicherheitsprobleme zu erhalten, kann sich aufgrund der hohen Anzahl der beteiligten Interessenträger als Herausforderung erweisen.
- **Fehlende Ressourcen für die Durchführung der Bewertung:** Abhängig vom lokalen Kontext und der nationalen Governance-Struktur für Cybersicherheit kann die Bewertung der NCSS und ihrer Ziele mehr als 15 Personentage in Anspruch nehmen.
- **Mangelnde Unterstützung für die Entwicklung von Cybersicherheitsfähigkeiten:** Einige Mitgliedstaaten teilten mit, dass sie zunächst eine Evaluierungsphase durchführen müssen, um Lücken und Grenzen zu ermitteln, um Haushaltsmittel begründen und Unterstützung bei der Entwicklung von Cybersicherheitsfähigkeiten erhalten zu können.
- **Schwierigkeiten bei der Zuordnung von Erfolgen oder Änderungen der Strategie:** Da sich Bedrohungen jeden Tag weiterentwickeln und sich die Technologie verbessert, müssen die Aktionspläne ständig entsprechend angepasst werden. Die Bewertung einer NCSS und die Zuordnung von Änderungen zur Strategie selbst bleiben jedoch eine schwierige Aufgabe. Dies wiederum erschwert die Ermittlung der Grenzen und Mängel der NCSS.
- **Schwierigkeiten bei der Messung der Wirksamkeit der NCSS:** Parameter können gesammelt werden, um verschiedene Bereiche wie Fortschritt, Umsetzung, Reife und Wirksamkeit zu messen. Während die Messung von Fortschritt und Umsetzung im Vergleich zur Messung der Wirksamkeit relativ einfach ist, bleibt letztere für die Bewertung der Ergebnisse und Auswirkungen einer NCSS aussagekräftiger. Im Rahmen der von der ENISA durchgeführten Befragungen haben zahlreiche Mitgliedstaaten angegeben, dass die quantitative Messung der Wirksamkeit einer NCSS wichtig ist, aber auch eine sehr anspruchsvolle Aufgabe darstellt, die in einigen Fällen nicht zu bewerkstelligen ist.

- **Schwierigkeiten bei der Annahme eines gemeinsamen Rahmens:** Die EU-Mitgliedstaaten agieren in unterschiedlichen Kontexten in Bezug auf Politik, Organisationen, Kultur, Gesellschaftsstruktur und NCSS-Reife. Bestimmte, im Rahmen dieser Studie befragte Mitgliedstaaten äußerten, dass es sich als schwierig erweisen könnte, einen für alle gleichen Selbstbewertungsrahmen zu rechtfertigen und anzuwenden.

2.5 VORTEILE EINER BEWERTUNG DER NATIONALEN FÄHIGKEITEN

Seit 2017 verfügen alle EU-Mitgliedstaaten über eine NCSS.[20] Obwohl dies eine positive Entwicklung ist, ist es auch wichtig, dass die Mitgliedstaaten in der Lage sind, diese NCSS angemessen zu bewerten, um so einen Mehrwert für ihre strategische Planung und Umsetzung zu erzielen.

Eines der Ziele des Rahmens zur Bewertung nationaler Fähigkeiten ist die Bewertung der Cybersicherheitsfähigkeiten auf der Grundlage der in den verschiedenen NCSS festgelegten Prioritäten. Grundsätzlich bewertet der Rahmen den Reifegrad der Cybersicherheitsfähigkeiten der Mitgliedstaaten in den durch die NCSS-Ziele festgelegten Bereichen. Die Ergebnisse des Rahmens unterstützen somit die politischen Entscheidungsträger der Mitgliedstaaten bei der Festlegung der nationalen Strategie zur Cybersicherheit, indem sie ihnen Erkenntnisse über den aktuellen Stand in den Ländern zur Verfügung stellen.[21] Der NCAF soll den Mitgliedstaaten letztendlich helfen, Verbesserungsbereiche zu identifizieren und Kapazitäten aufzubauen.

Der Rahmen zielt darauf ab, den Mitgliedstaaten eine Selbstbewertung ihres Reifegrads durch Bewertung ihrer NCSS-Ziele zu ermöglichen, die ihnen helfen wird, die Cybersicherheitsfähigkeiten sowohl auf strategischer als auch auf operativer Ebene zu verbessern und auszubauen.

Auf der Grundlage der von der ENISA durchgeführten Befragungen mehrerer für den Bereich Cybersicherheit zuständiger Stellen in verschiedenen Mitgliedstaaten wurden anhand eines praktischeren Ansatzes die folgenden Vorteile des Rahmens für die Bewertung von nationalen Fähigkeiten ermittelt und unterstrichen:

- Bereitstellung nützlicher Informationen zur Entwicklung einer langfristigen Strategie (z. B. bewährte Verfahren, Leitlinien);
- Hilfestellung bei der Ermittlung fehlender Elemente in der NCSS;
- Hilfestellung beim weiteren Ausbau der Cybersicherheitskapazitäten;
- Stärkung der Rechenschaftspflicht für politische Maßnahmen;
- Vermittlung von Glaubwürdigkeit gegenüber der Öffentlichkeit und internationalen Partnern;
- Unterstützung der Öffentlichkeitsarbeit und Verbesserung der öffentlichen Wahrnehmung als transparente Organisation;
- Hilfestellung bei der Antizipierung künftiger Probleme;
- Hilfestellung bei der Ermittlung der gewonnenen Erkenntnisse und bewährten Verfahren;
- Bereitstellung einer Basis für die Cybersicherheitskapazitäten in der gesamten EU, um Diskussionen zu erleichtern;
- Hilfestellung bei der Bewertung der nationalen Fähigkeiten in Bezug auf Cybersicherheit.

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). The interface between evaluation and public policy. Evaluation, 5(4), 468-486.

3. METHODIK DES RAHMENS ZUR BEWERTUNG NATIONALER FÄHIGKEITEN

3.1 ALLGEMEINER ZWECK

Das **Hauptziel** des NCAF besteht darin, den Reifegrad der Cybersicherheitsfähigkeiten der **Mitgliedstaaten** zu messen, um diese bei der Bewertung ihrer nationalen Cybersicherheitsfähigkeiten zu unterstützen, das Bewusstsein für den Reifegrad des Landes zu schärfen, Verbesserungsmöglichkeiten zu ermitteln und Cybersicherheitskapazitäten aufzubauen.

3.2 REIFEGRADE

Der Rahmen basiert auf **fünf Reifegradstufen,** in denen die Phasen festgelegt sind, die die Mitgliedstaaten beim Aufbau von Cybersicherheitskapazitäten in dem von jedem NCSS-Ziel abgedeckten Bereich durchlaufen. Die Reifegrade stellen die zunehmende Reife dar, beginnend mit **Grad 1** (die Mitgliedstaaten verfügen über kein klar definiertes Konzept für den Aufbau von Cybersicherheitskapazitäten in den von den NCSS-Zielen abgedeckten Bereichen) bis **Grad 5** (Strategie zum Aufbau der Cybersicherheitskapazitäten ist dynamisch und fähig, sich an Umweltentwicklungen anzupassen). Tabelle 4 zeigt die Skala der Reifegrade mit einer Beschreibung jeder Reifegradstufe.

Tabelle 4: Die fünfstufige Reifegradskala des ENISA-Rahmens zur Bewertung nationaler Fähigkeiten

GRAD 1 – ERSTE SCHRITTE / AD HOC	GRAD 2 – FRÜHE DEFINITION	GRAD 3 – ETABLIERUNG	GRAD 4 – OPTIMIERUNG	GRAD 5 – ANPASSUNGSFÄHIGKEIT
Der Mitgliedstaat hat in den von den NCSS-Zielen abgedeckten Bereichen kein klar definiertes Konzept für den Aufbau von Cybersicherheitskapazitäten. Dennoch könnte das Land einige allgemeine Ziele haben und einige Studien (technisch, politisch, regulatorisch) durchgeführt haben, um die nationalen Fähigkeiten zu verbessern.	Das nationale Konzept für den Kapazitätenaufbau in dem von den NCSS-Zielen abgedeckten Bereich wurde definiert. Die Aktionspläne oder Aktivitäten zur Erreichung der Ergebnisse sind bereits in einem frühen Stadium vorhanden. Darüber hinaus wurden möglicherweise aktive Interessenträger identifiziert und/oder eingeschaltet.	Der Aktionsplan für den Kapazitätenaufbau in dem von den NCSS-Zielen abgedeckten Bereich ist klar definiert und wird von den entsprechenden Interessenträgern unterstützt. Die Verfahren und Aktivitäten werden auf nationaler Ebene einheitlich durchgesetzt und implementiert. Die Aktivitäten werden mit einer klaren Ressourcenzuweisung und Governance sowie einer Reihe von Fristen definiert und dokumentiert.	Der Aktionsplan wird regelmäßig bewertet: Er ist priorisiert, optimiert und nachhaltig. Die Leistung beim Aufbau von Cybersicherheitskapazitäten wird regelmäßig gemessen. Erfolgsfaktoren, Herausforderungen und Lücken bei der Implementierung von Aktivitäten werden identifiziert.	Die Strategie zum Aufbau von Cybersicherheitskapazitäten ist dynamisch und anpassungsfähig. Die ständige Beachtung der Umgebungsentwicklungen (technologischer Fortschritt, globaler Konflikt, neue Bedrohungen usw.) fördert eine schnelle Entscheidungsfähigkeit und die Fähigkeit, schnell mit Verbesserungen zu reagieren.

3.3 CLUSTER & ÜBERGREIFENDE STRUKTUR DES SELBSTBEWERTUNGSRAHMENS

Der Selbstbewertungsrahmen ist durch **vier Cluster** gekennzeichnet: (I) Governance und Standards im Bereich der Cybersicherheit, (II) Kapazitätenaufbau und Sensibilisierung, (III) Gesetze und Bestimmungen und (IV) Zusammenarbeit. Jeder dieser Cluster deckt einen wichtigen Themenbereich für den Aufbau von Cybersicherheitskapazitäten in einem Land ab und enthält einen Pool verschiedener Ziele, die die Mitgliedstaaten möglicherweise in ihre NCSS aufnehmen. Diese sind:

- **(I) Governance und Standards im Bereich der Cybersicherheit**: Dieser Cluster misst die Fähigkeit der Mitgliedstaaten, eine angemessene Governance, Standards und bewährte Verfahren im Bereich Cybersicherheit festzulegen. Diese Dimension berücksichtigt verschiedene Aspekte der Cyberabwehr und der Widerstandsfähigkeit (Resilienz) und unterstützt gleichzeitig die Entwicklung der nationalen Cybersicherheitsbranche und die Vertrauensbildung in den Staat.
- **(II) Kapazitätenaufbau und Sensibilisierung:** In diesem Cluster wird die Fähigkeit der Mitgliedstaaten bewertet, das Bewusstsein für Cybersicherheitsrisiken und -bedrohungen und deren Bekämpfung zu schärfen. Darüber hinaus misst diese Dimension die Fähigkeit des Landes, kontinuierlich Cybersicherheitsfähigkeiten auszubauen und das allgemeine Niveau an Kenntnissen und Kompetenzen in diesem Bereich zu verbessern. Es befasst sich mit der Entwicklung des Cybersicherheitsmarktes und den Fortschritten in Forschung und Entwicklung im Bereich der Cybersicherheit. In diesem Cluster werden alle Ziele zusammengefasst, die die Grundlage für den Aufbau von Kapazitäten bilden.
- **(III) Gesetze und Bestimmungen**: Dieser Cluster misst die Fähigkeit der Mitgliedstaaten, die erforderlichen gesetzlichen und rechtlichen Instrumente einzurichten, um der Zunahme von Cyberkriminalität und damit verbundenen Cybervorfällen zu begegnen und entgegenzuwirken sowie kritische Informationsinfrastrukturen zu schützen. Darüber hinaus wird in dieser Dimension auch die Fähigkeit der Mitgliedstaaten bewertet, einen Rechtsrahmen zum Schutz von Bürgern und Unternehmen zu schaffen, wie beispielsweise im Fall der Vereinbarkeit von Sicherheit und Datenschutz.
- **(IV) Zusammenarbeit:** In diesem Cluster wird die Zusammenarbeit und der Informationsaustausch zwischen verschiedenen Interessenträgern auf nationaler und internationaler Ebene als wichtiges Instrument zum besseren Verständnis und zur Reaktion auf ein sich ständig änderndes Bedrohungsumfeld bewertet.

Die Ziele, die in das Modell aufgenommen wurden, werden von den Mitgliedstaaten üblicherweise angenommen und wurden aus den im Abschnitt 2.2 aufgeführten Zielen ausgewählt. Das Modell bewertet insbesondere die folgenden Ziele:

- 1. Entwicklung von nationalen Cybernotfallplänen (I)
- 2. Festlegung grundlegender Sicherheitsvorkehrungen (I)
- 3. Sicherung der digitalen Identität und Aufbau von Vertrauen in digitale öffentliche Dienste (I)
- 4. Einrichtung einer Kapazität zur Reaktion auf Sicherheitsvorfälle (II)
- 5. Sensibilisierung der Benutzer (II)
- 6. Organisation von Cybersicherheitsübungen (II)
- 7. Stärkung von Schulungs-, Ausbildungs- und Bildungsprogrammen (II)
- 8. Förderung von F&E (II)
- 9. Schaffung von Anreizen für den privaten Sektor, in Sicherheitsvorkehrungen zu investieren (II)
- 10. Verbesserung der Cybersicherheit der Lieferkette (II)
- 11. Schutz der kritischen Informationsinfrastruktur, OES und DSP (III)
- 12. Bekämpfung der Cyberkriminalität (III)
- 13. Einrichtung von Mechanismen zur Meldung von Vorfällen (III)
- 14. Stärkung des Schutzes der Privatsphäre und des Datenschutzes (III)
- 15. Institutionalisierung der Zusammenarbeit zwischen öffentlichen Stellen (IV)
- 16. Internationale Zusammenarbeit (IV)

- 17. Aufbau einer öffentlich-privaten Partnerschaft (IV)

Die vier Cluster und zugrunde liegenden Ziele werden im Modell kombiniert, um eine ganzheitliche Sicht auf die Reife der Cybersicherheitsfähigkeiten der Mitgliedstaaten zu erhalten. Abbildung 1 stellt die übergreifende Struktur des Selbstbewertungsrahmens vor und zeigt, wie diese Elemente, nämlich Ziele, Cluster und Selbstbewertungsrahmen, mit der Bewertung der Leistung eines Landes verknüpft sind.

Abbildung 1: Rahmenstruktur für die Selbstbewertung

Für jedes im Selbstbewertungsrahmen enthaltene Ziel gibt es eine Reihe von Indikatoren, die auf die fünf Reifegrade verteilt sind. Jeder Indikator basiert auf einer geschlossenen Frage (Ja/Nein). Der Indikator kann erforderlich oder nicht erforderlich sein.

3.4 BEWERTUNGSSCHEMA

Im **Bewertungsschema** des Selbstbewertungsrahmens werden die oben genannten Elemente und die in Abschnitt 3.5 aufgeführten Grundsätze berücksichtigt. Tatsächlich liefert das Modell eine Wertung basierend auf dem Wert von zwei Parametern, dem **Reifegrad** und der **Abdeckungsquote**. Jeder dieser Parameter kann auf verschiedenen Ebenen berechnet werden: (i) pro Ziel, (ii) pro Zielcluster oder (iii) allgemein.

Wertung auf Zielebene

Die **Reifegradwertung** gibt einen Überblick über den Reifegrad und zeigt, welche Fähigkeiten und Verfahren eingeführt wurden. Bei der Reifegradwertung wird die höchste Stufe erreicht, wenn der Befragte alle Anforderungen erfüllt (d. h. auf alle erforderlichen Fragen mit JA geantwortet hat) und zusätzlich bereits alle Anforderungen der vorherigen Reifegrade erfüllt hat.

Die **Abdeckungsquote** gibt an, inwieweit alle Indikatoren abgedeckt sind, für die mit JA geantwortet wurde, unabhängig vom Grad der Abdeckung. Dies ist ein komplementärer Wert, der alle Indikatoren berücksichtigt, die ein Ziel messen. Die Abdeckungsquote wird berechnet

als das Verhältnis zwischen der Gesamtzahl der Fragen innerhalb des Ziels und der Anzahl der Fragen, die mit JA beantwortet wurden.

Hier ist anzumerken, dass im übrigen Dokument der Begriff **Ergebnis** verwendet wird, wenn es sowohl um den Wert des Reifegrads als auch um die Abdeckungsquote geht.

Abbildung 2 – Das Bewertungsschema pro Ziel bietet eine Visualisierung der in Abschnitt 3.1 beschriebenen Bewertungsfunktion, die im Folgenden weiter ausgeführt wird.

Abbildung 2: Bewertungsschema pro Ziel

Abbildung 2 zeigt ein Beispiel dafür, wie der Reifegrad pro Ziel berechnet wird. Es ist anzumerken, dass der Befragte alle Anforderungen der ersten drei Reifegrade erfüllt hat und diejenigen der Reifegradstufe 4 nur teilweise erfüllt hat. Daher zeigt das Ergebnis, dass der ***Reifegrad des Befragten für das Ziel „Cybersicherheitsübung organisieren“ bei Stufe 3 liegt.***

In dem in Abbildung 2dargestellten Beispiel kann der Reifegrad des Ziels jedoch nicht die Informationen erfassen, die von den Indikatoren bereitgestellt werden, die eine positive Wertung aufweisen und über Stufe 3 liegen. In diesem Fall kann die Abdeckungsquote einen Überblick über alle Elemente geben, die der Befragte umgesetzt hat, um dieses Ziel trotz seines tatsächlichen Reifegrads zu erreichen. In diesem Fall ist das Verhältnis zwischen der Gesamtzahl der Fragen innerhalb des Ziels und der Anzahl der Fragen, auf die mit JA geantwortet wurde, gleich 19/27, d. h. ***der Wert der Abdeckungsquote liegt bei 70 %****.*

Um außerdem den Besonderheiten der Mitgliedstaaten Rechnung zu tragen und gleichzeitig einen einheitlichen Überblick zu ermöglichen, wird die Wertung aus zwei verschiedenen Stichproben auf Cluster- und Gesamtebene berechnet:

- **Allgemeine Ergebnisse:** Eine vollständige Stichprobe, die alle im Cluster oder im Gesamtrahmen enthaltenen Ziele abdeckt (von 1 bis 17);
- **Spezifische Ergebnisse:** Eine spezifische Stichprobe, die nur die vom Mitgliedstaat ausgewählten Ziele (in der Regel entsprechen diese den in der NCSS des jeweiligen

Landes enthaltenen Zielen) innerhalb des Clusters oder innerhalb des Gesamtrahmens abdeckt.

Wertung auf Cluster-Ebene

Der **allgemeine Reifegrad jedes Clusters** wird als arithmetisches Mittel des Reifegrads aller Ziele innerhalb dieses Clusters berechnet.

Der **spezifische Reifegrad jedes Clusters** wird als arithmetisches Mittel des Reifegrads der Ziele innerhalb dieses Clusters berechnet, für die der Mitgliedstaat eine Bewertung abgegeben hat (in der Regel entsprechen diese Ziele den in der NCSS des jeweiligen Landes enthaltenen Zielen).

Abbildung 1 zeigt beispielsweise, dass Cluster (I) Governance und Standards im Bereich der Cybersicherheit aus drei Zielen besteht. Geht man davon aus, dass der Befragte nur die ersten beiden Ziele bewertet hat, nicht jedoch das dritte, und unter der Annahme, dass die ersten beiden Ziele einen Reifegrad von 2 bzw. 4 aufweisen, liegt der Reifegrad des Clusters unter Berücksichtigung aller Ziele bei Stufe 2 (allgemeiner Reifegrad des Clusters (I) = (2+4)/3), während der Reifegrad des Clusters unter Berücksichtigung nur der vom Bewerter ausgewählten spezifischen Ziele Stufe 3 (spezifischer Reifegrad des Clusters (I) = (2+4)/2) beträgt.

Die **allgemeine Abdeckungsquote jedes Clusters** wird berechnet als das Verhältnis zwischen der Gesamtzahl der Fragen innerhalb des Clusters und der Anzahl der Fragen, die mit JA beantwortet wurden.

Die **spezifische Abdeckungsquote jedes Clusters** wird berechnet als das Verhältnis zwischen der Gesamtzahl der Fragen innerhalb des Clusters zu den Zielen, für die der Mitgliedstaat eine Bewertung abgegeben hat (in der Regel entsprechen diese den in der NCSS des jeweiligen Landes enthaltenen Zielen), und der Anzahl der Fragen, die mit JA beantwortet wurden.

Wertung auf Gesamtebene

Der **allgemeine Gesamtreifegrad eines Landes** wird als arithmetisches Mittel des Reifegrads aller Ziele innerhalb des Rahmens von 1 bis 17 berechnet.

Der **spezifische Gesamtreifegrad eines Landes** wird als arithmetisches Mittel des Reifegrads der Ziele innerhalb dieses Rahmens berechnet, für die der Mitgliedstaat eine Bewertung abgegeben hat (in der Regel entsprechen diese Ziele den in der NCSS des jeweiligen Landes enthaltenen Zielen).

Die **allgemeine Gesamtabdeckungsquote eines Landes** wird berechnet als das Verhältnis zwischen der Gesamtzahl der Fragen innerhalb aller Ziele, die im Rahmen enthalten sind, (von 1 bis 17) und der Anzahl der Fragen, die mit JA beantwortet wurden.

Die **spezifische Gesamtabdeckungsquote eines Landes** wird berechnet als das Verhältnis zwischen der Gesamtzahl der Fragen innerhalb der Ziele innerhalb des Rahmens, für die der Mitgliedstaat eine Bewertung abgegeben hat (in der Regel entsprechen diese Ziele den in der NCSS des jeweiligen Landes enthaltenen Zielen), und der Anzahl der Fragen, die mit JA beantwortet wurden.

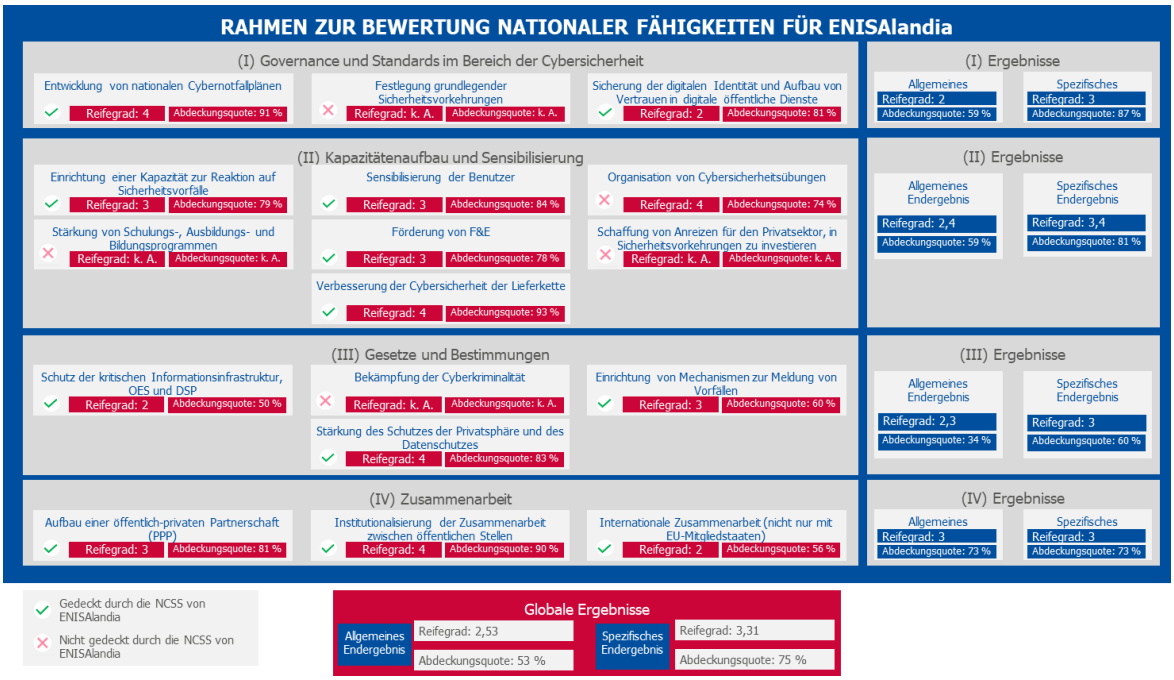
Für jeden Indikator können die Befragten eine dritte Antwortoption („Weiß nicht / nicht zutreffend“) auswählen. In diesem Fall wird der Indikator von der Gesamtberechnung der Ergebnisse ausgeschlossen.

Die Reifegrade auf Cluster- und Gesamtebene werden mit dem arithmetischen Mittel angegeben, um den Fortschritt zwischen zwei Bewertungen anzuzeigen. In der Tat kann die Alternative, die darin besteht, den Cluster- und den Gesamtreifegrad als Reifegrad des am wenigsten ausgereiften Ziels zu berechnen – obwohl dies unter dem Gesichtspunkt der Reife relevant ist – die Fortschritte in Bereichen, die von anderen Zielen abgedeckt werden, nicht berücksichtigen.

Da die Cluster- und die Gesamtebene für Berichtszwecke konsolidiert werden, wurde entschieden, das arithmetische Mittel zu verwenden. Für mehr Genauigkeit verwenden Sie bitte die Ergebnisse auf objektiver Ebene für Berichtszwecke.

Abbildung 3 unten fasst die Bewertungsschemata auf den verschiedenen Ebenen des Modells (Ziel, Cluster, allgemein) zusammen.

Abbildung 3: Gesamtbewertungsschema



3.5 ANFORDERUNGEN AN DEN RAHMEN ZUR SELBSTBEWERTUNG

Der in diesem Abschnitt vorgestellte Rahmen zur Bewertung nationaler Fähigkeiten basiert auf dem von den Mitgliedstaaten genannten Bedarf sowie auf einer Reihe von Anforderungen, die nachstehend aufgeführt sind:

- Der NCAF wird vom Mitgliedstaat als Selbstbewertungsrahmen auf freiwilliger Basis eingesetzt;
- Mit diesem Rahmen sollen die Cybersicherheitsfähigkeiten der Mitgliedstaaten in Bezug auf die 17 Ziele gemessen werden. Der Mitgliedstaat kann jedoch die Ziele auswählen, anhand derer er die Bewertung durchführen möchte, und nur einen Teil der 17 Ziele berücksichtigen;
- Mit dem Selbstbewertungsrahmen soll der Reifegrad der Cybersicherheitsfähigkeiten des Mitgliedstaats gemessen werden;
- Die Ergebnisse der Bewertung werden nur veröffentlicht, wenn der Mitgliedstaat dies von sich aus beschließt;

- Der Mitgliedstaat kann die Bewertungsergebnisse anzeigen lassen und den Reifegrad seiner Cybersicherheitsfähigkeiten, eines Bündels von Zielen oder auch nur eines einzelnen Ziels angeben;
- Alle bewerteten Ziele sind innerhalb des Bewertungsrahmens gleichermaßen relevant und sind daher gleich wichtig. Gleiches gilt für die verwendeten Indikatoren;
- Der Mitgliedstaat kann seine Fortschritte im Zeitverlauf verfolgen.

Der Selbstbewertungsrahmen soll die Mitgliedstaaten beim Aufbau von Cybersicherheitsfähigkeiten unterstützen. Daher enthält er auch eine Reihe von Empfehlungen und Leitlinien, die die europäischen Länder bei der Verbesserung ihres Reifegrads unterstützen sollen.

Hinweis: Diese Empfehlungen bzw. Leitlinien sind allgemeiner Art, stützen sich auf ENISA-Veröffentlichungen und Erkenntnisse anderer Länder und sind von den Ergebnissen der Selbstbewertung abhängig.

4. NCAF-INDIKATOREN

4.1 RAHMENINDIKATOREN

In diesem Abschnitt werden die Indikatoren des ENISA-Rahmens zur Bewertung nationaler Fähigkeiten vorgestellt. Die folgenden Abschnitte sind nach Gruppen unterteilt.

Für jede Gruppe werden in einer Tabelle die alle Indikatoren in Form von Fragen aufgeführt, die für einen bestimmten Reifegrad repräsentativ sind. Der Fragebogen ist das Hauptinstrument für die Selbstbewertung. Für jedes Ziel sind zwei Indikatorensätze zu beachten:

- Eine Fragenreihe zur allgemeinen Reife-Strategie (9 Fragen), die für jeden Reifegrad von „a“ bis „c“ gekennzeichnet sind und für jedes Ziel wiederholt werden,
- und eine Fragenreihe Fragen zur Cybersicherheitskapazität (319 Fragen), die für jeden Reifegrad von „1“ bis „10“ nummeriert sind und sich auf den vom jeweiligen Ziel abgedeckten Bereich beziehen.

Jede Frage wird mit einer Kennung (0-1) versehen, die angibt, ob die Frage ein für den Reifegrad erforderlicher (1) oder nicht erforderlicher (0) Indikator ist.

Jede Frage trägt eine Kennnummer, die sich aus folgenden Elementen zusammensetzt:

- Nummer des Ziels,
- Reifegrad,
- Nummer der Frage

So etwa ist Frage mit der Kennnummer 1.2.4 die vierte Frage im Reifegrad 2 des strategischen Ziels (I) „Entwicklung nationaler Cybernotfallpläne“.

Es ist zu beachten, dass sich die Fragen des gesamten Fragebogens, sofern nicht anders angegeben, auf die nationale Ebene beziehen. In allen Fragen bezieht sich die Anrede „Sie“ allgemein auf den Mitgliedstaat, für den die Bewertung durchgeführt wird, und nicht auf die Person oder staatliche Stelle, die die Bewertung durchführt.

Die Definition jedes Ziels ist zu finden in Kapitel 2.2 – Gemeinsame Ziele innerhalb der europäischen NCSS festgelegt.

4.1.1 Cluster Nr. 1: Governance und Standards im Bereich der Cybersicherheit

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
1 – Entwicklung von nationalen Cybernotfallplänen	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Haben Sie begonnen, nationale Cybernotfallpläne zu erstellen (z. B. Festlegung der allgemeinen Ziele, des Umfangs und/oder der Grundsätze der Notfallpläne)?	1	Haben Sie ein Grundsatzpapier/eine nationale Strategie, worin Cybersicherheit als Krisenfaktor berücksichtigt wird, (d. h. einen Plan, eine Politik o. ä.)?	1	Haben Sie einen Cyberkrisenmanagementplan auf nationaler Ebene?	1	Sind Sie mit der Anzahl oder dem Prozentsatz der kritischen Sektoren zufrieden, die im nationalen Cybernotfallplan enthalten sind?	1	Verfügen Sie über ein Erkenntnisverfahren zur Nachverfolgung von Cyberübungen oder tatsächlichen Krisen auf nationaler Ebene?	1
	2	Ist allgemein bekannt, dass Cybervorfälle einen Krisenfaktor darstellen, der die nationale Sicherheit gefährden könnte?	0	*Haben Sie eine Schaltstelle, um Informationen zu erhalten und Entscheidungsträger zu informieren? D. h. Methoden, Plattformen oder Standorte, um sicherzustellen, dass alle Krisenreaktionsbeteiligten auf dieselben Echtzeitinformationen über die Cyberkrise zugreifen können.*	1	Verfügen Sie über krisenspezifische Cybersicherheitsverfahren auf nationaler Ebene?	1	Organisieren Sie häufig genug Aktivitäten (z. B. Übungen) im Zusammenhang mit der nationalen Cybernotfallplanung im Internet?	1	Verfügen Sie über ein Verfahren, um den nationalen Plan regelmäßig zu testen?	1
	3	Wurden Studien (technisch, operativ, politisch) auf dem Gebiet der Cybernotfallplanung durchgeführt?	0	Werden die maßgeblichen Ressourcen eingesetzt, um die Entwicklung und Durchführung nationaler Cybernotfallpläne zu überwachen?	1	Haben Sie ein Kommunikationsteam, das speziell dafür ausgebildet ist, auf Cyberkrisen zu reagieren und die Öffentlichkeit zu informieren?	1	Haben Sie genügend Mitarbeiter, die sich der Krisenplanung widmen, die gewonnenen Erkenntnisse untersuchen und Veränderungen umsetzen?	1	Haben Sie geeignete Tools und Plattformen, um das Lagebewusstsein zu schärfen?	1
	4	-		Haben Sie eine Methode zur Bewertung von Cyberbedrohungen auf nationaler Ebene, die Verfahren zur Folgenabschätzung umfasst?	0	Binden Sie alle maßgeblichen nationalen Interessenträger ein (nationale Sicherheit, Verteidigung, Zivilschutz, Strafverfolgung, Ministerien, Behörden usw.)?	1	Haben Sie genügend geschulte Mitarbeiter, um auf nationaler Ebene auf Cyberkrisen zu reagieren?	1	Folgen Sie einem bestimmten Reifegradmodell, um den Cybernotfallplan zu überwachen und zu verbessern?	0

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
1 – Entwicklung von nationalen Cybernotfallplänen	5	-		-		Haben Sie angemessene Krisenmanagementeinrichtungen und Lagezentren?	1	-		Verfügen Sie über Ressourcen, die entweder auf die Antizipation von Bedrohungen spezialisiert sind oder an einer potenziellen Cybersicherheit arbeiten, die sich mit künftige Krisen bzw. den Herausforderungen von morgen befassen?	0
	6	-		-		Arbeiten Sie bei Bedarf mit internationalen Interessenträgern in der EU zusammen?	0	-		-	
	7	-		-		Arbeiten Sie bei Bedarf mit internationalen Interessenträgern in Nicht-EU-Ländern zusammen?	0	-		-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5
2 – Festlegung grundlegender Sicherheitsvorkehrungen	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1	
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0					
	1	Haben Sie eine Studie durchgeführt, um Anforderungen und Lücken für **öffentliche** Organisationen auf der Grundlage international anerkannter Standards zu ermitteln (z. B. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS usw.)?	1	Entsprechen die Sicherheitsvorkehrungen internationalen/nationalen Standards?	1	Sind grundlegende Sicherheitsvorkehrungen vorgeschrieben?	1	Gibt es ein Verfahren, um grundlegende Sicherheitsvorkehrungen regelmäßig zu aktualisieren?	1	Verfügen Sie über ein Verfahren, um IKT zu stärken, wenn Vorfälle durch die Maßnahmen nicht berücksichtigt werden?

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5
2 – Festlegung grundlegender Sicherheitsvorkehrungen	2	Haben Sie eine Studie durchgeführt, um Anforderungen und Lücken für **private** Organisationen auf der Grundlage international anerkannter Standards zu ermitteln (z. B. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS usw.)?	1	Werden der Privatsektor und andere Interessenträger bei der Festlegung grundlegender Sicherheitsvorkehrungen konsultiert?	1	Implementieren Sie horizontale Sicherheitsvorkehrungen in allen kritischen Sektoren?	1	Gibt es einen Überwachungsmechanismus, um die Anwendung grundlegender Sicherheitsvorkehrungen zu prüfen?	1	Bewerten Sie die Relevanz neuer Standards, die als Reaktion auf die neuesten Entwicklungen in der Bedrohungslandschaft entwickelt werden?
	3	-		-		Implementieren Sie spezielle Sicherheitsvorkehrungen in allen kritischen Sektoren?	1	Gibt es eine nationale Behörde, die prüft, ob grundlegende Sicherheitsvorkehrungen durchgesetzt werden?	1	Haben oder fördern Sie einen nationalen Prozess zur koordinierten Offenlegung von Sicherheitslücken (CVD)?
	4	-				Stehen die grundlegenden Sicherheitsvorkehrungen im Einklang mit den relevanten Zertifizierungssystemen?	1	Haben Sie ein Verfahren eingerichtet, um nicht konforme Organisationen innerhalb eines bestimmten Zeitraums zu ermitteln?	1	-
	5	-		-		Gibt es ein Selbstrisikobewertungsverfahren für grundlegende Sicherheitsvorkehrungen?	1	Gibt es ein Prüfungsverfahren, um sicherzustellen, dass die Sicherheitsvorkehrungen ordnungsgemäß angewendet werden?	1	-
	6	-		-		Überprüfen Sie die obligatorischen grundlegenden Sicherheitsvorkehrungen in den Beschaffungsverfahren staatlicher Stellen?	0	Definieren oder fördern Sie aktiv die Einführung sicherer Standards für die Entwicklung kritischer IT-/OT-Produkte (medizinische Geräte, vernetzte und autonome Fahrzeuge, professionell genutzte Funkgeräte, Geräte für die Schwerindustrie usw.)?	0	-

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
3 – Sicherung der digitalen Identität und Aufbau von Vertrauen in digitale öffentliche Dienste	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
3 – Sicherung der digitalen Identität und Aufbau von Vertrauen in digitale öffentliche Dienste	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Haben Sie Studien oder Lückenanalysen durchgeführt, um zu ermitteln, inwieweit Bedarf besteht, digitale öffentliche Dienste für Bürger und Unternehmen abzusichern?	1	Führen Sie Risikoanalysen durch, um das Risikoprofil von Anlagen oder Dienstleistungen zu ermitteln, bevor Sie sie in die Cloud verschieben, oder um Projekte zur digitalen Transformation durchzuführen?	1	Fördern Sie Methoden des Datenschutzes durch Technikgestaltung („Privacy-by-Design“) in allen Projekten der elektronischen Behördendienste („E-Government“)?	1	Sammeln Sie Indikatoren zu Cybersicherheitsvorfällen, bei denen digitale öffentliche Dienste betroffen sind?	1	Nehmen Sie an europäischen Arbeitsgruppen teil, um Standards aufrechtzuerhalten und/oder neue Anforderungen für elektronische Vertrauensdienste zu entwerfen (elektronische Signaturen, elektronische Siegel, elektronisch registrierte Zustelldienste, Zeitstempel, Website-Authentifizierung) z. B. ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU usw.?	1
	2	-		Verfügen Sie über eine Strategie zum Aufbau bzw. zur Förderung sicherer nationaler elektronischer Identifizierungssysteme (eID) für Bürger und Unternehmen?	1	Beziehen Sie private Interessenträger in die Gestaltung und Bereitstellung sicherer digitaler öffentlicher Dienste ein?	1	Haben Sie die gegenseitige Anerkennung von elektronischen Identifizierungsmitteln mit anderen Mitgliedstaaten eingeführt?	1	Nehmen Sie im Rahmen der Notifizierung der Europäischen Kommission über elektronische Identifizierungssysteme aktiv an Peer Reviews teil?	1
	3	-		Verfügen Sie über eine Strategie zum Aufbau oder zur Förderung sicherer nationaler elektronischer Vertrauensdienste (elektronische Signaturen, elektronische Siegel, elektronisch registrierte Zustelldienste, Zeitstempel, Website-Authentifizierung) für Bürger und Unternehmen?	1	Sehen Sie eine Mindestsicherheitsbasis für alle digitalen öffentlichen Dienste vor?	1	-		-	
	4	-		Verfügen Sie über eine Strategie für die Behörden-Cloud (eine Cloud-Computing-Strategie für staatliche und öffentliche Stellen wie Ministerien, Behörden und öffentliche Verwaltungen usw.), die die Auswirkungen auf die Sicherheit berücksichtigt?	0	Stehen Bürgern und Unternehmen elektronische Identifizierungssysteme mit einem substanziellen oder hohen Sicherheitsniveau im Sinne des Anhangs der eIDAS-Verordnung (EU) Nr. 910/2014 zur Verfügung?	1	-		-	
	5	-		-		Haben Sie digitale öffentliche Dienste, die elektronische Identifizierungssysteme mit einem substanziellen oder hohen Sicherheitsniveau im Sinne des Anhangs der eIDAS-Verordnung (EU) Nr. 910/2014 erfordern?	1	-		-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
3 – Sicherung der digitalen Identität und Aufbau von Vertrauen in digitale öffentliche Dienste	6	-		-		Haben Sie Vertrauensdiensteanbieter für Bürger und Unternehmen (elektronische Signaturen, elektronische Siegel, elektronisch registrierte Zustelldienste, Zeitstempel, Website-Authentifizierung)?	1	-		-	
	7	-		-		Fördern Sie die Einführung grundlegender Sicherheitsvorkehrungen für alle Cloud-Einsatzmodelle (z. B. privat, öffentlich, gemischt; IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Cluster Nr. 2: Kapazitätenaufbau und Sensibilisierung

NCSS-Ziel	Nr.	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
4 – Einrichtung einer Kapazität zur Reaktion auf Sicherheitsvorfälle	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Verfügen Sie über informelle Kapazitäten zur Reaktion auf Sicherheitsvorfälle, die innerhalb des öffentlichen und des privaten Sektor bzw. von ihnen gemeinsam gesteuert werden?	1	Haben Sie mindestens ein offizielles nationales CSIRT?	1	Verfügen Sie über Fähigkeiten zur Reaktion auf Sicherheitsvorfälle für die in Anhang II der NIS-Richtlinie aufgeführten Sektoren?	1	Haben Sie standardisierte Verfahren für die Reaktion auf Sicherheitsvorfälle und Schemata für die Klassifizierung von Sicherheitsvorfällen festgelegt und gefördert?	1	Verfügen Sie über Mechanismen zur Früherkennung, Ermittlung, Prävention, Reaktion und Verringerung von Zero-Day-Sicherheitslücken?	1

NCSS-Ziel	Nr.	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
4 – Einrichtung einer Kapazität zur Reaktion auf Sicherheitsvorfälle	2	-		Haben Ihre nationalen CSIRT einen klar definierten Einsatzbereich (z. B. Sektoren, Arten der Sicherheitsvorfälle und Auswirkungen)?	1	Gibt es in Ihrem Land einen CSIRT-Kooperationsmechanismus zur Reaktion auf Sicherheitsvorfälle?	1	Bewerten Sie Ihre Kapazität zur Reaktion auf Sicherheitsvorfälle, um sicherzustellen, dass Sie über angemessene Ressourcen und Kompetenzen verfügen, um die in Anhang I Ziffer 2 der NIS-Richtlinie genannten Aufgaben auszuführen?	1	-	
	3	-		Verfügt Ihr nationales CSIRT über klar definierte Beziehungen zu anderen nationalen Interessenträgern in Bezug auf die nationale Cybersicherheitslandschaft und die Vorgehensweisen zur Reaktion auf Vorfälle (z. B. Strafverfolgungsbehörde, Militär, ISP, NCSC)?	0	Verfügt Ihr nationales CSIRT über eine Kapazität zur Reaktion auf Sicherheitsvorfälle gemäß Anhang I der NIS-Richtlinie (d. h. Verfügbarkeit, physische Sicherheit, Betriebskontinuität, internationale Kooperation, Überwachung von Sicherheitsvorfällen, Frühwarn- und Warnkapazität, Reaktion auf Sicherheitsvorfälle, Risikoanalyse und Lagebeurteilung, Kooperation mit dem Privatsektor, standardisierte Abläufe usw.)?	1	-		-	
	4	-				Gibt es einen Kooperationsmechanismus mit anderen Nachbarländern in Bezug auf Sicherheitsvorfälle?	1	-		-	
	5	-		-		Haben Sie formell klare Leitlinien und Verfahren für den Umgang mit Sicherheitsvorfällen definiert?	1	-		-	
	6	-		-		Nehmen Ihre nationale CSIRT an Cybersicherheitsübungen auf nationaler und internationaler Ebene teil?	1	-		-	
	7	-		-		Sind Ihre nationalen CSIRT dem FIRST (Forum der Notfall- und Sicherheitsteams) angeschlossen?	0	-		-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
5 – Sensibilisierung der Benutzer	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Wird von staatlicher Seite, seitens des Privatsektors oder der allgemeinen Nutzer allgemein anerkannt, dass das Bewusstsein für Cybersicherheits- und Datenschutzfragen geschärft werden muss?	1	Haben Sie eine bestimmte Zielgruppe für die Benutzersensibilisierung ermittelt (z. B. allgemeine Nutzer, junge Leute, gewerbliche Nutzer, die nach SME, OES, DSP usw. weiter aufgeschlüsselt werden können)?	1	Haben Sie Kommunikationspläne/-strategien für die Kampagnen entwickelt?	1	Legen Sie in der Planungsphase Parameter für die Bewertung Ihrer Kampagne fest?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass Sensibilisierungskampagnen in Bezug auf technologischen Fortschritt, Änderungen der Bedrohungslandschaft, gesetzliche Vorschriften und nationale Sicherheitsrichtlinien ständig relevant sind?	1
	2	Führen öffentliche Stellen Ad-hoc-Kampagnen zur Sensibilisierung für Cybersicherheit in ihrer Organisation durch (z. B. nach einem Cybersicherheitsvorfall)?	0	Erstellen Sie einen Projektplan, um das Bewusstsein für Fragen der Informationssicherheit und des Datenschutzes zu schärfen?	1	Verfügen Sie auf staatlicher Ebene über ein Verfahren zum Erstellen von Inhalten?	1	Bewerten Sie Ihre Kampagnen nach ihrer Durchführung?	1	Führen Sie regelmäßige Bewertungen oder Studien durch, um Einstellungs- oder Verhaltensänderungen in Bezug auf Cybersicherheit und Datenschutz im privaten und öffentlichen Sektor zu messen?	1
	3	Führen öffentliche Stellen Ad-hoc-Kampagnen zur Sensibilisierung für Cybersicherheit für die breite Öffentlichkeit durch (z. B. nach einem Cybersicherheitsvorfall)?	0	Haben Sie für Benutzer, die sich über Cybersicherheits- und Datenschutzfragen informieren möchten, Ressourcen zur Verfügung gestellt und sind diese leicht zugänglich (z. B. ein zentrales Online-Portal, Sensibilisierungsinstrumente)?	1	Haben Sie Mechanismen zur Ermittlung der Zielgebiete für die Sensibilisierung (d. h. ENISA-Bedrohungslandschaft, nationale Landschaften, internationale Landschaften, Feedback von nationalen Zentren für Cyberkriminalität usw.)?	1	Verfügen Sie über Mechanismen, um die relevantesten Medien oder Kommunikationskanäle je nach Zielgruppe zu ermitteln und so die Reichweite und die Beteiligung zu maximieren (z. B. verschiedene Arten von digitalen Medien, Broschüren, E-Mail, Lehrmittel, Poster in häufig frequentierten Bereichen, Fernsehen, Radio usw.)?	1	Konsultieren Sie Verhaltensexperten, um Ihre Kampagne auf die Zielgruppe zuzuschneiden?	1
	4	-		-		Bringen Sie Interessenträger mit Sachverständigen und Kommunikationsteams zusammen, um Inhalte zu erstellen?	1			-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
5 – Sensibilisierung der Benutzer	5	-		-		Beziehen Sie den Privatsektor in Ihre Sensibilisierungsbemühungen ein, um für die Botschaften zu werben und sie einem breiteren Publikum bekannt zu machen?	1	-		-	
	6	-		-		Bereiten Sie spezifische Sensibilisierungsinitiativen für Führungskräfte im öffentlichen, privaten, akademischen oder zivilgesellschaftlichen Sektor vor?	1	-		-	
	7	-		-		Nehmen Sie an den ECSM-Kampagnen der ENISA (Europäischer Monat der Cybersicherheit) teil?	0	-		-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
6 – Organisation von Cybersicherheitsübungen	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Führen Sie Krisenübungen in anderen Sektoren (außer Cybersicherheit) auf nationaler oder europaweiter Ebene durch?	1	Haben Sie ein nationales Programm für Cybersicherheitsübungen?	1	Beziehen Sie alle betroffenen Behörden der öffentlichen Verwaltung ein (auch wenn das Szenario sektorspezifisch ist)?	1	Schreiben Sie danach Aktionsberichte/Bewertungsberichte?	1	Verfügen Sie über Analysekapazitäten, um aus den gewonnenen Erkenntnissen im Cyberbereich zu lernen (Berichterstattungsverfahren, Analyse, Schadensbegrenzung)?	1
	2	Sind Ressourcen für die Gestaltung und die Planung von Krisenmanagementübungen zugewiesen?	1	Führen Sie Cyberkrisenmanagementübungen für wichtige gesellschaftliche Funktionen und kritische Infrastrukturen durch bzw. priorisieren Sie diese?	1	Beziehen Sie den Privatsektor in die Planung und Durchführung der Übungen ein?	1	Testen Sie nationale Pläne und Verfahren?	1	Verfügen Sie über ein etabliertes Verfahren, um aus den gewonnenen Erkenntnissen zu lernen?	1

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
6 – Organisation von Cybersicherheitsübungen	3	-		Haben Sie eine Koordinierungsstelle benannt, die die Gestaltung und Planung von Cybersicherheitsübungen überwacht (Behörde, Beratungsdienst o. Ä.)?	0	Organisieren Sie sektorspezifische Übungen auf nationaler und/oder internationaler Ebene?	1	Nehmen Sie an europaweiten Cybersicherheitsübungen teil?	1	Passen Sie die Übungsszenarien an die neuesten Entwicklungen an (technologischer Fortschritt, globale Konflikte, Bedrohungslandschaft usw.)?	1
	4	-		-		Organisieren Sie Übungen in allen kritischen Sektoren, die in Anhang II der NIS-Richtlinie aufgeführt sind?	1	-		Stimmen Sie Ihre Krisenmanagementverfahren mit anderen Mitgliedstaaten ab, um ein wirksames europaweites Krisenmanagement sicherzustellen?	1
	5	-		-		Organisieren Sie sektorinterne und/oder sektorübergreifende Cybersicherheitsübungen?	1	-		Verfügen Sie über einen Mechanismus, um die Strategie, Pläne und Verfahren entsprechend den während der Übungen gewonnenen Erkenntnissen schnell anzupassen?	0
	6	-		-		Organisieren Sie Cybersicherheitsübungen für verschiedene Ebenen (technische und operative Ebene, Prozessebene, Entscheidungsebene, politische Ebene usw.)?	0	-		-	

NCSS-Ziel	#	Level 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
7 – Stärkung von Schulungs-, Ausbildungs- und Bildungsprogrammen	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Denken Sie darüber nach, Schulungs-, Ausbildungs- und Bildungsprogramme für Cybersicherheit zu entwickeln?	1	Richten Sie Kurse zur Cybersicherheit ein?	1	Berücksichtigt Ihr Land Cybersicherheitskultur in der frühen Bildungsphase von Schülerinnen und Schülern? Fördern Sie beispielsweise die Behandlung von Cybersicherheitsfragen in der Mittel- und Oberstufe?	1	Halten Sie Beschäftigte im privaten und öffentlichen Sektor an, sich akkreditieren bzw. zertifizieren zu lassen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass Schulungs-, Ausbildungs- und Bildungsbildungsprogramme in Bezug auf aktuelle und zukünftige technologische Entwicklungen, Änderungen der Bedrohungslandschaft, gesetzliche Vorschriften und nationale Sicherheitsleitlinien auf dem neuesten Stand sind?	1
	2	-		Bieten Universitäten Ihres Landes Promotionsstudien in Cybersicherheit als eigenständige Fachrichtung und nicht als eine Informatikfachrichtung an?	1	Haben Sie nationale Forschungslabors und Bildungseinrichtungen, die auf Cybersicherheit spezialisiert sind?	1	Hat Ihr Land Schulungs-, Ausbildungs- oder Mentorenprogramme für Cybersicherheit entwickelt, um nationale Start-ups und KMU zu unterstützen?	1	Richten Sie akademische Kompetenzzentren für Cybersicherheit ein, die als Drehscheiben für Forschung und Bildung dienen?	1
	3	-		Planen Sie, Lehrkräfte und Ausbilder unabhängig von ihrem Fachgebiet in Fragen der Informationssicherheit und des Datenschutzes auszubilden (z. B. Online-Sicherheit, Schutz personenbezogener Daten, Cyber-Mobbing)?	1	Fördern/finanzieren Sie spezielle Cybersicherheitskurse und Schulungs-/Ausbildungspläne im Cyberbereich für Mitarbeiter von Arbeitsvermittlungsstellen in Mitgliedstaaten?	1	Fördern Sie aktiv die Aufnahme von Kursen zur Informationssicherheit in der Hochschulbildung nicht nur für Informatikstudenten, sondern auch für andere Fachgebiete (z. B. Kurse, die auf den Bedarf im jeweiligen Beruf zugeschnitten sind)?	1	Nehmen Hochschuleinrichtungen an führenden Diskussionen im Bereich der Cybersicherheitsbildung und -forschung auf internationaler Ebene teil?	0
	4	-		-		Verfügen Sie über Cybersicherheitskurse und/oder spezielle Lehrpläne für den Europäischen Qualifikationsrahmen (EQR) Stufe 5 bis 8?	1	Bewerten Sie regelmäßig die Kompetenzlücken (Mangel an Cybersecurity-Mitarbeitern) im Bereich der Informationssicherheit?	1	-	

NCSS-Ziel	#	Level 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
7 - Stärkung von Schulungs-, Ausbildungs- und Bildungsprogrammen	5	-		-		Ermutigen und/oder unterstützen Sie Initiativen, Kurse über Cybersicherheit in die Grund- und Sekundarstufe aufzunehmen?	1	Fördern Sie die Vernetzung und den Informationsaustausch zwischen Hochschuleinrichtungen auf nationaler und internationaler Ebene?	1		
	6	-		-		Finanzieren oder bieten Sie den Bürgerinnen und Bürgern kostenlose Basisschulungen in Cybersicherheit an?	0	Beziehen Sie den Privatsektor in irgendeiner Form in Initiativen zur Aufklärung über Cybersicherheit ein (z. B. Kursgestaltung und -durchführung, Praktika usw.)?	1	-	
	7	-		-		Organisieren Sie jährliche Veranstaltungen zu Informationssicherheit (z. B. Hacking-Wettbewerbe oder Hackathons)?	0	Bestehen Finanzierungsmechanismen, um die Einführung von Ausbildungsabschlüssen in Cybersicherheit zu fördern (z. B. Stipendien, garantierte Ausbildung/Praktika, garantierte Arbeitsplätze in bestimmten Sektoren oder Stellen im öffentlichen Sektor)?	0	-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
8 – Förderung von F&E	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
8 – Förderung von F&E	1	Haben Sie Studien oder Analysen durchgeführt, um die F&E-Prioritäten für Cybersicherheit zu ermitteln?	1	Verfügen Sie über ein Verfahren zur Festlegung von F&E-Prioritäten (z. B. aufkommende Themen zur Abschreckung, zum Schutz, zur Erkennung und zur Anpassung an neue Arten von Cyberangriffen)?	1	Gibt es einen Plan, um F&E-Initiativen mit der Realwirtschaft zu verbinden?	1	Entsprechen F&E-Cybersicherheitsinitiativen den einschlägigen strategischen Zielen, z. B DSM, H2020, „Digitales Europa“, EU-Strategie für die Cybersicherheit?	1	Betreiben Sie eine Zusammenarbeit mit internationalen F&E-Initiativen im Bereich Cybersicherheit auf nationaler Ebene?	1
	2	-		Ist der Privatsektor an der Festlegung von F&E-Prioritäten beteiligt?	1	Bestehen nationale Projekte im Zusammenhang mit Cybersicherheit?	1	Gibt es ein Bewertungsschema für F&E-Initiativen?	1	Sind die F&E-Prioritäten auf die aktuelle oder kommende (nationale) Regelung abgestimmt?	1
	3	-		Sind Hochschuleinrichtungen an der Festlegung von F&E-Prioritäten beteiligt?	1	Gibt es lokale/regionale Startup-Ökosysteme und andere Netzwerkkanäle (z. B. Technologieparks, Innovationscluster, Netzwerkveranstaltungen/-plattformen), um Innovationen zu fördern (auch für Startups im Bereich Cybersicherheit)?	1	Bestehen Kooperationsvereinbarungen mit Universitäten und anderen Forschungseinrichtungen?	1	Nehmen Sie an Spitzengesprächen zu einem oder mehreren hochaktuellen F&E-Themen auf internationaler Ebene teil?	0
	4	-		Bestehen nationale F&E-Initiativen im Zusammenhang mit Cybersicherheit?	0	Werden in der Wissenschaft und im privaten Sektor Investitionen in F&E-Programme für Cybersicherheit getätigt?	1	Gibt es eine anerkannte Institution, die die F&E-Aktivitäten im Bereich Cybersicherheit überwacht?	0	-	
	5	-		-		Gibt es Lehrstühle für industrielle/wirtschaftliche Forschung an Universitäten, um Forschungsthemen und den Bedarf des Marktes in Einklang zu bringen?	1	-		-	
	6	-		-		Bestehen spezielle F&E-Finanzierungsprogramme für Cybersicherheit?	0	-		-	

NCSS-Ziel	#	Level 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
9 – Schaffung von Anreizen für den Privatsektor, in Sicherheitsvorkehrungen zu investieren	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1

NCSS-Ziel	#	Level 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
9 – Schaffung von Anreizen für den Privatsektor, in Sicherheitsvorkehrungen zu investieren	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Gibt es eine Industrie-/Wirtschaftspolitik bzw. den politischen Willen, die Entwicklung der Cybersicherheitsbranche zu fördern?	1	Ist der Privatsektor an der Gestaltung von Anreizen beteiligt?	1	Gibt es wirtschaftliche/gesetzliche oder andere Anreize zur Förderung von Investitionen in die Cybersicherheit?	1	Gibt es private Akteure, die auf Anreize reagieren, indem sie in Sicherheitsvorkehrungen investieren (z. B. auf Cybersicherheit spezialisierte Investoren und nicht spezialisierte Investoren)?	1	Berücksichtigten Sie bei den Anreizen im Bereich Cybersicherheit insbesondere die neuesten Bedrohungsentwicklungen?	1
	2	-		Haben Sie bestimmte Cybersicherheitsthemen ermittelt, die entwickelt werden sollen (z. B. Kryptographie, Datenschutz, neue Form der Authentifizierung, KI für Cybersicherheit usw.)?	0	Bieten Sie Unterstützung (z. B. steuerliche Anreize) für Startups und KMU im Bereich Cybersicherheit?	1	Bieten Sie dem Privatsektor Anreize, sich auf die Sicherheit modernster Technologien zu konzentrieren (z. B. 5G, künstliche Intelligenz, IoT, Quanteninformatik usw.)?	1	-	
	3	-		-		Bieten Sie privaten Investoren in Cybersicherheits-Startups steuerliche Anreize oder andere finanzielle Anreize?	1	-		-	
	4	-		-		Erleichtern Sie Startups und KMU im Bereich Cybersicherheit den Zugang zu öffentlichen Beschaffungsverfahren?	0	-		-	
	5	-		-		Sind Finanzmittel vorgesehen, um Anreize für den Privatsektor zu schaffen?	0	-		-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
10 – Verbesserung der Cybersicherheit der Lieferkette	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
10 – Verbesserung der Cybersicherheit der Lieferkette	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Haben Sie eine Studie zu bewährten Sicherheitsverfahren für das Lieferkettenmanagement durchgeführt, die bei Beschaffungsverfahren in verschiedenen Wirtschaftssegmenten und/oder im öffentlichen Sektor angewendet werden?	1	Führen Sie Cybersicherheitsbewertungen entlang der gesamten Lieferkette von IKT-Diensten und -Produkten in kritischen Sektoren (gemäß Definition in Anhang II der NIS-Richtlinie (2016/1148)) durch?	1	Verwenden Sie ein Sicherheitszertifizierungsschema für IKT-basierte Produkte und Dienstleistungen, wie etwa SOG-IS MRA in Europa (Abkommen über die gegenseitige Anerkennung des Beratenden Ausschusses für die Maßnahmen auf dem Gebiet der Sicherheit von Informationssystemen), das Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC (CCRA), nationale Initiativen, Brancheninitiativen usw.	1	Verfügen Sie über einen Prozess zur Aktualisierung der Cybersicherheitsbewertungen entlang der Lieferkette von IKT-Diensten und -Produkten in kritischen Sektoren (gemäß Definition in Anhang II der NIS-Richtlinie (2016/1148))?	1	Haben Sie Erkennungssonden in Schlüsselelementen der Lieferkette, um frühzeitig Anzeichen einer Kompromittierung zu erkennen (z. B. Sicherheitskontrollen auf ISP-Ebene, Sicherheitsprüfungen in wichtigen Infrastrukturkomponenten usw.)?	1
	2	-		Wenden Sie in den Beschaffungsvorschriften der Behörden Standards an, um sicherzustellen, dass Anbieter von IKT-Produkten oder -Dienstleistungen die grundlegenden Anforderungen an die Informationssicherheit erfüllen (z. B. ISO/IEC 27001 und 27002, ISO/IEC 27036 usw.)?	1	Fördern Sie aktiv Sicherheit und Datenschutz durch Technikgestaltung, indem Sie bewährte Verfahren für die Entwicklung von IKT-Produkten und -Dienstleistungen entwickeln (z. B. sicherer Softwareentwicklungs-Lebenszyklus, IoT-Lebenszyklus)?	1	Verfügen Sie über ein Verfahren zur Erkennung von Schwachstellen in Bezug auf die Cybersicherheit in der Lieferkette kritischer Sektoren (gemäß Definition in Anhang II der NIS-Richtlinie (2016/1148))?	1	-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
10 – Verbesserung der Cybersicherheit der Lieferkette	3	-		-		Entwickeln Sie und stellen Sie zentralisierte Kataloge mit ausführlichen Informationen zu vorhandenen Standards für Informationssicherheit und Datenschutz bereit, die für KMU skalierbar und anwendbar sind?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass IKT-Produkte und -Dienstleistungen, die für OES von entscheidender Bedeutung sind, Cyber-Resilienz besitzen (d. h. die Fähigkeit haben, Verfügbarkeit und Sicherheit gegen einen Cybervorfall aufrechtzuerhalten, z. B. durch Tests, regelmäßige Bewertungen, Erkennung kompromittierter Elemente usw.)?	1	-	
	4	-				Beteiligen Sie sich aktiv an der Ausarbeitung eines EU-Zertifizierungsrahmens für digitale IKT-Produkte, -Dienstleistungen und -Prozesse gemäß dem EU-Rechtsakt zur Cybersicherheit (Verordnung (EU) 2019/881), z. B. Teilnahme an der Europäischen Gruppe für die Cybersicherheitszertifizierung (ECCG), Förderung technischer Standards und Verfahren für die Sicherheit von IKT-Produkten/-Dienstleistungen?	0	Fördern Sie die Entwicklung von Zertifizierungssystemen für KMU, um die Einführung von Standards für Informationssicherheit und Datenschutz zu verbessern?	0	-	
	5	-		-		Bieten Sie KMU Anreize für die Einführung von Sicherheits- und Datenschutzstandards?	0	Haben Sie Vorkehrungen getroffen, um große Unternehmen zu ermutigen, die Cybersicherheit kleiner Unternehmen in ihren Lieferketten zu erhöhen (z. B. Zentrum für Cybersicherheit, Schulungs- und Sensibilisierungskampagnen)?	0	-	
	6	-		-		Ermutigen Sie Softwareanbieter, KMU zu unterstützen, indem sie sichere Standardkonfigurationen in Produkten sicherstellen, die für kleine Unternehmen bestimmt sind?	0	-		-	

4.1.3 Cluster Nr. 3: Gesetze und Bestimmungen

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
11 – Schutz der kritischen Informationsinfrastruktur, OES und DSP	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Besteht allgemein Einvernehmen darüber, dass Betreiber kritischer Informationsinfrastruktur zur nationalen Sicherheit beitragen?	1	Verfügen Sie über eine Methode, um wesentliche Dienste zu identifizieren?	1	Haben Sie die NIS-Richtlinie (2016/1148) umgesetzt?	1	Verfügen Sie über ein Verfahren zur Aktualisierung des Risikoregisters?	1	Erstellen und aktualisieren Sie Berichte über Bedrohungslandschaften?	1
	2	-		Verfügen Sie über eine Methode zur Ermittlung kritischer Informationsinfrastrukturen (CII)?	1	Haben Sie die ECI-Richtlinie (2008/114) über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, umgesetzt?	1	Verfügen Sie über andere Mechanismen, um zu messen, ob die von den Betreibern wesentlicher Dienste (OES) implementierten technischen und organisatorischen Maßnahmen geeignet sind, um die Risiken für die Netz- und Informationssicherheit zu bewältigen (z. B. regelmäßige Cybersicherheitsprüfungen, nationaler Rahmen für die Einführung von Standardmaßnahmen, von staatlicher Seite bereitgestellte technische Instrumente wie Erkennungssonden oder systemspezifische Konfigurationsüberprüfungen usw.)?	1	Können Sie entsprechend den neuesten Entwicklungen in der Bedrohungslandschaft einen neuen Bereich in Ihren Aktionsplan für den Schutz kritischer Informationsinfrastrukturen aufnehmen?	1
	3	-		Verfügen Sie über eine Methode, um OES zu ermitteln?	1	Besteht ein nationales Register für ermittelte OES für jeden kritischen Sektor?	1	Überprüfen und aktualisieren Sie dementsprechend die Liste der ermittelten OES mindestens alle zwei Jahre?	1	Können Sie entsprechend den neuesten Entwicklungen in der Bedrohungslandschaft neue Anforderungen in Ihren Aktionsplan für den Schutz kritischer Informationsinfrastrukturen aufnehmen?	1

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
11 – Schutz der kritischen Informationsinfrastruktur, OES und DSP	4	-		Verfügen Sie über eine Methode, um Anbieter digitaler Dienste (DSP) zu ermitteln?	1	Verfügen Sie über ein nationales Register für ermittelte Anbieter digitaler Dienste?	1	Verfügen Sie über andere Mechanismen, um zu messen, ob die von den Anbietern digitaler Dienste implementierten technischen und organisatorischen Maßnahmen geeignet sind, um die Risiken für die Netz- und Informationssicherheit zu bewältigen (z. B. regelmäßige Cybersicherheitsprüfungen, nationaler Rahmen für die Einführung von Standardmaßnahmen, von staatlicher Seite bereitgestellte technische Instrumente wie Erkennungssonden oder systemspezifische Konfigurationsüberprüfungen usw.)?	1	-	
	5	-		Gibt es eine oder mehrere nationale Behörden, die den Schutz kritischer Informationsinfrastrukturen (CII) und die Netz- und Informationssicherheit überwachen (wie etwa gemäß der NIS-Richtlinie (2016/1148) erforderlich)?	1	Haben Sie ein nationales Risikoregister für ermittelte bzw. bekannte Risiken?	1	Überprüfen und aktualisieren Sie dementsprechend die Liste der ermittelten Anbieter digitaler Dienste mindestens alle zwei Jahre?	1	-	
	6	-		Entwickeln Sie sektorspezifische Schutzpläne (z. B. einschließlich grundlegender Cybersicherheitsvorkehrungen (obligatorisch oder als Leitlinien))?	0	Verfügen Sie über eine Methode, um CII-Abhängigkeiten zu ermitteln?	1	Verwenden Sie ein Sicherheitszertifizierungssystem (national oder international), um OES und Anbietern digitaler Dienste bei der Identifizierung sicherer IKT-Produkte zu helfen (z. B. SOG-IS MRA in Europa, nationale Initiativen usw.)?	1	-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
11 – Schutz der kritischen Informationsinfrastruktur, OES und DSP	7	-		-		Setzen Sie Risikomanagementverfahren ein, um Risiken im Zusammenhang mit CII auf nationaler Ebene zu ermitteln, zu quantifizieren und zu bewältigen?	1	Verwenden Sie ein Sicherheitszertifizierungsschema oder ein Qualifizierungsverfahren, um Diensteanbieter zu bewerten, die mit OES zusammenarbeiten (z. B. Diensteanbieter im Bereich der Erkennung von Sicherheitsvorfällen, Reaktion auf Sicherheitsvorfälle, Prüfung der Cybersicherheit, Cloud-Dienste, Smartcards usw.)?	1	-	
	8	-		-		Nehmen Sie an einem Konsultationsprozess teil, um grenzüberschreitende Abhängigkeiten zu ermitteln?	1	Verfügen Sie über Mechanismen zur Messung der Einhaltung grundlegender Cybersicherheitsvorkehrungen durch OES und Anbieter digitaler Dienste?	0	-	
	9					Gibt es eine zentrale Anlaufstelle, die für die Koordinierung von Fragen im Zusammenhang mit der Netz- und Informationssicherheit auf nationaler Ebene und der grenzüberschreitenden Zusammenarbeit auf Unionsebene zuständig ist?	1	Haben Sie Vorkehrungen getroffen, um die Kontinuität der von kritischen Informationsinfrastrukturen bereitgestellten Dienste sicherzustellen (z. B. Antizipation von Krisen, Verfahren zum Wiederaufbau kritischer Informationssysteme, Betriebskontinuität ohne IT, Verfahren zur Sicherung von Air Gaps usw.)?	0		
	10					Legen Sie grundlegende Cybersicherheitsvorkehrungen (obligatorisch oder als Leitlinien) für Anbieter digitaler Dienste und alle in Anhang II der NIS-Richtlinie (2016/1148) aufgeführte Sektoren fest?	1				
	11	-		-		Stellen Sie Instrumente oder Methoden zur Erkennung von Cybervorfällen bereit?	1	-		-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
12 – Bekämpfung von Cyberkriminalität	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Haben Sie eine Studie durchgeführt, um die Anforderungen der Strafverfolgung (Rechtsgrundlage, Ressourcen, Kompetenzen usw.) zur wirksamen Bekämpfung der Cyberkriminalität zu ermitteln?	1	Entspricht Ihr nationaler Rechtsrahmen vollständig dem einschlägigen EU-Rechtsrahmen, einschließlich der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme (z. B. illegaler Zugang zu Informationssystemen, illegale Systeminterferenz, illegale Dateninterferenz, illegales Abfangen, Instrumente zur Begehung von Straftaten usw.)?	1	Haben Sie in Strafverfolgungsbehörden Stellen, die sich mit Cyberkriminalität befassen?	1	Erfassen Sie statistische Daten gemäß Artikel 14 Absatz 1 der Richtlinie 2013/40/EU (Richtlinie über Angriffe auf Informationssysteme)?	1	Gibt es auf nationaler und/oder multilateraler Ebene institutionsübergreifende Schulungen oder Schulungsworkshops für Strafverfolgungsbehörden, Richter, Staatsanwälte und nationale/staatliche CSIRT?	1
	2	Haben Sie eine Studie durchgeführt, um die Anforderungen an Staatsanwälte und Richter (Rechtsgrundlage, Ressourcen, Kompetenzen usw.) zur wirksamen Bekämpfung der Cyberkriminalität zu ermitteln?	1	Bestehen gesetzliche Bestimmungen zur Bewältigung von Online-Identitätsdiebstahl und Diebstahl personenbezogener Daten?	1	Verfügen Sie über zweckgebundene Finanzmittel für Cyberkriminalitätseinheiten?	1	Erfassen Sie separate statistische Daten zur Cyberkriminalität (z. B. Betriebsstatistiken, Statistiken zu Cyberkriminalitätstrends, Statistiken zu Cyberkriminalitätserlösen und verursachten Schäden usw.)?	1	Nehmen Sie an koordinierten Maßnahmen auf internationaler Ebene teil, um kriminelle Aktivitäten zu stören (z. B. Infiltration in kriminelle Hacking-Foren, Gruppen organisierter Cyberkriminalität, Dark-Web-Märkte und Botnet-Zerschlagungen)?	1
	3	Hat Ihr Land das Budapester Übereinkommen des Europarates über Cyberkriminalität unterzeichnet?	1	Bestehen gesetzliche Bestimmungen in Bezug auf Verletzungen von Rechten des geistigen Eigentums und Urheberrechten?	1	Haben Sie eine zentrale Stelle eingerichtet, um die Aktivitäten zur Bekämpfung der Cyberkriminalität zu koordinieren?	1	Bewerten Sie die Angemessenheit der Schulungen für Strafverfolgungsbehörden, Justiz- und nationales CSIRT-Personal zur Bekämpfung der Cyberkriminalität?	1	Gibt es eine klare Aufgabentrennung zwischen CSIRT, Strafverfolgungsbehörden und der Justiz (Staatsanwälte und Richter), wenn sie bei der Bekämpfung von Cyberkriminalität zusammenarbeiten?	1

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
12 – Bekämpfung von Cyberkriminalität	4			Bestehen gesetzliche Bestimmungen in Bezug auf Online-Belästigung oder Cyber-Mobbing?	1	Haben Sie Kooperationsmechanismen zwischen einschlägigen nationalen Institutionen, die an der Bekämpfung der Cyberkriminalität beteiligt sind (einschließlich nationaler CSIRT der Strafverfolgungsbehörden) eingerichtet?	1	Führen Sie regelmäßige Bewertungen durch, um sicherzustellen, dass Sie über ausreichende Ressourcen (Personal, Finanzmittel und Instrumente) für Cyberkriminalitätseinheiten innerhalb von Strafverfolgungsbehörden verfügen?	1	Erleichtert Ihr Rechtsrahmen die Zusammenarbeit zwischen CSIRT/Strafverfolgung und der Justiz (Staatsanwälte und Richter)?	1
	5			Bestehen gesetzliche Bestimmungen zur Bekämpfung von Computerbetrug (z. B. Einhaltung der Bestimmungen des Budapester Übereinkommens des Europarates über Cyberkriminalität)?	1	Arbeiten Sie im Bereich der Bekämpfung der Cyberkriminalität mit anderen Mitgliedstaaten zusammen und tauschen Sie Informationen aus?	1	Führen Sie regelmäßige Bewertungen durch, um sicherzustellen, dass Sie über ausreichende Ressourcen (Personal, Finanzmittel und Instrumente) für Cyberkriminalitätseinheiten innerhalb von Strafverfolgungsbehörden verfügen?	1	Beteiligen Sie sich am Aufbau und der Pflege standardisierter Instrumente und Methoden, Formen und Verfahren, die mit Interessenträgern der EU ausgetauscht werden sollen (Strafverfolgungsbehörden, CSIRT, ENISA, EC3 von Europol usw.)?	1
	6	-		Bestehen gesetzliche Bestimmungen für den Schutz von Kindern im Netz/Internet (z. B. Einhaltung der Bestimmungen der Richtlinie 2011/93/EU und des Budapester Übereinkommens des Europarates über Cyberkriminalität)?	1	Arbeiten Sie im Bereich der Bekämpfung der Cyberkriminalität mit EU-Agenturen (z. B. EC3 von Europol, Eurojust, ENISA) zusammen und tauschen Sie Informationen mit ihnen aus?	1	Gibt es spezielle Gerichte oder spezialisierte Richter für die Befassung mit Fällen von Cyberkriminalität?	1	Verfügen Sie über gut entwickelte Mechanismen, um Einzelpersonen davon abzuhalten, von Cyberkriminalität angezogen zu werden oder sich darauf einzulassen?	0
	7	-		Haben Sie eine operative nationale Kontaktstelle für den Informationsaustausch und die Beantwortung dringender Informationsanfragen anderer Mitgliedstaaten im Zusammenhang mit Straftaten gemäß der Richtlinie 2013/40/EU (Richtlinie über Angriffe auf Informationssysteme) benannt?	1	Verfügen Sie über die geeigneten Tools zur Bekämpfung von Cyberkriminalität (z. B. Taxonomie und Klassifizierung von Cyberkriminalität, Instrumente zum Erheben elektronischer Beweismittel, Computerforensik-Instrumente, vertrauenswürdige gemeinsame Plattformen usw.)?	1	Haben Sie Vorkehrungen getroffen, um Opfern von Cyberkriminalität (allgemeine Nutzer, KMU, große Unternehmen) Unterstützung und Hilfe zu leisten?	1	Verwendet Ihr Land einen EU-Plan und/oder das EU-Strafverfolgungs-Notfallprotokoll (EU LE ERP), um effektiv auf große Cybervorfälle zu reagieren?	0

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
12 – Bekämpfung von Cyberkriminalität	8			Gibt es in Ihrer Strafverfolgungsbehörde eine Abteilung eigens für Cyberkriminalität?	1	Bestehen Standardarbeitsanweisungen für den Umgang mit elektronischen Beweismitteln?	1	Gibt es einen institutionsübergreifenden Rahmen und solche Kooperationsmechanismen zwischen allen relevanten Interessenträgern (z. B. Strafverfolgungsbehörde, nationales CSIRT, gerichtliche Akteure), einschließlich des Privatsektors (z. B. Betreiber wesentlicher Dienste, Diensteanbieter), um gegebenenfalls auf Cyberangriffe zu reagieren?	1	-	
	9			Haben Sie in Einklang mit Artikel 35 des Budapester Übereinkommens eine rund um die Uhr erreichbare Anlaufstelle benannt?	1	Nimmt Ihr Land an Schulungs-/Ausbildungsmöglichkeiten teil, die von EU-Agenturen (z. B. Europol, Eurojust, OLAF, Cepol, ENISA) angeboten und/oder unterstützt werden?	0	Erleichtert Ihr Rechtsrahmen die Zusammenarbeit zwischen CSIRT und Strafverfolgung)?	1	-	
	10	-		Haben Sie eine rund um die Uhr erreichbare nationale Anlaufstelle für das Notfallprotokoll für die Reaktion der Strafverfolgungsbehörden der EU (EU LE ERP) benannt, um auf größere Cyberangriffe zu reagieren?	1	Erwägt Ihr Land, das 2. Zusatzprotokoll zum Budapester Übereinkommen des Europarates über Cyberkriminalität anzunehmen?	0	Verfügen Sie über Mechanismen (z. B. Instrumente, Verfahren), um den Informationsaustausch und die Zusammenarbeit zwischen CSIRT/Strafverfolgung und möglicherweise der Justiz (Staatsanwälte und Richter) im Bereich der Bekämpfung der Cyberkriminalität zu erleichtern?	1	-	
	11			Bieten Sie Interessenträgern, die an der Bekämpfung von Cyberkriminalität beteiligt sind (Strafverfolgungsbehörden, Justiz, CSIRT), regelmäßig spezielle Schulungen an (z. B. Schulungen zum Melden/Verfolgen von durch den Cyberraum ermöglichte Straftaten, Schulungen zum Erheben elektronischer Beweismittel und zur Gewährleistung der Integrität in der gesamten digitalen Überwachungskette, Computer-Forensik u. a.)?	1						

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
12 – Bekämpfung von Cyberkriminalität	12			Hat Ihr Land das Budapester Übereinkommen des Europarates über Cyberkriminalität ratifiziert oder ist ihm beigetreten?	1			-	-	-	
	13	-		Hat Ihr Land das Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Cyberkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art unterzeichnet und ratifiziert?	0	-	-	-		-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
13 – Einrichtung von Mechanismen zur Meldung von Vorfällen	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Verfügen Sie über informelle Mechanismen zum Informationsaustausch über Cybersicherheitsvorfälle zwischen privaten Organisationen und nationalen Behörden?	1	Verfügen Sie über ein System zur Meldung von Vorfällen für alle in Anhang II der NIS-Richtlinie aufgeführten Sektoren?	1	Verfügen Sie über ein obligatorisches System zur Meldung von Vorfällen, das in der Praxis funktioniert?	1	Verfügen Sie über ein harmonisiertes Verfahren für sektorspezifische Meldesysteme für Vorfälle?	1	Erstellen Sie einen jährlichen Vorfallbericht?	1

13 – Einrichtung von Mechanismen zur Meldung von Vorfällen	2	-		Haben Sie die Meldepflichten für Telekommunikationsdienstleister gemäß Artikel 40 der Richtlinie (EU 2018/1972) umgesetzt? Laut der Richtlinie müssen die Mitgliedstaaten sicherstellen, dass die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste der zuständigen Behörde einen Sicherheitsvorfall, der beträchtliche Auswirkungen auf den Betrieb der Netze oder die Bereitstellung der Dienste hatte, unverzüglich mitteilen.	1	Besteht ein Koordinierungs-/Kooperationsmechanismus für die Meldepflicht für Vorfälle in Bezug auf DSGVO, die NIS-Richtlinie, Artikel 40 (vormals Artikel 13a) und eIDAS?	1	Haben Sie ein System zur Meldung von Vorfällen für andere Sektoren als die in Anhang II der NIS-Richtlinie genannten?	1	Liegen Berichte zur Cybersicherheitslandschaft oder andere Arten von Analysen vor, die von der Stelle erstellt wurden, die die Vorfallberichte erhält?	1
	3	-		Haben Sie die Meldepflichten für Vertrauensdiensteanbieter gemäß Artikel 19 der eIDAS-Verordnung (Verordnung (EU) Nr. 910/2014) umgesetzt? Artikel 19 verlangt unter anderem, dass Vertrauensdiensteanbieter der Aufsichtsstelle erhebliche Sicherheitsvorfälle/-verletzungen melden.	1	Verfügen Sie über die geeigneten Instrumente, um die Vertraulichkeit und Integrität der Informationen zu gewährleisten, die über die verschiedenen Meldekanäle ausgetauscht werden?	1	Messen Sie die Wirksamkeit der Verfahren zur Meldung von Vorfällen (z. B. Indikatoren für Vorfälle, die über die entsprechenden Kanäle gemeldet wurden, Zeitpunkt des Vorfallberichts usw.)?	1	-	
	4	-		Haben Sie die Meldepflichten für Anbieter digitaler Dienste gemäß Artikel 16 der NIS-Richtlinie umgesetzt? Gemäß Artikel 16 müssen Anbieter digitaler Dienste die zuständige Behörde oder das nationale CSIRT unverzüglich über Vorfälle informieren, die erhebliche Auswirkungen auf die Erbringung eines Dienstes gemäß Anhang III haben, den sie innerhalb der Union anbieten.	1	Verfügen Sie über eine Plattform/ein Instrument, um das Meldeverfahren zu erleichtern?	0	Verfügen Sie auf nationaler Ebene über eine gemeinsame Taxonomie für die Klassifizierung von Vorfällen und die Ursachenkategorien?	0	-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
14 – Stärkung des Schutzes der Privatsphäre und des Datenschutzes	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Haben Sie Studien oder Analysen durchgeführt, um Verbesserungsbereiche zu identifizieren, um die Datenschutzrechte der Bürgerinnen und Bürger besser zu schützen?	1	Ist die nationale Datenschutzbehörde in Themenbereiche im Zusammenhang mit Cybersicherheit involviert (z. B. Ausarbeitung neuer Gesetze und Vorschriften zur Cybersicherheit, Festlegung von Mindestsicherheitsvorkehrungen)?	1	Fördern Sie bewährte Verfahren für Sicherheitsvorkehrungen und Datenschutz durch Technikgestaltung für den öffentlichen und/oder privaten Sektor?	1	Führen Sie regelmäßige Bewertungen durch, um sicherzustellen, dass Sie über ausreichende Ressourcen (Personal, Finanzmittel und Instrumente) für die Datenschutzbehörden verfügen?	1	Verfügen Sie über Mechanismen zur Überwachung der neuesten technologischen Entwicklungen, um einschlägige Leitlinien und gesetzliche Bestimmungen/Auflagen anzupassen?	1
	2	Haben Sie auf nationaler Ebene eine Rechtsgrundlage zur Durchsetzung der Datenschutz-Grundverordnung (Verordnung EU Nr. 2016/679) entwickelt (z. B. Beibehaltung oder Einführung spezifischerer Bestimmungen oder Einschränkungen der Vorschriften der Verordnung)?	0	-		Starten Sie Sensibilisierungs- und Schulungs-/Ausbildungsprogramme zu diesem Thema?	1	Ermutigen Sie Organisationen und Unternehmen, sich nach ISO/IEC 27701:2019 (Datenschutz-Managementsystem (DSMS)) zertifizieren zu lassen?	1	Nehmen Sie aktiv an F&E-Initiativen in Bezug auf Technologien zum Schutz der Privatsphäre (PET) teil bzw. fördern Sie diese?	0
	3	-		-		Koordinieren Sie die Verfahren zur Meldung von Vorfällen mit der Datenschutzbehörde?	1	-		-	
	4	-		-		Fördern und unterstützen Sie die Entwicklung technischer Normen für Informationssicherheit und Datenschutz? Sind diese speziell auf kleine und mittlere Unternehmen (KMU) zugeschnitten?	0	-		-	

	5	-		-		Bieten Sie praktische und skalierbare Leitlinien an, um verschiedene Arten von Datenverarbeitungsverantwortliche bei der Erfüllung der gesetzlichen Anforderungen und Pflichten zum Schutz der Privatsphäre und des Datenschutzes zu unterstützen?	0	-		-

4.1.4 Cluster Nr. 4: Zusammenarbeit

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
15 – Aufbau einer öffentlich-privaten Partnerschaft (PPP)	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Besteht allgemein Einvernehmen darüber, dass PPP auf unterschiedliche Weise zur Steigerung des Cybersicherheitsniveaus im Land beitragen (z. B. gemeinsames Interesse am Wachstum der Cybersicherheitsbranche, Zusammenarbeit beim Aufbau eines relevanten Rechtsrahmens für Cybersicherheit, Förderung von F&E usw.)?	1	Verfügen Sie über einen nationalen Aktionsplan zum Aufbau von PPP?	1	Haben Sie nationale öffentlich-private Partnerschaften aufgebaut?	1	Haben Sie sektorübergreifende PPP aufgebaut?	1	Können Sie PPP je nach den neuesten technologischen und gesetzlichen Entwicklungen anpassen bzw. aufbauen?	1
	2	-		Stellen Sie eine rechtliche oder vertragliche Grundlage (spezifische Gesetze, NDA, geistiges Eigentum) für den Geltungsbereich von PPP auf?	1	Haben Sie sektorspezifische PPP aufgebaut?	1	Konzentrieren Sie sich in den etablierten PPP auch auf die öffentlich-öffentliche und privat-private Zusammenarbeit?	1		
	3	-		-		Fördern Sie den Aufbau von PPP finanziell?	1	Fördern Sie PPP bei kleinen und mittleren Unternehmen (KMU)?	1	-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
15 – Aufbau einer öffentlich-privaten Partnerschaft (PPP)	4	-		-		Leiten öffentliche Einrichtungen die PPP insgesamt (d. h. eine zentrale Anlaufstelle des öffentlichen Sektors regelt und koordiniert die PPP, öffentliche Stellen vereinbaren im Voraus, was sie erreichen wollen, es gibt klare Leitlinien der öffentlichen Verwaltungen zu ihrem Bedarf und den Einschränkungen für den Privatsektor usw.?)	1	Messen Sie die Ergebnisse von PPP?	1	-	
	5	-		-		Sind Sie Mitglied der vertraglichen öffentlich-privaten Partnerschaft (vPPP) der Europäischen Cybersicherheitsorganisation (ECSO)?	0	-		-	
	6	-		-		Haben Sie eine oder mehrere PPP, die an CSIRT-Aktivitäten arbeiten?	0	-		-	
	7					Haben Sie eine oder mehrere PPP, die sich mit dem Schutz kritischer Informationsinfrastrukturen befassen?	0				
	8	-		-		Haben Sie eine oder mehrere PPP, die daran arbeiten, das Bewusstsein für Cybersicherheit und die Entwicklung von Kompetenzen zu schärfen?	0	-		-	

NCSS-Ziel	Nr.	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
16 – Institutionalisierung der Zusammenarbeit zwischen öffentlichen Stellen	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1

NCSS-Ziel	Nr.	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
16 – Institutionalisierung der Zusammenarbeit zwischen öffentlichen Stellen	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Haben Sie informelle Kooperationskanäle zwischen öffentlichen Stellen?	1	Haben Sie ein nationales Kooperationsprogramm, das sich mit Cybersicherheit befasst (z. B. Beiräte, Lenkungsgruppen, Foren, Räte, Cyber-Zentren oder Expertentreffen)?	1	Beteiligen sich öffentliche Behörden an dem Kooperationsprogramm?	1	Stellen Sie sicher, dass Kooperationskanäle für Cybersicherheit mindestens zwischen den folgenden öffentlichen Stellen bestehen: Geheimdienste, nationale Strafverfolgung, Strafverfolgungsbehörden, staatliche Akteure, nationales CSIRT und Militär?	1	Werden öffentliche Stellen mit einheitlichen Mindestinformationen über die neuesten Entwicklungen in der Bedrohungslandschaft und das Lagebewusstsein für Cybersicherheit versorgt?	1
	2	-		-		Haben Sie Kooperationsplattformen für den Informationsaustausch eingerichtet?	1	Messen Sie die Erfolge und Grenzen der verschiedenen Kooperationsprogramme bei der Förderung einer effektiven Zusammenarbeit?	1	-	
	3	-		-		Haben Sie den Anwendungsbereich der Kooperationsplattformen definiert (z. B. Aufgaben und Zuständigkeiten, Anzahl der Themenbereiche)?	1	-		-	
	4	-		-		Organisieren Sie jährliche Treffen?	1	-		-	
	5	-		-		Verfügen Sie über Kooperationsmechanismen zwischen den zuständigen Behörden der geografischen Regionen (z. B. Netzwerk von regionalen Sicherheitskorrespondenten, Cybersicherheitsbeauftragte in regionalen Wirtschaftskammern usw.)?	1	-		-	

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
17 – Internationale Zusammenarbeit (Nicht nur mit EU-MS)	a	Berücksichtigen Sie das Ziel in Ihrer aktuellen NCSS oder planen Sie, es in der nächsten Ausgabe zu berücksichtigen?	1	Gibt es informelle Verfahren oder Aktivitäten, die dazu beitragen, das Ziel auf nicht koordinierte Weise zu erreichen?	1	Verfügen Sie über einen Aktionsplan, der formal definiert und dokumentiert ist?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um seine Leistung zu testen?	1	Verfügen Sie über Mechanismen, um sicherzustellen, dass der Aktionsplan dynamisch an Entwicklungen des Umfelds angepasst wird?	1
	b			Haben Sie beabsichtigte Ergebnisse, Leitprinzipien oder Schlüsselaktivitäten Ihres Aktionsplans definiert?	1	Verfügen Sie über einen Aktionsplan mit einer klaren Ressourcenzuweisung und Governance?	1	Überprüfen Sie Ihren Aktionsplan hinsichtlich des Ziels, um sicherzustellen, dass er korrekt priorisiert und optimiert ist?	1		
	c			Ist Ihr Aktionsplan gegebenenfalls umgesetzt und in begrenztem Umfang bereits wirksam?	0						
	1	Verfügen Sie über eine Strategie für die internationale Zusammenarbeit?	1	Bestehen Kooperationsabkommen mit anderen Ländern (bilateral, multilateral) oder Partnern in anderen Ländern (z. B. hinsichtlich Informationsaustausch, Kapazitätenaufbau, Unterstützung usw.)?	1	Tauschen Sie Informationen auf strategischer Ebene aus (z. B. übergeordnete Strategie, Risikowahrnehmung usw.)?	1	Sind nationale öffentliche Stellen für Cybersicherheit in Ihrem Land an internationalen Kooperationsprogrammen beteiligt?	1	Führen Sie Diskussionen zu einem oder mehreren Themen im Rahmen multilateraler Abkommen?	1
	2	Bestehen informelle Kooperationskanäle mit anderen Ländern?	1	Haben Sie eine zentrale Anlaufstelle, die eine Verbindungsfunktion ausüben kann, um die grenzüberschreitende Zusammenarbeit mit den Behörden der Mitgliedstaaten (Kooperationsgruppe, CSIRT-Netzwerk usw.) sicherzustellen?	1	Tauschen Sie Informationen auf taktischer Ebene aus (z. B. Bulletin der Bedrohungsakteure, ISAC, TTP usw.)?	1	Bewerten Sie regelmäßig die Ergebnisse internationaler Kooperationsinitiativen?	1	Führen Sie Diskussionen zu einem oder mehreren Themen im Rahmen internationaler Verträge oder Übereinkommen?	1
	3	Haben führende öffentliche Stellen die Absicht bekundet, im Bereich der Cybersicherheit international zusammenzuarbeiten?	1	Haben Sie Mitarbeiter, die speziell für die internationale Zusammenarbeit zuständig sind?	1	Tauschen Sie Informationen auf operativer Ebene aus (z. B. Informationen zur operativen Koordinierung, aktuelle Vorfälle, IOC usw.)?	1	-		Führen Sie Diskussionen oder Verhandlungen zu einem oder mehreren Themen innerhalb internationaler Sachverständigengruppen (z. B. Globale Kommission für die Stabilität des Cyberspace (GCSC), ENISA-NIS-Kooperationsgruppe, UN-Gruppe von Regierungssachverständigen für Informationssicherheit (GGE) usw.)?	1

NCSS-Ziel	#	Grad 1	R	Grad 2	R	Grad 3	R	Grad 4	R	Grad 5	R
17 – Internationale Zusammenarbeit (Nicht nur mit EU-MS)	4	-		-		Nehmen Sie an internationalen Cybersicherheitsübungen teil?	1	-		-	
	5	-		-		Beteiligen Sie sich an internationalen Initiativen zum Kapazitätenaufbau (z. B. Schulungen/Ausbildung, Kompetenzentwicklung, Entwurf von Standardverfahren usw.)?	0	-		-	
	6	-		-		Haben Sie Vereinbarungen über gegenseitige Unterstützung mit anderen Ländern geschlossen (z. B. Aktivitäten der Strafverfolgungsbehörden, Gerichtsverfahren, gegenseitige Unterstützung der Kapazitäten zur Reaktion auf Sicherheitsvorfälle, gemeinsame Nutzung von Cybersicherheitsanlagen usw.)?	0	-		-	
	7	-		-		Haben Sie internationale Verträge oder Übereinkommen im Bereich der Cybersicherheit unterzeichnet bzw. ratifiziert (z. B. Internationaler Verhaltenskodex für Informationssicherheit, Übereinkommen über Cyberkriminalität)?	0	-		-	

4.2 LEITLINIEN ZUR NUTZUNG DES RAHMENS

Dieser Abschnitt soll den Mitgliedstaaten einige Leitlinien und Empfehlungen für die Einführung des Rahmens und das Ausfüllen des Fragebogens geben. Die nachstehend aufgeführten Empfehlungen beruhen hauptsächlich auf den Rückmeldungen aus den Befragungen der Vertreter der Mitgliedstaaten:

- **Antizipierung von Koordinierungsaktivitäten, um Daten zusammenzutragen und Daten zu konsolidieren.** Die meisten Mitgliedstaaten gehen davon aus, dass die Durchführung einer solchen Selbstbewertung etwa 15 Personentage dauern wird. Um die Selbstbewertung durchführen zu können, muss eine Vielzahl unterschiedlicher Interessenträger angesprochen werden. Es wird daher empfohlen, Zeit für die Vorbereitungsphase vorzusehen, um alle relevanten Interessenträger in staatlichen und öffentlichen Stellen und im Privatsektor zu identifizieren.
- **Festlegung einer zentralen Stelle, die für die Durchführung der Selbstbewertung auf nationaler Ebene zuständig ist.** Da das Zusammentragen von Material für alle Indikatoren des NCAF viele Interessenträger betreffen kann, wird empfohlen, eine zentrale Stelle oder Agentur mit der Durchführung der Selbstbewertung zu beauftragen, indem sie mit allen relevanten Interessenträgern in Kontakt tritt und diese koordiniert.
- **Verwendung der Bewertungsübung, um Cybersicherheitsthemen auszutauschen und zu kommunizieren.** Die von den Mitgliedstaaten ausgetauschten Erkenntnisse zeigten, dass Diskussionen (ob im Format von Einzelbefragungen oder kollektiven Workshops) eine gute Gelegenheit sind, den Dialog über Cybersicherheitsthemen zu fördern und gemeinsame Ansichten und verbesserungswürdige Bereiche auszutauschen. Der Austausch von Ergebnissen kann nicht nur auf entscheidende Errungenschaften hinweisen, sondern auch zur Förderung von Cybersicherheitsthemen beitragen.
- **Verwendung der NCSS als Mittel, um die Ziele auszuwählen, die der Bewertung unterzogen werden sollen.** Die 17 Ziele, aus denen sich der NCAF zusammensetzt, wurden auf der Grundlage der Ziele erstellt, die die Mitgliedstaaten in ihrer NCSS üblicherweise abdecken. Die im Rahmen der NCSS abgedeckten Ziele sollten als Mittel zur Bestimmung des Umfangs der Bewertung herangezogen werden. Die NCSS sollte die Bewertung jedoch nicht einschränken. Da sich die NCSS natürlich auf Prioritäten konzentriert, werden bestimmte Bereiche absichtlich nicht in die NCSS aufgenommen. Dies bedeutet jedoch nicht, dass eine bestimmte Fähigkeit nicht vorhanden ist. Wenn beispielsweise ein bestimmtes Ziel in der NCSS nicht aufgeführt ist, das Land jedoch über Cybersicherheitsfähigkeiten in Bezug auf dieses Ziel verfügt, kann dieses Ziel in die Bewertung einbezogen werden.
- **Wenn sich der NCSS-Umfang weiterentwickelt, ist sicherzustellen, dass die Interpretation des Ergebnisses der NCSS-Entwicklung folgt.** Der NCSS-Lebenszyklus ist ein mehrjähriger Prozess. Die NCSS einiger Mitgliedstaaten werden normalerweise in einem 3- bis 5-Jahresplan umgesetzt, wobei sich der Umfang zwischen zwei aufeinanderfolgenden NCSS-Ausgaben ändern kann. Daher muss bei der Darstellung der Ergebnisse der Selbstbewertung zwischen zwei NCSS-Ausgaben besonders sorgfältig vorgegangen werden: Änderungen des Umfangs können sich durchaus auf das endgültige Bewertungsergebnis des Reifegrads auswirken. Es wird empfohlen, die Bewertungen über die gesamten strategischen Ziele von einem Jahr zum anderen zu vergleichen (d. h. die allgemeine Gesamtbewertung).

Hinweis zum Bewertungsschema – Beispiel für die Abdeckungsquote
Das Bewertungsschema umfasst zwei Bewertungsergebnisse:
(i) Eine **allgemeine Gesamtabdeckungsquote** auf der Grundlage der vollständigen Liste der im Selbstbewertungsrahmen enthaltenen strategischen Ziele und

(ii) eine **spezifische Gesamtabdeckungsquote** auf der Grundlage der vom Mitgliedstaat ausgewählten strategischen Ziele (in der Regel entsprechend den in der NCSS des jeweiligen Landes festgelegten Zielen).

Aufgrund des gewählten Ansatzes (siehe Abschnitt 3.1 über das Bewertungsschema) wird die spezifische Gesamtabdeckungsquote gleich oder höher als die allgemeine Gesamtabdeckungsquote sein, da letztere möglicherweise Ziele enthält, die nicht vom Mitgliedstaat abgedeckt werden, wodurch die allgemeine Gesamtabdeckungsquote niedriger ausfällt. Wenn ein Mitgliedstaat ein neues Ziel aufnimmt, wird sich die Gesamtabdeckungsquote erhöhen (d. h. es werden mehr Reifegradindikatoren abgedeckt), während sich der spezifische Gesamtreifegrad niedriger ausfallen kann (falls sich das neu aufgenommene Ziel in einem Anfangsstadium befindet und daher einen niedrigen Reifegrad aufweist).

- **Beachten Sie beim Ausfüllen des Fragebogens zur Selbstbewertung, dass das Hauptziel darin besteht, die Mitgliedstaaten beim Aufbau von Kapazitäten für Cybersicherheit zu unterstützen.** Daher wird empfohlen, beim Ausfüllen der Selbstbewertung die Antwort zu wählen, die im Allgemeinen akzeptiert wird, auch wenn es in bestimmten Situationen schwierig sein kann, die Frage eindeutig zu beantworten. Wenn die Antwort auf eine Frage beispielsweise in einem bestimmten Bereich JA lautet, in einem anderen Bereich jedoch NEIN, sollten die Mitgliedstaaten berücksichtigen, dass eine NEIN-Antwort eine Maßnahme erfordert, nämlich entweder einen Plan mit Abhilfemaßnahmen oder einen Plan mit Maßnahmen für einem verbesserungswürdigen Bereich, der bei künftigen Entwicklungen berücksichtigt werden muss.

5. NÄCHSTE SCHRITTE

5.1 ZUKÜNFTIGE VERBESSERUNGEN

In Befragungen von Vertretern der Mitgliedstaaten und während der Phase der Schreibtischstudie wurden die folgenden Empfehlungen zur Verbesserung des aktuellen Rahmens zur Bewertung nationaler Fähigkeiten als potenzielle künftige Entwicklungen ermittelt:

- **Weiterentwicklung des Bewertungssystems, um mehr Genauigkeit zu erreichen.** So könnte beispielsweise anstelle der binären JA/NEIN-Antwort ein Prozentsatz der Abdeckung eingeführt werden, um der Komplexität der Konsolidierung der Fähigkeiten auf nationaler Ebene besser Rechnung zu tragen. In einem ersten Schritt wurde ein einfacher Ansatz mit JA/NEIN-Antworten gewählt.
- **Einführung quantitativer Parameter zur Messung der Wirksamkeit der NCSS der Mitgliedstaaten.** In der Tat konzentriert sich der Rahmen zur Bewertung nationaler Fähigkeiten auf die Bewertung des Reifegrads der Cybersicherheitsfähigkeiten der Mitgliedstaaten. Dies könnte durch Parameter ergänzt werden, mit denen die Wirksamkeit der von den Mitgliedstaaten durchgeführten Aktivitäten und umgesetzten Aktionspläne zum Aufbau dieser Fähigkeiten gemessen werden kann. Es schien nicht realistisch, solche Wirksamkeitsparameter zum gegenwärtigen Zeitpunkt aufzustellen, da es nur wenige Rückmeldungen aus der Praxis gibt, es schwierig ist, aussagekräftige Indikatoren zu finden, die das Ergebnis mit der Umsetzung der NCSS verknüpfen, und es ferner schwierig ist, realistische Indikatoren zu bilden, die anschließend zusammengetragen werden können. Dies bleibt jedoch ein Thema für die zukünftige Arbeit.
- **Übergang von einer Selbstbewertungsübung zu einem Bewertungskonzept.** Eine mögliche zukünftige Entwicklung des Rahmens könnte die Umstellung auf ein Bewertungskonzept sein, um die Reife der Mitgliedstaaten in Bezug auf Cybersicherheitsfähigkeiten in einheitlicherer Weise zu bewerten. Wenn ein Dritter die Bewertung durchführt, kann dies möglicherweise potenzielle Verzerrungen minimieren.

ANHANG A – ÜBERSICHT ÜBER DIE ERGEBNISSE DER SCHREIBTISCHSTUDIE

Anhang A enthält eine Zusammenfassung der früheren Arbeiten der ENISA zu NCSS und eine Überprüfung der einschlägigen öffentlich verfügbaren Reifegradmodelle für Cybersicherheitskapazitäten. Folgende Annahmen werden bei der Auswahl und Überprüfung der Modelle berücksichtigt:

- Nicht alle Modelle basieren auf einer strengen Forschungsmethode.
- Die Struktur und die Ergebnisse der Modelle werden nicht immer ausführlich erklärt und es sind nicht immer eindeutige Verknüpfungen zwischen den verschiedenen Elementen, die jedes Modell charakterisieren, erkennbar.
- Einige Modelle umfassen keine Einzelheiten zum Entwicklungsprozess, zur Struktur und zur Bewertungsmethode.
- Andere Modelle und Instrumente, die wir gefunden haben, umfassen keine Einzelheiten zu Struktur und Inhalt und sind daher nicht aufgeführt.
- Die Auswahl der zu überprüfenden Modelle basiert auf dem geografischen Erfassungsbereich. Das Hauptaugenmerk wird auf Reifegradmodellen für Cybersicherheitskapazitäten liegen, die zur Bewertung der Leistung europäischer Länder entwickelt wurden. Es ist jedoch wichtig, den geografischen Erfassungsbereich zu erweitern, um bewährte Verfahren für die Erstellung von Reifegradmodellen weltweit zu analysieren.

Diese systematische Überprüfung relevanter öffentlich verfügbarer Reifegradmodelle für Cybersicherheitskapazitäten wurde unter Verwendung eines maßgeschneiderten Analyserahmens durchgeführt, der auf der von Becker für die Entwicklung von Reifegradmodellen definierten Methodik[22] basiert. Die folgenden Elemente wurden für jedes vorhandene Reifegradmodell analysiert:

- **Bezeichnung des Reifegradmodells:** Die Bezeichnung des Reifegradmodells und die Hauptreferenzen
- **Ursprungsorganisation:** Die Einrichtung/Organisation (öffentlich oder privat), die für das Modellkonzept verantwortlich ist
- **Allgemeiner Zweck und Ziel:** Der allgemeine Zweck des Modells und das/die beabsichtigten Ziel(e)
- **Anzahl und Definition der Reifegrade:** Die Anzahl der Reifegrade des Modells sowie deren allgemeine Beschreibung
- **Anzahl und Bezeichnung der Attribute:** Die Anzahl und Bezeichnung der Attribute, die das Reifegradmodell verwendet. Die Analyse der Attribute hat ein dreifaches Ziel:
  - Unterteilung des Reifegradmodells in leicht verständliche Abschnitte
  - Zusammenfassung mehrerer Attribute zu Attributclustern, die dasselbe Ziel erreichen
  - Aufzeigen unterschiedlicher Sichtweisen auf das Thema des Reifegrades.
- **Bewertungsmethode:** Die Methode zur Bewertung des Reifegradmodells

[22] J. Becker, R. Knackstedt, and J. Pöppelbuß, „Developing Maturity Models for IT Management: A Procedure Model and its Application“, Business & Information Systems Engineering, Band 1, Nr. 3, S. 213-222, Juni 2009.

- **Ergebnisdarstellung:** Festlegung der Visualisierungsmethode für die Ergebnisse des Reifegradmodells. Die Logik hinter diesem Schritt besteht darin, dass Reifegradmodelle dazu neigen, zu scheitern, wenn sie zu komplex sind, und daher muss die Darstellungsweise dem praktischen Bedarf entsprechen.

Frühere Arbeiten zu NCSS

Die ENISA veröffentlichte 2012 im Rahmen ihrer frühen Arbeiten zwei Dokumente zum Thema NCSS. Zunächst wurde im praktischen Leitfaden für die Entwicklungs- und Umsetzungsphase von NCSS[23] eine Reihe konkreter Maßnahmen zur wirksamen Implementierung einer NCSS vorgeschlagen und der Lebenszyklus einer NCSS in vier Phasen vorgestellt: Strategieentwicklung, Strategieumsetzung, Strategiebewertung und Strategiepflege. Zweitens wurde in einem Dokument zur Ausrichtung des Kurses für nationale Bemühungen zur Stärkung der Sicherheit im Cyberspace[24] der Status von Cybersicherheitsstrategien innerhalb der EU und darüber hinaus im Jahr 2012 dargelegt und vorgeschlagen, dass die Mitgliedstaaten gemeinsame Themen und Unterschiede zwischen ihren NCSS bestimmen sollten.

Im Jahr 2014 wurde der erste ENISA-Rahmen zur Bewertung der NCSS eines Mitgliedstaats veröffentlicht.[25] Dieser Rahmen enthält Empfehlungen und bewährte Verfahren sowie eine Reihe von Instrumenten zum Kapazitätenaufbau zur Bewertung einer NCSS (z. B. identifizierte Ziele, Inputs, Outputs, wichtige Leistungsindikatoren usw.). Diese Instrumente werden in ihrer strategischen Planung an die unterschiedlichen Bedürfnisse von Ländern mit unterschiedlichem Reifegrad angepasst. Im selben Jahr veröffentlichte die ENISA eine interaktive Online-Karte zu NCSS[26], mit der Benutzer schnell die NCSS aller Mitgliedstaaten und EFTA-Länder konsultieren können, einschließlich ihrer strategischen Ziele und guter Beispiele für die Umsetzung. Die Karte wurde als erstes NCSS-Verzeichnis (2014) entwickelt und 2018 mit Umsetzungsbeispielen aktualisiert. Seit 2019 dient sie nun als *Informationsdrehscheibe* zur Zentralisierung der von den Mitgliedstaaten bereitgestellten Daten über ihre Bemühungen zur Verbesserung der nationalen Cybersicherheit.

Der im Jahr 2016 veröffentlichte NCSS-Leitfaden über bewährte Verfahren („NCSS Good Practice Guide“)[27] beschreibt 15 strategische Ziele. In diesem Leitfaden wird auch der Umsetzungsstatus der NCSS jedes Mitgliedstaats analysiert und es werden verschiedene Lücken und Herausforderungen in Bezug auf diese Umsetzung ermittelt.

Im Jahr 2018 veröffentlichte die ENISA daraufhin das Nationale Cybersicherheitsstrategie-Bewertungsinstrument[28]. Dabei handelt es sich um ein interaktives Instrument zur Selbstbewertung, mit dem die Mitgliedstaaten ihre strategischen Prioritäten und Ziele im

[23] NCSS: Practical Guide on Development and Execution (ENISA, 2012).
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012).
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] An evaluation framework for NCSS (ENISA, 2014).
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] National Cybersecurity Strategies - Interactive Map (ENISA 2014, aktualisiert 2019).
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Dieses Dokument ersetzt den Leitfaden von 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016).
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] National Cybersecurity Strategies Evaluation Tool (2018).
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Zusammenhang mit ihrer NCSS bewerten können. Durch eine Reihe einfacher Fragen liefert dieses Instrument den Mitgliedstaaten spezifische Empfehlungen für die Umsetzung jedes Ziels. Schließlich wird in den 2019 veröffentlichten bewährten Verfahren bei Innovationen im Bereich der Cybersicherheit im Rahmen der NCSS („Good practices in innovation on Cybersecurity under the NCSS“)[29] das Thema Innovation in Bezug auf Cybersicherheit im Rahmen der NCSS vorgestellt. Das Dokument enthält Herausforderungen und bewährte Verfahren in den verschiedenen Innovationsdimensionen aus der Sicht von sachkundigen Sachverständigen, um bei der Ausarbeitung künftiger innovativer strategischer Ziele zu helfen.

A.1 Reifegradmodell für Cybersicherheitskapazitäten für Nationen (CMM)

Das Reifegradmodell für Cybersicherheitskapazitäten für Nationen (CMM) wurde vom Global Cyber Security Capacity Centre entwickelt, dem Kapazitätszentrum der Oxford Martin School an der Universität von Oxford. Ziel des Kapazitätszentrums ist es, den Umfang und die Wirksamkeit des Aufbaus von Cybersicherheitskapazitäten – sowohl in Großbritannien als auch international – durch den Einsatz des Reifegradmodells für Cybersicherheitskapazitäten (CMM) zu verbessern. Das CMM richtet sich gezielt an Länder, die ihre nationale Cybersicherheitskapazitäten erhöhen möchten. Das im Jahr 2014 erstmals eingesetzte CMM wurde 2016 überarbeitet, nachdem es bei der Überprüfung von 11 nationalen Cybersicherheitskapazitäten verwendet wurde.

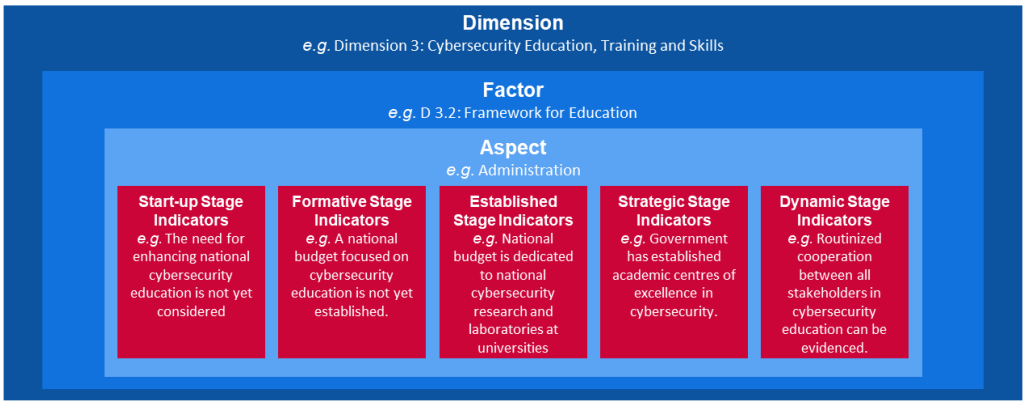
Attribute/Dimensionen

Im CMM umfasst die Cybersicherheitskapazität **fünf Dimensionen**, die die Cluster der Cybersicherheitskapazität darstellen. Jeder Cluster stellt eine andere Forschungsperspektive dar, anhand derer die Cybersicherheitskapazität untersucht und verstanden werden kann. Innerhalb der fünf Dimensionen beschreiben **Faktoren** die Einzelheiten des Vorhandenseins von Cybersicherheitsfähigkeiten. Dies sind Elemente, die zur Verbesserung der Reife der Cybersicherheitskapazität in jeder Dimension beitragen. Für jeden Faktor repräsentieren verschiedene **Aspekte** unterschiedliche Komponenten des Faktors. Aspekte stellen eine organisatorische Methode dar, um Indikatoren in kleinere Cluster zu unterteilen, die leichter zu verstehen sind. Jeder Aspekt wird sodann anhand von **Indikatoren** bewertet, um die Schritte, Maßnahmen oder Bausteine zu beschreiben, die auf einen bestimmten Reifegrad (im nächsten Abschnitt definiert) innerhalb eines bestimmten Aspekts, eines bestimmten Faktors und einer bestimmten Dimension hinweisen.

Die vorstehend genannten Begriffe können, wie in der nachstehenden Abbildung gezeigt, geschichtet werden.

Abbildung 4: Zu CMM-Indikatoren

[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1



Dimension
e.g. Dimension 3: Cybersecurity Education, Training and Skills

Factor
e.g. D 3.2: Framework for Education

Aspect
e.g. Administration

Start-up Stage Indicators
e.g. The for enhancing national cybersecurity education is not yet considered

Formative Stage Indictors
e.g. A national budget focused on cybersecurity education is not yet established

Established Stage Indicators
e.g. National budget is dedicated to national cybersecurity research and laboratories at universities

Strategic Stage Indicators
e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.

Dynamic Stage Indicators
e.g. Routinized cooperation between all stakeholder

Dimension
z. B. Dimension 3: Bildung, Ausbildung und Schulung sowie Kompetenzen im Bereich Cybersicherheit

Faktor
z. B. D 3.2: Bildungsrahmen

Aspekt
z. B. Verwaltung

Indikatoren für die Start-up-Phase
z. B. die Indikatoren zur Verbesserung der nationalen Cybersicherheitsausbildung sind noch nicht berücksichtigt

Indikatoren für die Festlegungsphase
z. B. nationale Haushaltsmittel für Cybersicherheitsausbildung sind noch nicht bereitgestellt

Indikatoren für die Einführungsphase
z. B. nationale Haushaltsmittel für nationale Cybersicherheitsforschung und zugehörige Labors an den Universitäten wurden zugewiesen

Indikatoren für die Strategiephase
z. B. von staatlicher Seite wurde ein akademisches Kompetenzzentrum für Cybersicherheit eingerichtet

Indikatoren für die dynamische Phase
z. B. routinierte Zusammenarbeit aller Interessenträger in der Cybersicherheitsausbildung kann nachgewiesen werden

Die fünf Dimensionen sind nachstehend näher ausgeführt:

i Entwicklung einer Cybersicherheitspolitik und -strategie (6 Faktoren)
ii Förderung einer verantwortungsbewussten Cybersicherheitskultur in der Gesellschaft (5 Faktoren)
iii Entwicklung von Cybersicherheitswissen (3 Faktoren)
iv Schaffung von wirksamen rechtlichen und regulatorischen Rahmen (3 Faktoren)
v Risikokontrolle durch Normen, Organisationen und Technologien (7 Faktoren)

Reifegrade

Das CMM verwendet **5 Reifegrade,** um zu bestimmen, inwieweit ein Land in Bezug auf einen bestimmten Faktor/Aspekt der Cybersicherheitskapazität Fortschritte erzielt hat. Diese Grade dienen als Momentaufnahme der vorhandenen Cybersicherheitskapazität:

- **Start-up-Phase**: Zu diesem Zeitpunkt besteht entweder keine Reife in Bezug auf Cybersicherheit oder diese ist noch sehr unausgereift. Es kann erste Diskussionen über den Aufbau von Cybersicherheitskapazitäten geben, aber es wurden noch keine konkreten Maßnahmen ergriffen. Zu diesem Zeitpunkt fehlen beobachtbare Nachweise.
- **Festlegungsphase:** Es wurde damit begonnen, einige Merkmale der Aspekte zu entwickeln und festzulegen, sie können jedoch ad-hoc, unorganisiert, schlecht definiert oder einfach „neu“ sein. Der Nachweis dieser Aktivität kann jedoch eindeutig erbracht werden.
- **Einführungsphase**: Die Elemente des Aspekts sind vorhanden und funktionieren. Die relative Verteilung der Ressourcen ist jedoch noch nicht gut durchdacht. In Bezug auf die „relative“ Investition in die verschiedenen Elemente des Aspekts wurden nur wenige Kompromissentscheidungen getroffen. Der Aspekt ist jedoch funktional und definiert.

- **Strategiephase:** Es wurde entschieden, welche Teile des Aspekts wichtig und welche für die jeweilige Organisation oder das jeweilige Land weniger wichtig sind. Die Strategiephase spiegelt die Tatsache wider, dass diese Entscheidungen je nach den besonderen Umständen des Landes oder der Organisation getroffen wurden.
- **Dynamische Phase**: In dieser Phase bestehen klare Verfahren, um die Strategie je nach den vorherrschenden Umständen, wie z. B. der Technologie der Bedrohungsumgebung, globalen Konflikten oder einer signifikanten Änderung in einem Problembereich (z. B. Cyberkriminalität oder Datenschutz), zu ändern. Dynamische Organisationen haben Methoden entwickelt, um Strategien den sich ggf. ändernden Umständen entsprechend zu ändern. Diese Phase ist gekennzeichnet durch schnelle Entscheidungsfindung, Umverteilung von Ressourcen und ständige Aufmerksamkeit für das sich ändernde Umfeld.

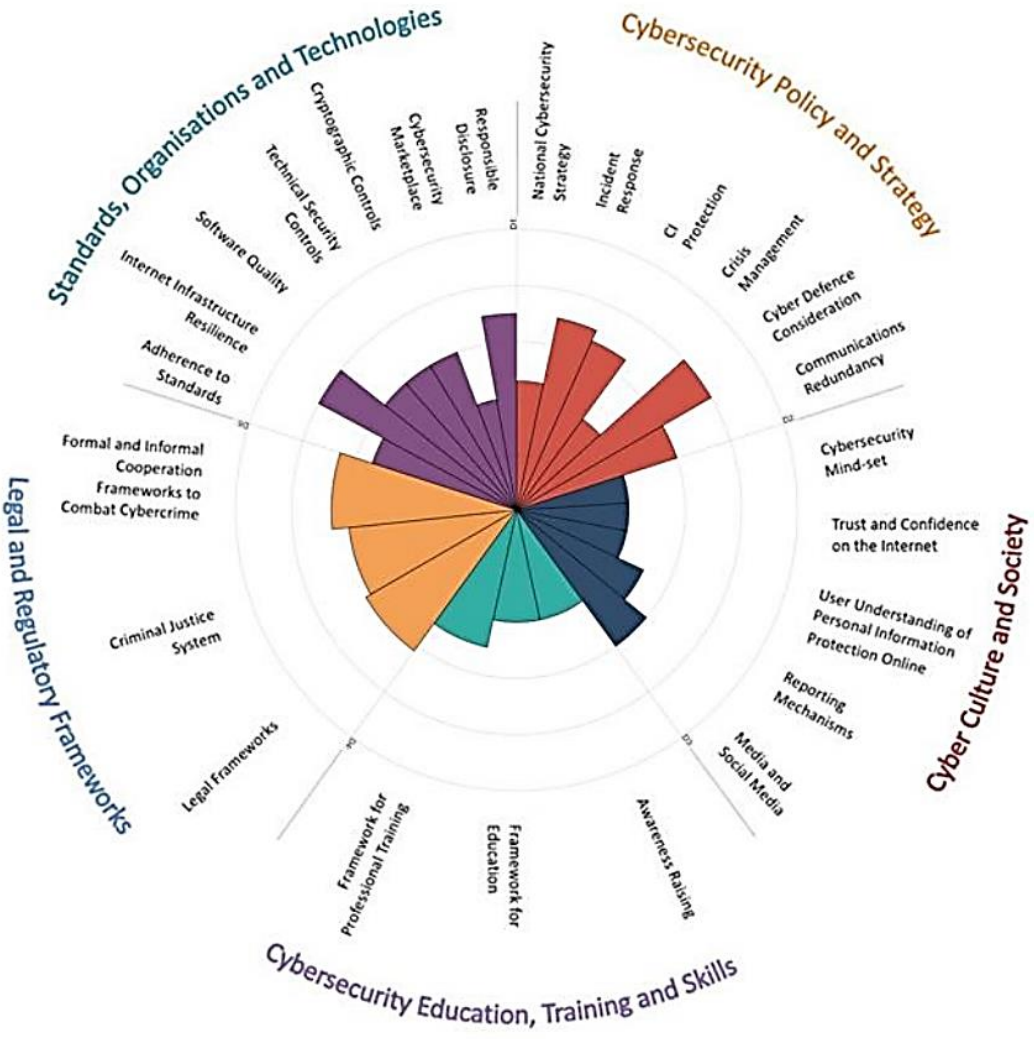
Bewertungsmethode

Da das Kapazitätszentrum nicht über ein gründliches und eingehendes Verständnis der einzelnen nationalen Kontexte verfügt, in denen das Modell eingesetzt wird, arbeitet es mit internationalen Organisationen sowie mit Ministerien oder Organisationen im jeweiligen Land zusammen, um den Reifegrad der Cybersicherheitskapazität zu überprüfen. Um den Reifegrad der fünf im CCM enthaltenen Dimensionen zu bewerten, treffen sich das Kapazitätszentrum und die Organisation des Landes innerhalb von zwei oder drei Tagen mit relevanten nationalen Interessenträgern des öffentlichen und privaten Sektors, um Fokusgruppen zu den Dimensionen durchzuführen. Jede Dimension wird mindestens zweimal von verschiedenen Gruppen von Interessenträgern erörtert. Dies bildet den vorläufige Datenpool für die folgende Bewertung.

Modus oder Darstellung der Ergebnisse

Das CCM bietet einen Überblick über den Reifegrad jedes Landes über ein Radar, das aus fünf Abschnitten besteht, einen für jede Dimension. Jede Dimension repräsentiert ein Fünftel der Grafik, wobei sich die fünf Reifegrade für jeden Faktor von der Mitte der Grafik nach außen erstrecken. Wie nachstehend gezeigt, befindet sich „Start-up“ nahe der Mitte der Grafik und „Dynamisch“ ganz außen.

Abbildung 5 CMM: Übersicht der Ergebnisse



Standards, Organisations and Technologies	Normen, Organisationen und Technologien
Legal Regulatory Frameworks	Rechtliche Rahmenbedingungen
Cybersecurity Education, Training and Skills	Bildung, Ausbildung und Schulung sowie Kompetenzen im Bereich Cybersicherheit
Cybersecurity Policy and Strategy	Cybersicherheitsleitlinien und -strategien
Cyber Culture and Society	Cyberkultur und Gesellschaft
Responsible Disclosure	Verantwortungsbewusste Offenlegung
Cybersecurity market place	Marktplatz für Cybersicherheit
Technical Security Controls	Technische Sicherheitskontrollen
Cryptographic Controls	Kryptografische Kontrollen
Software Quality	Softwarequalität
Internet Infrastructure Resilience	Resilienz der Internetinfrastruktur
Adherence to Standards	Einhaltung von Standards
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formeller und informeller Kooperationsrahmen zur Bekämpfung von Cyberkriminalität
Criminal Justice System	Strafrechtssystem
Legal Frameworks	Rechtsrahmen
Framework for Professional Training	Rahmen für professionelle Schulung/Ausbildung
Framework for Education	Bildungsrahmen
Awareness Raising	Sensibilisierung

Media and Social Medai	Medien und soziale Medien
Reporting Mechanisms	Meldeverfahren
User Understanding of Personal Information Protection Online	Benutzerverständnis zum Schutz personenbezogener Daten online
Trust and Confidence on the Internet	Vertrauen im Internet
Cybersecurity Mind-set	Cybersicherheitsmentalität
Communications Redundancy	Kommunikationsredundanz
Cyber Defence Consideration	Überlegungen zur Cyberabwehr
Crisis Management	Krisenmanagement
CI Protection	Schutz kritischer Infrastrukturen
Incident Response	Reaktion auf Sicherheitsvorfälle
National Cybersecurity Strategy	Nationale Cybersicherheitsstrategie

Global Cyber Security Capacity Centre, Oxford Martin School, Universität Oxford, 2017.

A.2 Reifegradmodell für Cybersicherheitskapazitäten (C2M2)

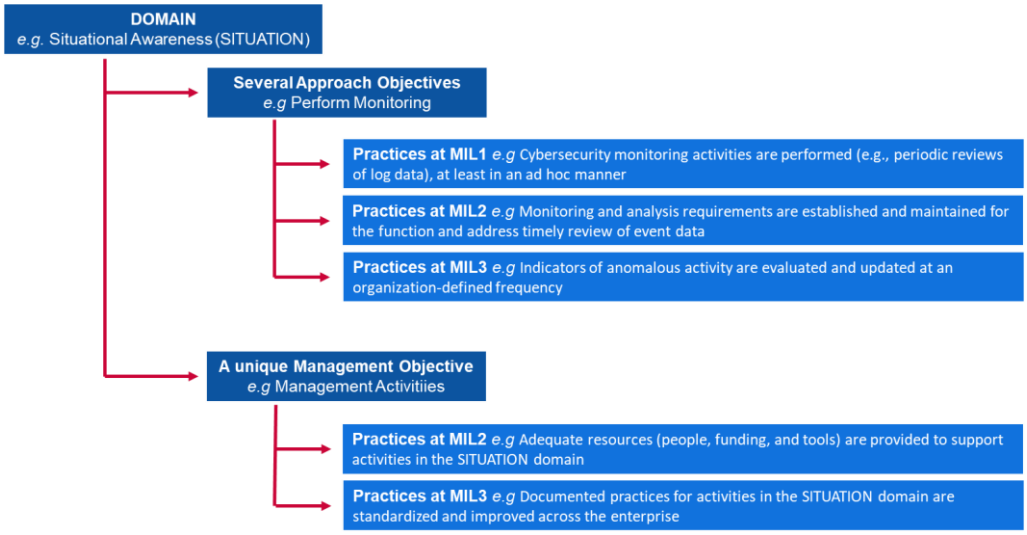
Das Reifegradmodell für Cybersicherheitskapazitäten (C2M2) wurde vom US-Energieministerium in Zusammenarbeit mit Sachverständigen des privaten und öffentlichen Sektors entwickelt. Ziel des Kapazitätszentrums ist es, Organisationen aller Sektoren, Arten und Größen dabei zu unterstützen, ihre Cybersicherheitsprogramme zu bewerten und zu verbessern und die Betriebssicherheit digitaler Systeme zu stärken. Das C2M2 konzentriert sich auf die Einführung und Verwaltung von Cybersicherheitsverfahren im Zusammenhang mit Ressourcen in den Bereichen Information, Informationstechnologie (IT) und Betriebstechnologie (OT) sowie den Umgebungen, in denen sie betrieben werden. Das C2M2 definiert Reifegradmodelle als: „Eine Reihe von Merkmalen, Attributen, Indikatoren oder Mustern, die die Kapazitäten und den Fortschritt in einer bestimmten Disziplin darstellen“. Das C2M2 wurde 2014 erstmals eingesetzt und 2019 überarbeitet.

Attribute/Dimensionen

Das C2M2 berücksichtigt **zehn Bereiche**, die eine logische Gruppierung von Cybersicherheitsverfahren darstellen. Jede Reihe von Verfahren stellt die Aktivitäten dar, die eine Organisation ausführen kann, um Fähigkeiten in dem Bereich zu etablieren und zu entwickeln. Jeder Bereich ist dann einem **einzigen Managementziel** und **mehreren Konzeptzielen** zugeordnet. Sowohl im Rahmen der Konzept- als auch der Managementziele werden **verschiedene Verfahren** detailliert beschrieben, um institutionalisierte Aktivitäten zu beschreiben.

Die Beziehung zwischen diesen Begriffen ist nachstehend zusammengefasst:

Abbildung 6: Zum C2M2-Indikator



Domain eg Situational Awareness (SITUATION)	**Bereich**, z. B. Lagebewusstsein (LAGE)
Several Approaches Objectives e.g. Perform Monitoring	**Mehrere Konzeptziele**, z. B. Durchführung der Überwachung
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Verfahren bei MIL1**, z. B. Cybersicherheitsüberwachungsaktivitäten werden zumindest ad hoc durchgeführt (z. B. regelmäßige Überprüfungen von Protokolldaten)
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Verfahren bei MIL2**, z. B. Überwachungs- und Analyseanforderungen werden für die Funktion festgelegt und aufrechterhalten und umfassen die rechtzeitige Überprüfung von Ereignisdaten
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Verfahren bei MIL3**, z. B. Indikatoren für anomale Aktivität, werden mit einer organisationsdefinierten Häufigkeit bewertet und aktualisiert
A unique Management Objectve e.g. Management Activities	Ein einziges Managementziel, z. B. Management-Aktivitäten
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Verfahren bei MIL2**, z. B. angemessene Ressourcen (Personen, Finanzmittel und Instrumente) werden bereitgestellt, um Aktivitäten im Bereich LAGE zu unterstützen
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Verfahren bei MIL3**, z. B. dokumentierte Verfahren für Aktivitäten im Bereich LAGE werden im gesamten Unternehmen standardisiert und verbessert

Die zehn Bereiche werden nachstehend näher ausgeführt:

i Risikomanagement (RISIKO)
ii Anlagen-, Änderungs- und Konfigurationsmanagement (ANLAGEN)
iii Identitäts- und Zugangsmanagement (ZUGANG)
iv Bedrohungs- und Sicherheitslückenmanagement (BEDROHUNG)
v Lagebewusstsein (LAGE)
vi Reaktion auf Ereignisse und Sicherheitsvorfälle (REAKTION)
vii Lieferketten- und externes Abhängigkeitsmanagement (ABHÄNGIGKEITEN)
viii Personalmanagement (PERSONAL)
ix Cybersicherheitsarchitektur (ARCHITEKTUR)
x Verwaltung von Cybersicherheitsprogrammen (PROGRAMM)

Reifegrade

Das C2M2 verwendet **4 Reifegrade** (Maturity Indicator Levels, MIL), um den Fortschritt der Reife auf zweifache Weise zu bestimmen: Fortschritte im Konzept und Fortschritte beim Management. Die MIL-Grade reichen von MIL0 bis MIL3 und sollen unabhängig auf jeden Bereich angewendet werden.

- **MIL0**: Es werden keine Verfahren durchgeführt.
- **MIL1**: Erste Verfahren werden durchgeführt, können jedoch ad hoc erfolgen.
- **MIL2**: Managementmerkmale:
  - Verfahren werden dokumentiert
  - Zur Unterstützung des Prozesses werden angemessene Ressourcen bereitgestellt
  - Das Personal, das die Verfahren durchführt, verfügt über angemessene Kompetenzen und Kenntnisse

- Verantwortung und Entscheidungskompetenz für die Durchführung der Verfahren werden zugewiesen.

Konzeptmerkmale:

- Die Verfahren sind vollständiger bzw. weiter fortgeschritten als bei MIL1.

- **MIL3**: Managementmerkmale:
  - Die Aktivitäten richten sich nach Leitlinien (oder anderen Bestimmungen der Organisation).
  - Leistungsziele für Bereichsaktivitäten werden festgelegt und überwacht, um die Leistung zu verfolgen.
  - Dokumentierte Verfahren für Bereichsaktivitäten werden unternehmensweit standardisiert und verbessert.

  Konzeptmerkmale:
  - Die Verfahren sind vollständiger oder weiter fortgeschritten als bei MIL2.

Bewertungsmethode

Das C2M2 wurde für die Verwendung mit einer **Selbstbewertungsmethode** und einem Toolkit (auf Anfrage erhältlich) entwickelt, mit denen eine Organisation ihr Cybersicherheitsprogramm bewerten und verbessern kann. Eine Selbstbewertung mit dem Toolkit kann an einem Tag abgeschlossen werden, das Toolkit kann jedoch auch für strengere Bewertungen entsprechend angepasst werden. Darüber hinaus kann das C2M2 als Orientierung für die Entwicklung eines neuen Cybersicherheitsprogramms verwendet werden.

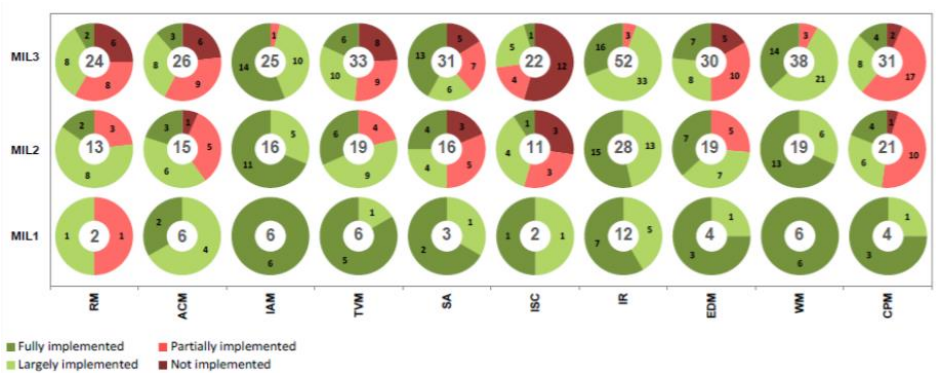
Der Inhalt des Modells wird stark abstrahiert dargestellt, sodass er von Organisationen verschiedener Arten, Strukturen, Größen und Branchen interpretiert werden kann. Eine breite Anwendung des Modells in einem Sektor kann das Benchmarking der Cybersicherheitsfähigkeiten des Sektors unterstützen.

Modus oder Darstellung der Ergebnisse

Das C2M2 bietet einen Bewertungsbericht, der aus den Umfrageergebnissen generiert wird. Der Bericht präsentiert die Ergebnisse in zwei Ansichten: In der Zielansicht, in der die Antworten auf Praxisfragen nach Bereichen und ihren Zielen angezeigt werden, und in der Bereichsansicht, in der die Antworten für alle Bereiche und MIL angezeigt werden. Beide Ansichten zeigen Kreisdiagramme (bzw. „Donuts“) –, ein Kreisdiagramm pro Antwort – und verwenden ein Ampelsystem für das Bewertungsschema. Wie in Abbildung 7 ersichtlich, zeigen die roten Abschnitte in einem Donut-Diagramm die Anzahl der Fragen an, die bei der Umfrage mit „Nicht eingeführt“ (dunkelrot) oder „Teilweise eingeführt“ (hellrot) beantwortet wurden. Die grünen Abschnitte zeigen die Anzahl der Fragen an, die mit „Weitgehend eingeführt“ (hellgrün) oder „Vollständig eingeführt“ (dunkelgrün) beantwortet wurden.

Nachstehende Abbildung 7 zeigt ein Beispiel für eine Bewertungskarte nach abgeschlossener Reifegradbewertung. Auf der X-Achse befinden sich die 10 Bereiche des C2M2 und auf der Y-Achse die Reifegrade (MIL). Betrachtet man auf der Grafik den Bereich Risikomanagement (RM), sind drei Kreisdiagramme zu sehen, von denen eines jeweils einem Reifegrad MIL1, MIL2 und MIL3 entspricht. Für den Bereich RM wird in der Grafik gezeigt, dass zwei Elemente bewertet werden müssen, um den ersten Reifegrad (MIL1) zu erreichen. In diesem Fall gibt es eine Bewertung „Weitgehend eingeführt“ und eine Bewertung „Teilweise eingeführt“. Für den zweiten Reifegrad (MIL2) sieht das Modell 13 zu bewertende Posten vor. Zwei dieser 13 Elemente gehören zur ersten Stufe (MIL1), und 11 zur zweiten Stufe (MIL2). Gleiches gilt für die dritte Reifegradstufe (MIL3).

Abbildung 7: C2M2 – Bereichsansicht (Beispiel)



Fully implemented	Vollständig eingeführt
Largely implemented	Weitgehend eingeführt
Partially implemented	Teilweise eingeführt
Not implemented	Nicht eingeführt
MIL1	MIL1
MIL2	MIL2
MIL3	MIL3
RM	Risikomanagement
ACM	Anlagen-, Änderungs- und Konfigurationsmanagement
IAM	Identitäts- und Zugangsmanagement
TVM	Bedrohungs- und Sicherheitslückenmanagement
SA	Lagebewusstsein
ISC	Informationsaustausch und Kommunikation
IR	Reaktion auf Ereignisse und Sicherheitsvorfälle
EDM	Lieferketten- und externes Abhängigkeitsmanagement
WM	Personalmanagement
CPM	Verwaltung von Cybersicherheitsprogrammen

Quelle: U.S. Department of Energy, Office of electricity delivery and energy reliability, 2015.

A.3 Rahmen zur Verbesserung der Cybersicherheit kritischer Infrastrukturen

Der Rahmen zur Verbesserung der Cybersicherheit kritischer Infrastrukturen wurde vom Nationalen Institut für Standards und Technologie (NIST) entwickelt. Dabei geht es um die Steuerung von Cybersicherheitsaktivitäten und den Umgang mit Risiken innerhalb einer Organisation. Er richtet sich an alle Arten von Organisationen, unabhängig von Größe, Grad des Cybersicherheitsrisikos oder der Komplexität der Cybersicherheit. Da es sich um einen Rahmen und nicht um ein Modell handelt, unterscheidet sich sein Aufbau von den vorstehend behandelten Modellen.

Der Rahmen besteht aus drei Teilen: dem Rahmenkern, den Implementierungsebenen und den Rahmenprofilen:

- Der **Rahmenkern** besteht aus einer Reihe von Cybersicherheitsaktivitäten, gewünschten Ergebnissen und anwendbaren Referenzen, die in allen kritischen Infrastruktursektoren üblich sind. Sie ähneln den Attributen oder Dimensionen der Reifegradmodelle für Cybersicherheitskapazitäten.
- Die **Implementierungsebenen des Rahmens** bieten einen Kontext dazu, wie eine Organisation das Cybersicherheitsrisiko und die Prozesse zur Steuerung dieses

Risikos betrachtet. Die Ebenen reichen von „Teilweise“ (Ebene 1) bis „Anpassungsfähig“ (Ebene 4) und beschreiben ein zunehmendes Maß an Stringenz und Komplexität bei den Risikomanagementverfahren für Cybersicherheit. Die Ebenen stellen keine Reifegrade dar, sondern sollen die Entscheidungsfindung der Organisation über das Risikomanagement im Bereich der Cybersicherheit unterstützen sowie in Bezug darauf, welche Dimensionen der Organisation eine höhere Priorität haben und zusätzliche Ressourcen erhalten könnten.

- Ein **Rahmenprofil** repräsentiert die Ergebnisse basierend auf den Geschäftsanforderungen, die eine Organisation aus den Kategorien und Unterkategorien des Rahmens ausgewählt hat. Das Profil kann im Hinblick auf die Anpassung von Standards, Leitlinien und Verfahren an den Rahmenkern in einem bestimmten Implementierungsszenario charakterisiert werden. Profile können verwendet werden, um Möglichkeiten zur Verbesserung der Cybersicherheitspositionierung zu ermitteln, indem ein „aktuelles“ Profil (Ist-Stand) mit einem „Ziel“-Profil (Soll-Stand) verglichen wird.

Rahmenkern

Der Rahmenkern besteht aus fünf **Funktionen.** Zusammengenommen bieten diese Funktionen eine allgemeine strategische Sicht auf den Lebenszyklus des Managements des Cybersicherheitsrisikos einer Organisation. Der Rahmenkern identifiziert dann die zugrunde liegenden **Schlüsselkategorien** und **Unterkategorien** für jede Funktion und ordnet sie beispielhaften informativen Referenzen zu, z. B. vorhandenen Normen, Leitlinien und Verfahren für jede Unterkategorie.

Funktionen und Kategorien werden nachstehend näher ausgeführt:

i **Ermitteln:** Entwicklung eines organisatorischen Verständnisses für das Management von Cybersicherheitsrisiken für Systeme, Personen, Anlagen, Daten und Kapazitäten.
- Unterkategorien: Anlagenmanagement; Geschäftsumfeld; Governance; Risikobewertung; Risikomanagementstrategie

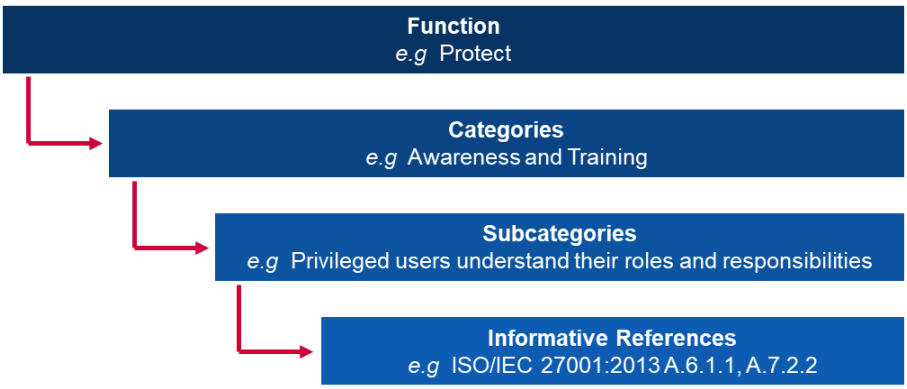
ii **Schützen:** Entwicklung und Einführung geeigneter Sicherheitsvorkehrungen, um die Bereitstellung kritischer Dienste sicherzustellen.
- Unterkategorien: Identitätsmanagement und Zugriffskontrolle; Sensibilisierung und Schulung/Ausbildung; Datensicherheit; Informationsschutzprozesse und -verfahren; Instandhaltung/Pflege; Schutztechnologie

iii **Erkennen:** Entwicklung und Umsetzung geeigneter Aktivitäten, um das Auftreten eines Cybersicherheitsvorfalles zu erkennen.
- Unterkategorien: Anomalien und Ereignisse; Kontinuierliche Sicherheitsüberwachung; Erkennungsverfahren

iv **Reagieren:** Entwicklung und Umsetzung geeigneter Aktivitäten, um Maßnahmen in Bezug auf einen erkannten Cybersicherheitsvorfall zu ergreifen.
- Unterkategorien: Reaktionsplanung; Kommunikation; Analyse; Schadensbegrenzung; Verbesserungen

v **Wiederherstellen:** Entwicklung und Umsetzung geeigneter Aktivitäten, um Pläne für die Betriebssicherheit digitaler Systeme (Resilienz) zu pflegen und alle Fähigkeiten oder Dienste wiederherzustellen, die aufgrund eines Cybersicherheitsvorfalls beeinträchtigt wurden.
- Unterkategorien: Wiederherstellungsplanung; Verbesserungen; Kommunikation

Abbildung 8: Zum Rahmen zur Verbesserung der Cybersicherheit kritischer Infrastrukturen



Function e.g Project	**Funktion** z. B. Projekt
Categories e.g Awarness and Training	**Kategorien** z. B. Sensibilisierung und Schulung/Ausbildung
Subcategories e.g Privileged useres understand their roles and responsibilities	**Unterkategorien** z. B. privilegierte Benutzer verstehen ihre Rollen und Verantwortlichkeiten
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Informative Referenzen** z. B. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Ebenen

Der Rahmen für die Verbesserung der Cybersicherheit kritischer Infrastrukturen basiert auf **4 Ebenen**, von denen jede hinsichtlich dreier Aspekte definiert ist: Risikomanagementprozess, integriertes Risikomanagementprogramm und externe Partizipation. Die Ebenen sind nicht als Reifegrad zu betrachten, sondern als Rahmen, um Organisationen eine Kontextualisierung ihrer Sichtweisen des Cybersicherheitsrisikos und der vorhandenen Verfahren zur Bewältigung dieses Risikos zu ermöglichen.

- **Ebene 1: Teilweise**
  - **Risikomanagementprozess**: Die Risikomanagementverfahren für die Cybersicherheit in Organisationen sind nicht formalisiert, und das Risikomanagement erfolgt ad hoc und bisweilen reaktiv.
  - **Integriertes Risikomanagementprogramm**: Auf organisatorischer Ebene besteht nur ein begrenztes Bewusstsein für das Cybersicherheitsrisiko. Die Organisation betreibt Risikomanagement für Cybersicherheit von unregelmäßig Fall zu Fall und verfügt möglicherweise nicht über Verfahren, mit denen Cybersicherheitsinformationen innerhalb der Organisation ausgetauscht werden können.
  - **Externe Partizipation**: Die Organisation versteht ihre Rolle im größeren Ökosystem weder in Bezug auf ihre Abhängigkeiten noch in Bezug auf die von ihr Abhängigen. Die Organisation ist sich im Allgemeinen der Risiken der Cyber-Lieferkette der von ihr angebotenen und verwendeten Produkte und Dienstleistungen nicht bewusst.
- **Ebene 2: Risikobewusst**
  - **Risikomanagementprozess**: Risikomanagementverfahren werden von der Leitung genehmigt, sind jedoch möglicherweise nicht als organisationsweite Leitlinie festgelegt.
  - **Integriertes Risikomanagementprogramm**: Auf organisatorischer Ebene besteht ein Bewusstsein für das Cybersicherheitsrisiko, ein organisationsweites Konzept für das Management des Cybersicherheitsrisikos wurde jedoch nicht festgelegt. Die Cyberrisikobewertung von organisatorischen und externen Vermögenswerten erfolgt, ist jedoch in der Regel nicht wiederholbar oder sich wiederholend.
  - **Externe Partizipation**: Im Allgemeinen versteht die Organisation ihre Rolle im größeren Ökosystem weder in Bezug auf ihre Abhängigkeiten noch in Bezug auf die von ihr Abhängigen. Darüber hinaus ist sich die Organisation der Risiken der Cyber-Lieferkette bewusst, die mit den von ihr angebotenen und verwendeten

Produkten und Dienstleistungen verbunden sind, reagiert jedoch nicht in einheitlicher bzw. formal festgelegter Weise auf diese Risiken.

- **Ebene 3: Wiederholbar**
  - **Risikomanagementprozess**: Die Risikomanagementverfahren der Organisation wurden formal genehmigt und als Leitlinie formuliert. Die Cybersicherheitsverfahren der Organisation werden regelmäßig auf der Grundlage der Anwendung von Risikomanagementverfahren bei Änderungen der Geschäfts-/Aufgabenanforderungen und einer sich ändernden Bedrohungs- und Technologielandschaft aktualisiert.
  - **Integriertes Risikomanagementprogramm**: Es gibt ein organisationsweites Konzept für das Management von Cybersicherheitsrisiken. Risikoinformierte Leitlinien, Prozesse und Verfahren werden wie beabsichtigt festgelegt, umgesetzt und überprüft. Führungskräfte stellen sicher, dass der Cybersicherheit in allen Geschäftsbereichen der Organisation Rechnung getragen wird.
  - **Externe Partizipation**: Die Organisation versteht ihre Rolle, ihre Abhängigkeiten und die von ihr Abhängigen im größeren Ökosystem und trägt möglicherweise zu einem breiteren Risikoverständnis der Gemeinschaft bei. Die Organisation ist sich im Allgemeinen der Risiken der Cyber-Lieferkette im Zusammenhang mit den von ihr angebotenen und verwendeten Produkten und Dienstleistungen bewusst.
- **Ebene 4: Anpassungsfähig**
  - **Risikomanagementprozess**: Die Organisation passt ihre Cybersicherheitsverfahren auf der Grundlage früherer und aktueller Cybersicherheitsaktivitäten an, einschließlich gewonnener Erkenntnisse und prädiktiver Indikatoren.
  - **Integriertes Risikomanagementprogramm**: Es gibt ein organisationsweites Konzept für das Management von Cybersicherheitsrisiken, bei dem risikoinformierte Leitlinien, Prozesse und Verfahren verwendet werden, um potenzielle Cybersicherheitsvorfällen zu bewältigen.
  - **Externe Partizipation**: Die Organisation versteht ihre Rolle, ihre Abhängigkeiten und die von ihr Abhängigen im größeren Ökosystem und trägt zu einem breiteren Risikoverständnis der Gemeinschaft bei.

Bewertungsmethode

Der Rahmen zur Verbesserung der Cybersicherheit kritischer Infrastrukturen soll es Organisationen ermöglichen, ihr Risiko selbst zu bewerten, um ihr Cybersicherheitskonzept und ihre Investitionen sachgerechter, wirksamer und werthaltiger zu gestalten. Um die Wirksamkeit von Investitionen zu prüfen, muss eine Organisation zunächst ein klares Verständnis ihrer Organisationsziele, der Beziehung dieser Ziele zueinander und der unterstützenden Ergebnisse in Bezug auf Cybersicherheit haben. Die Cybersicherheitsergebnisse des Rahmenkerns unterstützen die Selbstbewertung der Investitionswirksamkeit und der Cybersicherheitsaktivitäten.

A.4 Reifegradmodell für Cybersicherheitskapazitäten von Katar (Q-C2M2)

Das Reifegradmodell für Cybersicherheitskapazitäten von Katar (Q-C2M2) wurde 2018 von der rechtswissenschaftlichen Fakultät der Universität Katar entwickelt. Das Q-C2M2 basiert auf verschiedenen vorhandenen Modellen, um eine umfassende Bewertungsmethode zur Verbesserung des Cybersicherheitsrahmens in Katar zu erstellen.

Attribute/Dimensionen

Das Q-C2M2 übernimmt das Konzept des Rahmens des National Institute of Standards and Technology (NIST) und verwendet fünf Kernfunktionen als Hauptbereiche des Modells. Die fünf Kernfunktionen sind im katarischen Kontext anwendbar, da sie in allen kritischen Infrastruktursektoren gleich sind, die ein wichtiges Element im Rahmen der Cybersicherheit in Katar darstellen. Das Q-C2M2 basiert auf **fünf Bereichen**. Jeder Bereich wird dann in mehrere **Unterbereiche** unterteilt, um die gesamte Reifespanne der Cybersicherheitskapazitäten abzudecken.

Die fünf Bereiche sind nachstehend näher ausgeführt:

i Der Bereich „**Verstehen**“ enthält vier Unterbereiche: Governance, Anlagen, Risiken und Schulung/Ausbildung im Bereich Cybersicherheit
ii Zu den Unterbereichen unter dem Bereich „**Sichern**“ gehören Datensicherheit, Technologiesicherheit, Sicherheit der Zugriffskontrolle, Kommunikationssicherheit und Sicherheit des Personals.
iii Der Bereich „**Exponieren**“ umfasst die Unterbereiche Überwachung, Vorfallmanagement, Erkennung, Analyse und Exposition.
iv Der Bereich „**Reagieren**“ umfasst Reaktionsplanung, Schadensbegrenzung und Reaktionskommunikation.
v Der Bereich „**Erhalten**“ umfasst Wiederherstellungsplanung, Kontinuitätsmanagement, Verbesserung und externe Abhängigkeiten.

Reifegrade

Das Q-C2M2 verwendet **5 Reifegrade**, die die Kapazitätsreife einer staatlichen Stelle oder nichtstaatlichen Organisation im Hinblick auf die Kernfunktionen messen. Diese Reifegrade zielen darauf ab, die Reife in den fünf im vorstehenden Abschnitt beschriebenen Bereichen zu bewerten.

- **Erste Schritte**: Verwendet Ad-hoc-Cybersicherheitsverfahren und -prozesse in einigen Bereichen.
- **Einführung**: Verabschiedete Leitlinien zur Einführung aller Cybersicherheitsaktivitäten in den Bereichen mit dem Ziel, die Einführung zu einem bestimmten Zeitpunkt abzuschließen.
- **Entwicklung**: Eingeführte Leitlinien und Verfahren zur Entwicklung und Verbesserung der Cybersicherheitsaktivitäten in den Bereichen mit dem Ziel, neue Aktivitäten zur Einführung vorzuschlagen.
- **Anpassung**: Überdenken und Überprüfen der Cybersicherheitsaktivitäten und Annahme von Verfahren auf der Grundlage prädiktiver Indikatoren, die aus früheren Erfahrungen und Maßnahmen abgeleitet wurden.
- **Agilität**: Weiterführung der Anpassungsphase mit einem zusätzlichen Schwerpunkt auf Agilität und Geschwindigkeit bei der Einführung von Aktivitäten in den Bereichen.

Bewertungsmethode

Das Q-C2M2 befindet sich in einem frühen Forschungsstadium und ist noch nicht ausgereift, um eingeführt zu werden Es handelt sich um einen Rahmen, der verwendet werden könnte, um in Zukunft ein detailliertes Bewertungsmodell für katarische Organisationen bereitzustellen.

A.5 Zertifizierung des Reifegradmodells für Cybersicherheit (CMMC)

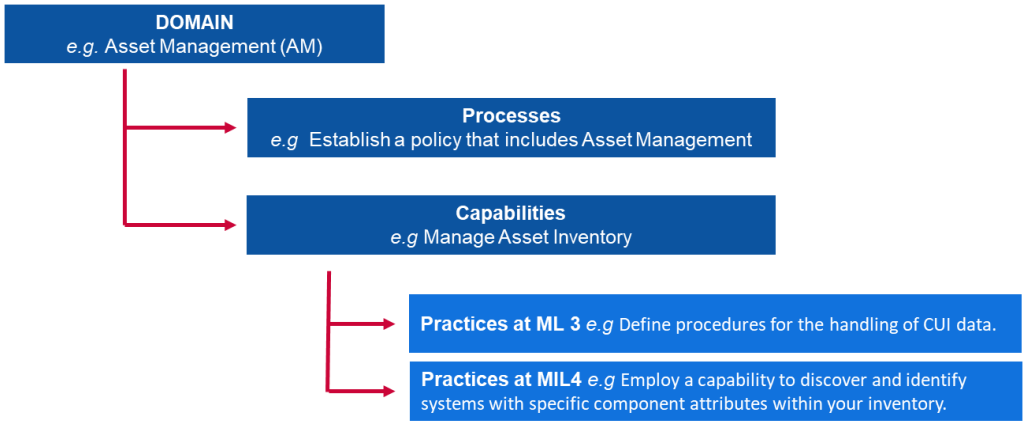
Die Zertifizierung des Reifegradmodells für Cybersicherheit (CMMC) wurde vom US-Verteidigungsministerium (DOD) in Zusammenarbeit mit der Carnegie Mellon Universität und dem Applied Physics Laboratory der Johns Hopkins Universität entwickelt. Das Hauptziel des DOD bei der Entwicklung dieses Modells ist der Schutz von Informationen aus der Rüstungsindustrie (DIB). Die Informationen, auf die sich die CMMC bezieht, sind entweder Vertragsinformationen des Bundes („Federal Contract Information“, FCI) – Informationen, die von der Regierung im Rahmen eines Vertrags bereitgestellt oder für diese generiert wurden und die nicht zur Veröffentlichung bestimmt sind – oder eingeschränkt zugängliche Informationen („Controlled Unclassified Information“, CUI) – Informationen, die gemäß Gesetzen, Vorschriften und staatlicher Politik geschützt werden müssen und nur eingeschränkt verbreitet werden dürfen. Durch die CMMC wird die Reife der Cybersicherheit gemessen und sie bietet bewährte Verfahren zusammen mit einer Zertifizierung, um die Anwendung der mit jedem Reifegrad verbundenen Verfahren sicherzustellen. Die neueste Version der CMMC wurde im Jahr 2020 veröffentlicht.

Attribute/Dimensionen

Die CMMC berücksichtigt **17 Bereiche**, die Cluster von Cybersicherheitsprozessen und -fähigkeiten darstellen. Jeder Bereich ist in mehrere **Prozesse** unterteilt, die für alle Bereiche ähnlich sind, und eine oder mehrere **Fähigkeiten**, die sich über fünf Reifegradstufen erstrecken. Die Fähigkeit(en) wird/werden dann in den einzelnen **Verfahren** für jeden relevanten Reifegrad weiter ausgeführt.

Die Beziehung zwischen diesen Begriffen ist wie folgt:

Abbildung 9: Zu CMMC-Indikatoren



DOMAIN e.g. Asset Management (AM)	**BEREICH** z. B. Anlagenmanagement (Asset Management, AM)
Processes e.g Establish a policy that includes Asset Management	**Prozesse** z. B. Erstellung von Leitlinien, die auch für das Anlagenmanagement gelten
Capabilities e.g Manage Asset Inventory	**Kapazitäten** z. B. Verwaltung des Anlageninventars
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Verfahren bei MIL3** z. B. Definition von Verfahren für den Umgang mit CUI-Daten
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Verfahren bei MIL4** z. B. Einsatz einer Fähigkeit zum Erkennen und Identifizieren von Systemen mit bestimmten Komponentenmerkmalen im Inventar

Die siebzehn Bereiche sind nachstehend näher ausgeführt:

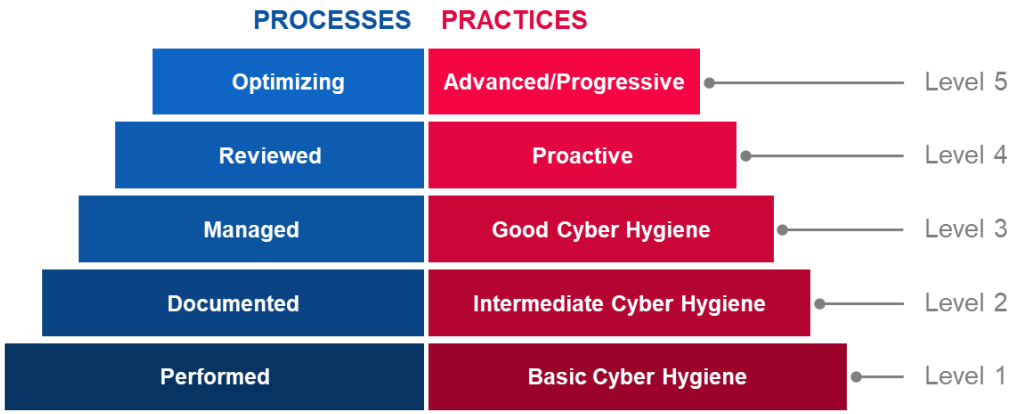
i Zugriffskontrolle (Access Control, AC)
ii Anlagenmanagement (Asset Management, AM)
iii Prüfung und Rechenschaftspflicht (Audit and Accountability, AU)
iv Sensibilisierung und Schulung/Ausbildung (Awareness and Training, AT)
v Konfigurationsmanagement (Configuration Management, CM)
vi Identifizierung und Authentifizierung (Identification and Authentication, IA)
vii Reaktion auf Sicherheitsvorfälle (Incident Response, IR)
viii Instandhaltung/Pflege (Maintenance, MA)
ix Medienschutz (Media Protection, MP)
x Sicherheit des Personals (Personnel Security, PS)
xi Physische Schutzmaßnahmen (Physical Protection, PE)
xii Wiederherstellung (Recovery, RE)
xiii Risikomanagement (Risk Management, RM)
xiv Sicherheitsbewertung (Security Assessment, CA)
xv Lagebewusstsein (Situational Awareness, SA)

xvi System- und Kommunikationssicherheit (System and Communications Protection, SC)
xvii System- und Informationsintegrität (System and Information Integrity, SI)

Reifegrade

Die CMMC verwendet **5 Reifegrade,** die basierend auf Prozessen und Verfahren definiert werden. Um einen bestimmten Reifegrad in der CMMC zu erreichen, muss eine Organisation die Voraussetzungen für die Prozesse und Verfahren für diesen jeweiligen Grad erfüllen. Dies schließt auch die Erfüllung der Voraussetzungen aller darunter liegenden Reifegrade ein.

Abbildung 10: CMMC-Reifegrade



PROCESSES	PROZESSE
Optimizing	Optimierung
Reviewed	Überprüfung
Managed	Steuerung
Documented	Dokumentierung
Performed	Durchführung
PRACTICES	VERFAHREN
Advanced/Progressive	Fortgeschritten/Fortschreitend
Proactive	Proaktiv
Good Cyber Hygiene	Gute Cyberhygiene
Intermediate Cyber Hygiene	Mittlere Cyberhygiene
Basic Cyber Hygiene	Grundlegende Cyberhygiene
Level 5	Grad 5
Level 4	Grad 4
Level 3	Grad 3
Level 2	Grad 2
Level 1	Grad 1

- **Grad 1**
  - **Prozesse – Durchführung**: Weil die Organisation diese Verfahren möglicherweise nur ad-hoc ausführen kann und sich möglicherweise auf Dokumentation stützt (oder auch nicht). Die Prozessreife wird für den Reifegrad 1 nicht bewertet.
  - **Verfahren – Grundlegende Cyberhygiene**: bei Reifegrad 1 steht der Schutz der FCI (Federal Contract Information – Vertragsinformationen des Bundes) im Mittelpunkt und es gibt nur Verfahren für grundlegende Sicherheitsanforderungen.
- **Grad 2**

- **Prozesse – Dokumentierung**: für Reifegrad 2 ist erforderlich, dass eine Organisation Verfahren und Leitlinien festlegt und dokumentiert, um die Umsetzung ihrer CMMC-Bemühungen zu steuern. Die Verfahrensdokumentation ermöglicht es Einzelpersonen, die Verfahren auf wiederholbare Weise durchzuführen. Organisationen entwickeln ausgereifte Fähigkeiten, indem sie ihre Prozesse dokumentieren und sie dann wie dokumentiert durchführen.
- **Verfahren – Mittlere Cyberhygiene**: Reifegrad 2 ist der nächste Schritt nach Grad 1 und umfasst eine Teilmenge der in NIST SP 800-171 festgelegten Sicherheitsanforderungen sowie aus anderen Normen und Referenzen entnommene Verfahren.

- **Grad 3**
  - **Prozesse – Steuerung**: bei Reifegrad 3 ist erforderlich, dass eine Organisation einen Plan erstellt, pflegt und mit Ressourcen ausstattet und so zeigt, dass sie die Aktivitäten für die Umsetzung der Verfahren steuert. Der Plan kann Informationen zu Aufgabenstellungen, Zielen, Projektplänen, Ressourcen, erforderlichen Schulungen und der Einbeziehung relevanter Interessenträger enthalten.
  - **Verfahren – Gute Cyberhygiene**: bei Reifegrad 3 steht der Schutz der CUI im Mittelpunkt und er umfasst alle in NIST SP 800-171 festgelegten Sicherheitsanforderungen sowie zusätzliche aus anderen Normen und Referenzen entnommene Verfahren zur Minderung von Bedrohungen.
- **Grad 4**
  - **Prozesse – Überprüfung**: Reifegrad 4 verlangt, dass eine Organisation Verfahren überprüft und auf ihre Wirksamkeit hin bewertet. Zusätzlich zur Wirksamkeitsbewertung der Verfahren können Organisationen in diesem Reifegrad bei Bedarf Korrekturmaßnahmen ergreifen und die Führungsebene regelmäßig über Status oder Schwierigkeiten informieren.
  - **Verfahren – Proaktiv**: bei Reifegrad 4 geht es insbesondere um den Schutz von CUI (Controlled Unclassified Information – eingeschränkt zugängliche Informationen) und er umfasst eine Teilmenge der erweiterten Sicherheitsanforderungen. Diese Verfahren verbessern die Erkennungs- und Reaktionsfähigkeiten einer Organisation, um sich mit den sich ändernden Taktiken, Techniken und Verfahren zu befassen und sich entsprechend anzupassen.
- **Grad 5**
  - **Prozesse – Optimierung**: In Reifegrad 5 muss eine Organisation die Umsetzung der Prozesse in der gesamten Organisation standardisieren und optimieren.
  - **Verfahren – Fortgeschritten/Proaktiv**: Bei Reifegrad 5 steht der Schutz der CUI im Mittelpunkt. Die zusätzlichen Verfahren erhöhen die Tiefe und Komplexität der Cybersicherheitsfähigkeiten.

Bewertungsmethode

Die CMMC ist ein relativ junges Modell, das im ersten Quartal 2020 fertiggestellt wurde. Bisher wurde es noch in keiner Organisation eingesetzt. Die Auftragnehmer des DOD planen jedoch, sich an zertifizierte Fremdprüfer zu wenden, um Prüfungen durchzuführen. Das DOD erwartet von seinen Auftragnehmern, dass sie bewährte Verfahren zur Stärkung der Cybersicherheit und des Schutzes sensibler Informationen einsetzen.

A.6 Das Community-Reifegradmodell für Cybersicherheit (CCSMM)

Das Community-Reifegradmodell für Cybersicherheit (CCSMM) wurde vom Centre for Infrastructure Assurance and Security der Universität von Texas entwickelt. Ziel des CCSMM ist es, die Methoden zur Bestimmung des aktuellen Status einer Gemeinschaft in Bezug auf ihre Abwehrbereitschaft im Cyberbereich besser zu definieren und einen Fahrplan für Gemeinschaften bereitzustellen, der sie bei ihren Vorbereitungsarbeiten unterstützt. Die Zielgruppe des CCSMM sind hauptsächlich Regierungsstellen auf lokaler und bundesstaatlicher Ebene. Das CCSMM wurde 2007 entwickelt.

Attribute/Dimensionen

Die Reifegrade werden anhand von **6 Hauptdimensionen** definiert, die die verschiedenen Aspekte der Cybersicherheit in Gemeinschaften und Organisationen abdecken. Diese Dimensionen werden für jeden Reifegrad klar definiert in (siehe dazu im Einzelnen Abbildung 11: Zusammenfassung der CCSMM). Die 6 Dimensionen sind:

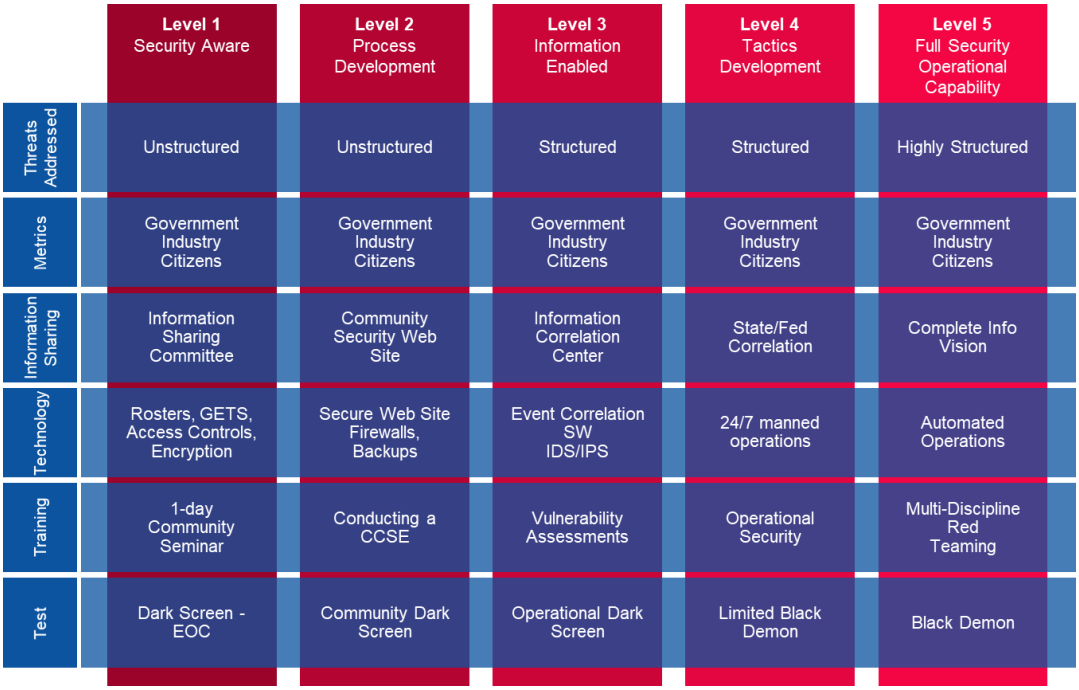
i Erfasste Bedrohungen
ii Parameter
iii Informationsaustausch
iv Technologie
v Schulung/Ausbildung
vi Test

Reifegrade

Das CCSMM umfasst **5 Reifegrade**, die auf den wichtigsten Arten der Bedrohungen und Aktivitäten dieser Reifegradstufe basieren:

- **Grad 1: Sicherheitsbewusstsein**
  Das Hauptthema der Aktivitäten in diesem Reifegrad ist die Sensibilisierung von Einzelpersonen und Organisationen für die Bedrohungen, Schwierigkeiten und Fragestellungen im Zusammenhang mit der Cybersicherheit.
- **Grad 2: Prozessentwicklung**
  Bei dieser Reifegradstufe geht es darum, Gemeinschaften dabei zu helfen, Sicherheitsprozesse einzuführen und zu verbessern, die erforderlich sind, um mit den Fragstellungen im Bereich der Cybersicherheit wirksam umzugehen.
- **Grad 3: Informationsfluss**
  In dieser Reifegradstufe sollen die Mechanismen für den Informationsaustausch innerhalb der Gemeinschaft verbessert werden, damit die Gemeinschaft wirksame Verbindungen zwischen augenscheinlich nicht zusammengehörenden Informationselementen herstellen kann.
- **Grad 4: Taktikentwicklung**
  Anhand der Elemente dieser Reifegradstufe sollen bessere und proaktivere Methoden entwickelt werden, um Angriffe erkennen und darauf reagieren zu können. In diesem Reifegrad sollten die meisten Präventionsmethoden vorhanden sein.
- **Grad 5: Volle Einsatzfähigkeit in Bezug auf die Cybersicherheit**
  Dieser Reifegrad stellt die Elemente dar, die vorhanden sein sollten, damit sich eine Organisation als voll einsatzfähig betrachtet, jeder Art von Cyberbedrohung zu begegnen.

Abbildung 11: Zusammenfassung der CCSMM Dimensionen für jeden Reifegrad



Level 1 Security Aware	Grad 1 Sicherheitsbewusstsein
Level 2 Process Development	Grad 2 Prozessentwicklung
Level 3 Information Enabled	Grad 3 Informationsfluss
Level 4 Tactics Development	Grad 4 Taktikentwicklung
Level 5 Full Security Operational Capability	Grad 5 Vollständige Funktionsfähigkeit in Bezug auf die Sicherheit
Threats Addressed	Bedrohungsbewältigung
Metrics	Parameter
Information sharing	Informationsaustausch
Technology	Technologie
Training	Schulung/Ausbildung
Test	Test
Unstructured	Unstrukturiert
Governement Industry Citizens	Staat Wirtschaft Bürger
Information Sharing Committee	Ausschuss für den Informationsaustausch
Rosters, GETS, Assess Controls, Encryption	Dienstpläne, GETS, Zugangskontrolle, Verschlüsselung
1-dat Community Seminar	Eintägiges Seminar
Dark Screen – EOC	Dark Screen – Notfallzentrum
Unstructured	Unstrukturiert
Governement Industry Citizens	Staat Wirtschaft Bürger
Community Security Web site	Sicherheitswebsite der Gemeinschaft
Secure Web Site Firewalls, Backups	Sichere Website-Firewalls, Backups
Conudcting a CCSE	Durchführung einer Cybersicherheitsübung
Community Dark Screen	Dark Screen – Gemeinschaft
Structured	Strukturiert
Governement Industry Citizens	Staat Wirtschaft Bürger
Information Correlation Center	Informationskorrelationszentrum
Event Correlation SW IDS/IPS	Ereigniskorrelation SW IDS/IPS
Vulnerability Assessment	Bewertung der Sicherheitslücken

Operational Dark Screen	Dark Screen auf operativer Ebene
Structured	Strukturiert
Governement Industry Citizens	Staat Wirtschaft Bürger
State/Fed Correlation	Bundesstaat/Bund-Korrelation
24/7 manned operations	Betrieb rund um die Uhr
Operational Security	Betriebssicherheit
Limited Black Demon	Black Demon – begrenzt
Highly Structured	Hochstrukturiert
Complete Info Vision	Vollständige Informationen Vision
Automated Operations	Automatisierte Vorgänge
Multi-Discipline Red Teaming	Multidisziplinäres Red Teaming
Black Demon	Black Demon

Bewertungsmethode

Das CCSMM als Bewertungsmethode soll – unter Einbeziehung von Beiträgen der Strafverfolgungsbehörden der Ebene der Bundesstaaten und des Bundes – von Gemeinschaften eingesetzt werden. Es soll der Gemeinschaft helfen festzulegen, was am wichtigsten ist, welche Ziele am wahrscheinlichsten sind und was geschützt werden muss (und in welchem Umfang). Unter Berücksichtigung dieser Ziele können Pläne entwickelt werden, um für jeden Aspekt die Gemeinschaft auf den erforderlichen Cybersicherheitsreifegrad zu bringen. Die vom CCSMM generierten spezifischen Informationen helfen dabei, die Ziele verschiedener Tests und Übungen festzulegen, mit denen die Wirksamkeit etablierter Programme gemessen werden kann.

A.7 Reifegradmodell für Informationssicherheit für das NIST-Cybersicherheitsregelwerk (ISMM)

Das Reifegradmodell für Informationssicherheit (ISMM) wurde an der Fakultät für Informatik und Ingenieurwesen der King-Fahd-Universität für Erdöl und Mineralien in Saudi-Arabien entwickelt. Es wird ein neues Reifegradmodell vorgeschlagen, um die Einführung von Cybersicherheitsvorkehrungen zu bewerten. Das Ziel des ISMM ist es, Organisationen zu ermöglichen, ihren Umsetzungsfortschritt im Zeitverlauf zu messen, indem sie in regelmäßigen Zeitabständen dasselbe Messinstrument verwenden, um sicherzustellen, dass die gewünschte Sicherheitspositionierung aufrechterhalten wird. Das ISMM wurde 2017 entwickelt.

Attribute/Dimensionen

Das ISMM baut auf den vorhandenen bewerteten Bereichen des NIST-Rahmens auf und fügt eine Dimension zur Bewertung der Einhaltung hinzu. So umfasst das Modell **23 Bereiche**, die im Hinblick auf die Sicherheitspositionierung einer Organisation bewertet werden. Die 23 bewerteten Bereiche sind:

i Anlagenmanagement
ii Geschäftsumfeld
iii Governance
iv Risikobewertung
v Risikomanagementstrategie
vi Bewertung der Einhaltung
vii Zugriffskontrolle
viii Sensibilisierung und Schulung/Ausbildung
ix Datensicherheit
x Informationsschutzprozesse und -verfahren
xi Instandhaltung/Pflege

xii Schutztechnologie
xiii Abweichungen und Ereignisse
xiv Kontinuierliche Sicherheitsüberwachung
xv Erkennungsprozesse
xvi Reaktionsplanung
xvii Reaktionskommunikation
xviii Reaktionsanalyse
xix Schadensbegrenzung
xx Reaktionsverbesserungen
xxi Wiederherstellungsplanung
xxii Wiederherstellungsverbesserungen
xxiii Wiederherstellungskommunikation

Reifegrade

Das ISMM umfasst **5 Reifegrade**, die in der verfügbaren Dokumentation leider nicht im Einzelnen detailliert aufgeführt sind.

- **Grad 1:** Prozess „Durchführung“
- **Grad 2:** Prozess „Steuerung“
- **Grad 3:** Prozess „Einrichtung“
- **Grad 4:** Prozess „Vorhersehbarkeit“
- **Grad 5:** Prozess „Optimierung“

Bewertungsmethode

Das ISMM schlägt keine spezifische Methode zur Durchführung der Bewertung für Organisationen vor.

A.8 Modell für interne Auditstellen (IA-CM) für den öffentlichen Sektor

Das Modell für interne Auditstellen (IA-CM) wurde von der Forschungsstiftung des Institute of Internal Auditors mit der Absicht entwickelt, durch Selbstbewertung im öffentlichen Sektor Kapazitäten und eine breite Befürwortung aufzubauen. Das IA-CM richtet sich an Fachleute für Innenrevision und bietet einen Überblick über das Modell selbst sowie einen Leitfaden, der bei der Verwendung des Modells als Selbstbewertungsinstrument unterstützt.

Obwohl sich das IA-CM eher auf die interne Auditkapazität als auf den Aufbau von Cybersicherheitskapazitäten konzentriert, wurde das Modell als Instrument zur Selbstbewertung der Reife für Unternehmen des öffentlichen Sektors entwickelt, das global angewendet werden kann, um Prozesse und Wirksamkeit zu verbessern. Da bei diesem Modell die Cybersicherheit nicht im Mittelpunkt steht, werden die Attribute hier nicht analysiert. Das IA-CM wurde 2009 fertiggestellt.

Reifegrade

Das Modell für interne Auditstellen (IA-CM) umfasst **5 Reifegrade**, von denen jeder die Merkmale und Fähigkeiten der Innenrevision auf dieser Ebene beschreibt. Die Reifegradstufen des Modells bieten einen Fahrplan für die kontinuierliche Verbesserung.

- **Grad 1: Erste Schritte**
  Keine nachhaltigen, wiederholbaren Fähigkeiten – abhängig von individuellen Anstrengungen
  - Ad hoc oder unstrukturiert.
  - Isolierte Einzelaudits oder Überprüfungen von Dokumenten und Transaktionen auf Richtigkeit und Konformität.

- Ergebnisse, die von den Kompetenzen der Person abhängen, die die Position innehat.
- Keine anderen professionellen Verfahren eingeführt als von Berufsverbänden vorgegeben.
- Genehmigung der Finanzierung durch das Management nach Bedarf.
- Fehlende Infrastruktur.
- Revisoren sind wahrscheinlich Teil einer größeren Organisationseinheit.
- Keine institutionellen Kapazitäten entwickelt.

Grad 2: Infrastruktur

Nachhaltige und wiederholbare Prozesse und Verfahren

- Die zentrale Frage oder Herausforderung im Reifegrad 2 ist, wie die Wiederholbarkeit von Prozessen und damit eine wiederholbare Fähigkeit hergestellt und aufrechterhalten werden kann.
- Es werden Beziehungen der Revisionsberichterstattung, Management- und Verwaltungsinfrastrukturen sowie professionelle Verfahren und Prozesse eingerichtet (Leitlinien, Prozesse und Verfahren für die Innenrevision).
- Die Innenrevisionsplanung richtet sich hauptsächlich nach den Prioritäten des Managements.
- Fortgesetztes Vertrauen vor allem in die Fähigkeiten und Kompetenzen bestimmter Personen.
- Teilweise Konformität mit den Normen.

Grad 3: Integration

Management- und professionelle Verfahren werden einheitlich angewendet

- Leitlinien, Prozesse und Verfahren der Innenrevision werden festgelegt, dokumentiert und miteinander verflochten und in die Infrastruktur der Organisation eingebunden.
- Das Revisionsmanagement und die professionellen Verfahren sind gut etabliert und werden überall bei der Innenrevision einheitlich angewendet.
- Die Innenrevision beginnt, sich an der Geschäftstätigkeit der Organisation und die damit verbundenen Risiken auszurichten.
- Die Innenrevision entwickelt sich von der ausschließlichen traditionellen Innenrevision hin zu einem eingebundenen Teamplayer und bietet Beratung in Bezug auf Leistung und Risikomanagement.
- Im Mittelpunkt steht die Teambildung und die Innenrevisionskapazität sowie ihre Unabhängigkeit und Objektivität.
- Im Allgemeinen herrscht Konformität mit den Normen.

Grad 4: Steuerung

Informationen aus der gesamten Organisation werden einbezogen, um die Governance und das Risikomanagement zu verbessern.

- Die Innenrevision erfüllt die Erwartungen der wichtigsten Interessenträger.
- Es sind Leistungsparameter vorhanden, um die Prozesse und Ergebnisse der Innenrevision zu messen und zu überwachen.
- Die Innenrevision liefert nachweislich wesentliche Beiträge zur Organisation.
- Die Innenrevision ist ein wesentlicher Bestandteil der Governance und des Risikomanagements der Organisation.
- Die interne Auditstelle ist eine gut geführte Geschäftseinheit.
- Risiken werden quantitativ gemessen und gesteuert.
- Erforderliche Fähigkeiten und Kompetenzen sind vorhanden, können erneuert werden und diesbezügliches Wissen kann ausgetauscht werden (innerhalb der internen Auditstelle und in der gesamten Organisation).

Grad 5: Optimierung

Lernen innerhalb der Organisation sowie durch Input von außen zur kontinuierlichen Verbesserung

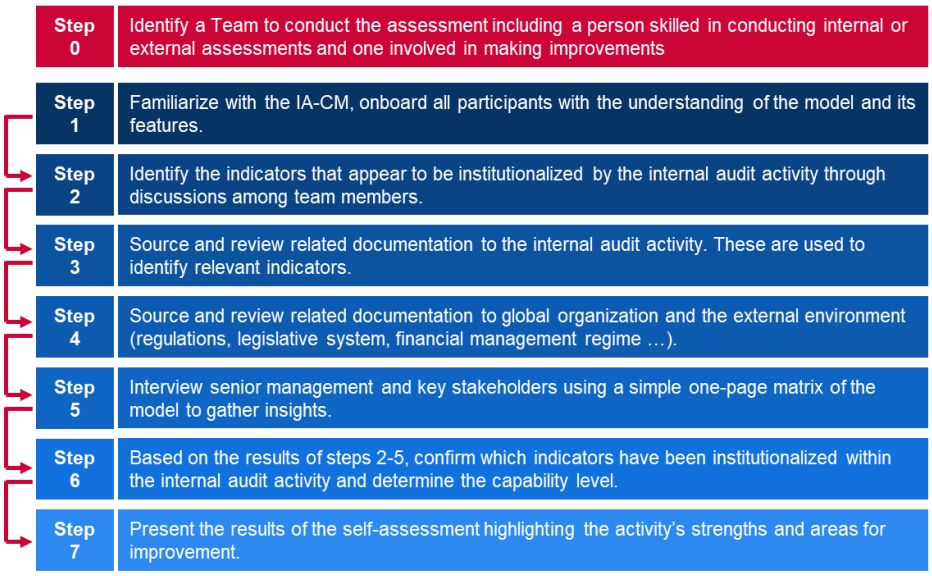
- Die interne Auditstelle ist eine lernende Einheit, verbessert kontinuierlich ihre Prozesse und ist innovationsfreudig.
- Die interne Auditstelle verwendet Informationen von innerhalb und außerhalb der Organisation, um zur Erreichung strategischer Ziele beizutragen.
- Leistung auf Weltklasse-Niveau/ entsprechend den Empfehlungen/ an bewährten Verfahren orientiert.

- Die interne Revision ist ein wichtiger Bestandteil der Governancestruktur der Organisation.
- Professionelle und spezialisierte Kompetenzen auf höchstem Niveau.
- Maßnahmen betreffend die Leistung von Einzelpersonen, Organisationseinheiten sowie der Organisation insgesamt sind vollständig integriert,
- um eine Leistungsverbesserung zu bewirken.

Bewertungsmethode

Das Modell für interne Auditstellen ist eindeutig auf Selbstbewertung ausgelegt. Es umfasst detaillierte Schritte für die Verwendung des IA-CM sowie ein jeweils anpassbares Inventarium von Mustervorlagen. Vor Beginn der Selbstbewertung ist ein Team festzulegen, dem mindestens eine Person angehört, die in der Durchführung interner oder externer Bewertungen von Innenrevisionsaktivitäten qualifiziert ist, sowie eine Person, die an Verbesserungen in diesem Bereich beteiligt ist.

Abbildung 12: Schritte zur Selbstbewertung im Rahmen des IC-AM



Step 0	Schritt 0
Step 1	Schritt 1
Step 2	Schritt 2
Step 3	Schritt 3
Step 4	Schritt 4
Step 5	Schritt 5
Step 6	Schritt 6
Step 7	Schritt 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Ernennung eines Teams, das die Bewertung durchführt, einschließlich einer Person, die in der Durchführung interner und externer Bewertungen qualifiziert ist, und einer Person, die an Verbesserungen beteiligt ist.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Familiarisierung mit dem IA-CM und dafür Sorge tragen, dass alle Teilnehmer das Modell und seine Funktionen verstehen.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Im Rahmen von Diskussionen der Teammitglieder Ermittlung der Indikatoren, die

	offensichtlich durch die Innenrevision institutionalisiert sind.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Beschaffung und Überprüfung der Dokumentation für die Innenrevision. Diese wird verwendet, um relevante Indikatoren zu ermitteln.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Beschaffung und Überprüfung der entsprechenden Dokumentation für die Organisation insgesamt sowie das externe Umfeld (Vorschriften, Gesetzgebungssystem, Finanzmanagementsystem usw.).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Befragung der Geschäftsführung und wichtiger Interessenträger anhand einer einfachen kurzen (1 Seite) Matrix des Modells, um Erkenntnisse zu gewinnen.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Bestätigung anhand der Ergebnisse der Schritte 2 bis 5, welche Indikatoren im Rahmen der Innenrevision institutionalisiert sind, sowie Bestimmung des Fähigkeitsniveaus.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Präsentation der Ergebnisse der Selbstbewertung unter Hervorhebung der Stärken der Aktivität sowie ihrer Verbesserungsmöglichkeiten.

A.9 Der Globale Cybersicherheitsindex (GCI)

Der Globale Cybersicherheitsindex (GCI) ist eine Initiative der Internationalen Fernmeldeunion (ITU) zur Überprüfung des Engagements und der Lage im Bereich Cybersicherheit in allen ITU-Regionen: Afrika, Amerika, arabische Staaten, Asien-Pazifik, GUS und Europa; wobei Länder mit hohem Engagement und empfehlenswerten Verfahren besondere Beachtung finden. Ziel des GCI ist es, den Ländern dabei zu helfen, Verbesserungsmöglichkeiten im Bereich der Cybersicherheit zu ermitteln, und sie zu motivieren, Maßnahmen zur Verbesserung ihres Platzes im Ranking zu ergreifen, um so das allgemeine Niveau der Cybersicherheit weltweit zu erhöhen.

Da der GCI ein Index und kein Reifegradmodell ist, verwendet er keine Reifegrade, sondern ein Punktesystem, um das globale Cybersicherheitsengagement von Nationen und Regionen zu bewerten und zu vergleichen.

Attribute/Dimensionen

Der Globale Cybersicherheitsindex (GCI) basiert auf den fünf Säulen der Globalen Cybersicherheitsagenda (GCA). Diese Säulen bilden die fünf Teilindizes des GCI und umfassen jeweils eine Reihe von Indikatoren. Die fünf Säulen und Indikatoren sind folgende:

i **Recht**: Maßnahmen, die sich auf das Vorhandensein von rechtlichen Institutionen und Rahmenbedingungen für Cybersicherheit und Cyberkriminalität stützen.
   - Rechtsvorschriften in Bezug auf Cyberkriminalität
   - Cybersicherheitsbestimmungen
   - Eindämmung der Spam-Gesetzgebung

ii **Technik**: Maßnahmen, die sich auf das Vorhandensein von technischen Institutionen und Rahmenbedingungen für Cybersicherheit stützen.
   - CERT/CIRT/CSRIT
   - Rahmen für die Implementierung von Standards
   - Normungsgremium
   - Technische Instrumente und Fähigkeiten zur Bekämpfung von Spam
   - Nutzung der Cloud für Cybersicherheitszwecke

- Instrumenten für den Schutz von Kindern im Internet

iii **Organisation**: Maßnahmen, die sich auf das Vorhandensein von Institutionen für die Politikkoordinierung und Strategien für die Entwicklung der Cybersicherheit auf nationaler Ebene beruhen.
- Nationale Cybersicherheitsstrategie
- Zuständige Behörde
- Cybersicherheit

iv **Kapazitätenaufbau:** Maßnahmen, die sich auf das Vorhandensein von Forschungs- und Entwicklungs-, Bildungs-, Ausbildungs- und Schulungsprogrammen, zertifizierten Fachleuten und Behörden des öffentlichen Sektors zur Förderung des Kapazitätenaufbaus stützen.
- Kampagnen zur Sensibilisierung der Öffentlichkeit
- Rahmen für die Zertifizierung und Akkreditierung von Cybersicherheitsfachleuten
- Professionelle Schulungs-/Ausbildungslehrgänge in Cybersicherheit
- Bildungsprogramme oder Hochschullehrpläne zu Cybersicherheit
- F&E-Programme in Bezug auf Cybersicherheit
- Anreizsysteme

v **Zusammenarbeit**: Maßnahmen, die sich auf das Vorhandensein von Partnerschaften, kooperativen Rahmenbedingungen und Netzwerken für den Informationsaustausch stützen.
- Bilaterale Vereinbarungen
- Mehrseitige Vereinbarungen
- Teilnahme an internationalen Foren/Verbänden
- Öffentlich-private Partnerschaften
- Partnerschaften zwischen oder innerhalb von Behörden
- Bewährte Verfahren

Bewertungsmethode

Der GCI ist ein Selbstbewertungsinstrument, bei dem die Bewertung anhand einer Umfrage[30] mit Entscheidungsfragen (Ja/Nein), Fragen mit Antwortvorgaben offenen Fragen durchgeführt wird. Die Verwendung von Entscheidungsfragen schließt eine meinungsbasierte Bewertung und jegliche mögliche Tendenz zu bestimmten Arten von Antworten aus. Die Fragen mit Antwortvorgaben sparen Zeit und ermöglichen eine genauere Datenanalyse. Darüber hinaus ermöglicht eine einfache dichotome Skala eine schnellere und komplexere Bewertung, da keine langen Antworten erforderlich sind, was den Prozess der Lieferung von Antworten und der weiteren Bewertung beschleunigt und rationalisiert. Die Befragten sollten nur das Vorhandensein oder Fehlen bestimmter vorab identifizierter Cybersicherheitslösungen bestätigen. Ein Online-Umfragemechanismus, mit dem Antworten gesammelt und relevantes Material hochgeladen werden, ermöglicht die Extraktion bewährter Verfahren und eine Reihe thematischer qualitativer Bewertungen durch eine Expertengruppe.

Der gesamte GCI-Prozess wird wie folgt durchgeführt:

- Allen Teilnehmern wird ein Einladungsschreiben zugesandt, in dem sie über die Initiative informiert werden und darum gebeten wird, eine Anlaufstelle anzugeben, die für die Erhebung aller relevanten Daten und das Ausfüllen des Online-GCI-Fragebogens zuständig ist. Während der Online-Umfrage wird die benannte Anlaufstelle von der ITU förmlich zur Beantwortung des Fragebogens aufgefordert.
- Primärdatenerfassung (für Länder, die den Fragebogen nicht beantworten):
  - Die ITU erarbeitet einen ersten Entwurf einer Antwort auf den Fragebogen unter Verwendung öffentlich verfügbarer Daten und Online-Recherchen.
  - Der Fragebogenentwurf wird zur Überprüfung an die Anlaufstellen übermittelt.

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf

- Die Anlaufstellen nehmen die Verbesserungen vor und senden dann den Fragebogenentwurf zurück.
- Der korrigierte Fragebogenentwurf wird jeder Anlaufstelle zur endgültigen Billigung übermittelt.
- Der validierte Fragebogen wird zur Analyse, Bewertung und Erstellung eines Rankings verwendet.

▶ Sekundärdatenerfassung (für Länder, die den Fragebogen beantworten):

- Die ITU ermittelt fehlende Antworten, unterstützende Dokumente, Links usw.
- Die Anlaufstelle verbessert bei Bedarf die Genauigkeit der Antworten.
- Der korrigierte Fragebogenentwurf wird jeder Anlaufstelle zur endgültigen Billigung übermittelt.
- Der gebilligte Fragebogen wird zur Analyse, Bewertung und Erstellung eines Rankings verwendet.

A.10 Der Cyber Power Index (CPI)

Der Cyber Power Index (CPI) wurde 2011 vom Forschungsprogramm der Economist Intelligence Unit erstellt und wird von Booz Allen Hamilton gesponsert. Der CPI ist ein: dynamisches quantitatives und qualitatives Modell, […] das spezifische Attribute der Cyberumgebung anhand von vier Triebkräften der Cyberwiderstandsfähigkeit misst: Rechtlicher und regulatorischer Rahmen; wirtschaftlicher und gesellschaftlicher Kontext; Technologie-Infrastruktur und Anwendung in der Wirtschaft, das den digitalen Fortschritt in Schlüsselsektoren der Wirtschaft untersucht.[31] Mithilfe des Cyber Power Index sollen die Fähigkeiten der G20-Länder, Cyberangriffen standzuhalten und die erforderliche digitale Infrastruktur für eine florierende und sichere Wirtschaft bereitzustellen, verglichen werden. Die vom CPI bereitgestellten Vergleichswerte beziehen sich auf 19 Länder der G20 (ohne EU). Der Index liefert dann eine Rangfolge (Ranking) der Länder für jeden Indikator.

Attribute/Dimensionen

Der Cyber Power Index (CPI) basiert auf vier Triebkräften der Cyberwiderstandsfähigkeit. Jede Kategorie wird anhand mehrerer Indikatoren gemessen, um jedem Land eine bestimmten Wert zuzuordnen. Die Kategorien und Säulen sind wie folgt:

i **Rechtlicher und regulatorischer Rahmen**
- Eigenverpflichtung des Staates für die Entwicklung von Cyberwiderstandsfähigkeiten
- Cybersicherheitskonzepte
- Cyberzensur (bzw. ein Fehlen derselben)
- Politische Wirksamkeit
- Schutz des geistigen Eigentums

ii **Wirtschaftlicher und gesellschaftlicher Kontext**
- Bildungsniveaus
- Technische Kompetenzen
- Offener Handel
- Innovationsgrad im Geschäftsumfeld

iii **Technologie-Infrastruktur**
- Zugang zu Informations- und Kommunikationstechnologie
- Qualität der Informations- und Kommunikationstechnologie
- Erschwinglichkeit von Informations- und Kommunikationstechnologie
- Ausgaben für Informationstechnologie
- Anzahl sicherer Server

iv **Anwendung in der Wirtschaft**
- Intelligente Netze
- Elektronische Gesundheitsdienste
- Elektronischer Handel

[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

- Intelligenter Transport
- Elektronische Behördendienste

Bewertungsmethode

Der CPI ist ein quantitatives und qualitatives Bewertungsmodell. Die Bewertung wurde von der Economist Intelligence Unit unter Verwendung quantitativer Indikatoren aus verfügbaren statistischen Quellen durchgeführt, wenn Daten fehlten, wurden Schätzwerte angenommen. Die wichtigsten Quellen sind die Economist Intelligence Unit, die Organisation der Vereinten Nationen für Erziehung, Wissenschaft und Kultur (UNESCO), die Internationale Fernmeldeunion (ITU) und die Weltbank.

A.11 Der Cyber Power Index (CPI)

Dieser Abschnitt fasst die wichtigsten Ergebnisse der Analyse der vorhandenen Reifegradmodelle zusammen. Tabelle 5: Übersicht über die analysierten Reifegradmodelle bietet einen Überblick über die Hauptmerkmale jedes Modells gemäß dem modifizierten Becker-Modell. Tabelle 6 Vergleich der Reifegrade zeigt die allgemeinen Definitionen der Reifegrade der analysierten Modelle. Tabelle 7 bietet einen Überblick über die in den einzelnen Modellen verwendeten Dimensionen bzw. Attribute.

Tabelle 5: Übersicht über die analysierten Reifegradmodelle

Bezeichnung des Modells	Ursprungsorganisation	Zweck	Ziel	Anzahl der Reifegrad-stufen	Anzahl der Attribute	Bewertungsmethode	Ergebnis-darstellung
Reifegradmodell für Cybersicherheits-kapazitäten für Nationen (CMM)	Zentrum für globale Cybersicherheitskapazitäten (GCSCC) Universität Oxford	Steigerung von Umfang und Wirksamkeit des Aufbaus von Cybersicherheits-kapazitäten im internationalen Maßstab	Länder	5	5 Haupt-dimensionen	Zusammenarbeit mit lokalen Organisationen zur Feinabstimmung des Modells, bevor es auf den nationalen Kontext angewendet wird	Darstellung in 5 Abschnitten
Reifegradmodell für Cybersicherheits-kapazitäten (C2M2)	US-Energieministerium (DOE)	Unterstützung von Organisationen bei der Bewertung und Verbesserung ihrer Cybersicherheitsprogramme und Stärkung der Widerstandsfähigkeit ihrer digitalen Systeme	Organisationen aller Sektoren, Arten und Größen	4	10 Haupt-bereiche	Selbstbewertungsmethode und -instrumentarium	Bewertungskarte mit Kreis-diagrammen
Rahmen zur Verbesserung der Cybersicherheit kritischer Infrastrukturen	Nationales Institut für Standards und Technologie (NIST)	Rahmen für die Steuerung von Cybersicherheitsaktivitäten und das Risikomanagement in Organisationen	Organisationen	Nicht zutreffend (4 Stufen)	5 Haupt-funktionen	Selbstbewertung	-
Reifegradmodell für Cybersicherheits-kapazitäten von Katar (Q-C2M2)	Rechtswissenschaftliche Fakultät der Universität Katar	Bereitstellung eines funktionsfähigen Modells, mit dem der Cybersicherheitsrahmen von Katar bewertet, gemessen und weiterentwickelt werden kann	Katarische Organisationen	5	5 Haupt-bereiche	-	-
Zertifizierung des Reifegradmodells für Cybersicherheit (CMMC)	US-Verteidigungsministerium (DOD)	Förderung von bewährten Verfahren für Cybersicherheit zum Schutz von Informationen	Organisationen der Rüstungs-industrie (DIB)	5	17 Haupt-bereiche	Bewertung durch externe Prüfer	-
Das Community-Reifegradmodell für Cybersicherheit (CCSMM)	Zentrum für Infrastruktursicherung und Sicherheit, Universität von Texas	Bestimmung des aktuellen Status einer Gemeinschaft in Bezug auf ihre Abwehrbereitschaft im Cyberbereich und Bereitstellung eines Fahrplans für Gemeinschaften zur Unterstützung bei ihren Vorbereitungsarbeiten	Gemeinschaften (Regierungs-stellen auf lokaler oder bundes-staatlicher Ebene)	5	6 Haupt-dimensionen	Bewertung innerhalb von Gemeinschaften mit Beiträgen von Strafverfolgungsbehörden der Bundesstaaten und des Bundes	-
Reifegradmodell für Informationssicherheit für das NIST-Cyber-sicherheitsregelwerk (ISMM)	Fakultät für Informatik und Ingenieurwesen King-Fahd-Universität für Erdöl und Mineralien, Dhahran, Saudi-Arabien	Befähigung von Organisationen, ihren Umsetzungsfortschritt im Zeitverlauf zu messen, um sicherzustellen, dass sie die gewünschte Sicherheitspositionierung aufrechterhalten	Organisationen	5	23 bewertete Bereiche	-	-
Modell für interne Auditstellen (IA-CM) für den öffentlichen Sektor	Die Forschungsstiftung des Institute of Internal auditors	Aufbau einer internen Auditkapazität und breite Befürwortung durch Selbstbewertung im öffentlichen Sektor	Organisationen des öffentlichen Sektors	5	6 Elemente	Selbstbewertung	-

Der Globale Cybersicherheitsindex (GCI)	Internationale Fernmeldeunion (ITU)	Überprüfung des Engagements und der Lage im Bereich Cybersicherheit und Unterstützung der Länder bei der Ermittlung von Verbesserungsmöglichkeiten im Bereich Cybersicherheit	Länder	Nicht zutreffend	5 Säulen	Selbstbewertung	Rangliste
Der Cyber Power Index (CPI)	The Economist Intelligence Unit und Booz Allen Hamilton	Vergleich der Fähigkeiten der G20-Länder, Cyberangriffen standzuhalten und die erforderliche digitale Infrastruktur für eine florierende und sichere Wirtschaft bereitzustellen	G20-Länder	Nicht zutreffend	4 Kategorien	Vergleich durch die Economist Intelligence Unit	Rangliste

Tabelle 6 Vergleich der Reifegrade

Modell	Grad 1	Grad 2	Grad 3	Grad 4	Grad 5
Reifegradmodell für Cybersicherheitskapazitäten für Nationen (CMM)	**Start-up** Es besteht entweder keine Reife auf Bezug auf Cybersicherheit oder sie ist noch sehr unausgereift. Es kann erste Diskussionen über den Aufbau von Cybersicherheitskapazitäten geben, aber es wurden noch keine konkreten Maßnahmen ergriffen. Zu diesem Zeitpunkt fehlen beobachtbare Nachweise.	**Festlegung** Es wurde damit begonnen, einige Merkmale der Aspekte zu entwickeln und festzulegen, sie können jedoch ad-hoc, unorganisiert, schlecht definiert oder einfach „neu“ sein. Der Nachweis dieser Aktivität kann jedoch eindeutig erbracht werden.	**Einführung** Die Elemente des Aspekts sind vorhanden und funktionieren. Die relative Verteilung der Ressourcen ist jedoch noch nicht gut durchdacht. In Bezug auf die „relative“ Investition in die verschiedenen Elemente des Aspekts wurden nur wenige Kompromissentscheidungen getroffen. Der Aspekt ist jedoch funktional und definiert.	**Strategiephase** Es wurde entschieden, welche Teile des Aspekts wichtig und welche für die jeweilige Organisation oder das jeweilige Land weniger wichtig sind. Die Strategiephase spiegelt die Tatsache wider, dass diese Entscheidungen je nach den besonderen Umständen des Landes oder der Organisation getroffen wurden.	**Dynamische Phase** Es bestehen klare Verfahren, um die Strategie je nach den vorherrschenden Umständen, wie z. B. der Technologie der Bedrohungsumgebung, globalen Konflikten oder einer signifikanten Änderung in einem Problembereich (z. B. Cyberkriminalität oder Datenschutz), zu ändern. Dynamische Organisationen haben Methoden entwickelt, um Strategien den sich ggf. ändernden Umständen entsprechend zu ändern. Diese Phase ist gekennzeichnet durch schnelle Entscheidungsfindung, Umverteilung von Ressourcen und ständige Aufmerksamkeit für das sich ändernde Umfeld.
Reifegradmodell für Cybersicherheitskapazitäten (C2M2)	**MIL0** Es werden keine Verfahren durchgeführt.	**MIL1** Erste Verfahren werden durchgeführt, können jedoch ad hoc erfolgen.	**MIL2** Managementmerkmale: Verfahren werden dokumentiert Zur Unterstützung des Prozesses werden angemessene Ressourcen bereitgestellt Das Personal, das die Verfahren durchführt, verfügt über angemessene Kompetenzen und Kenntnisse	**MIL3** Managementmerkmale: Die Aktivitäten richten sich nach Leitlinien (oder anderen Bestimmungen der Organisation). Leistungsziele für Bereichsaktivitäten werden festgelegt und überwacht, um die Leistung zu verfolgen. Dokumentierte Verfahren für Bereichsaktivitäten werden	-

			Verantwortung und Entscheidungskompetenz für die Durchführung der Verfahren werden zugewiesen. Konzeptmerkmale: Die Verfahren sind vollständiger bzw. weiter fortgeschritten als bei MIL1.	unternehmensweit standardisiert und verbessert. Konzeptmerkmale: Die Verfahren sind vollständiger oder weiter fortgeschritten als bei MIL2.	
Reifegradmodell für Informationssicherheit für das NIST-Cybersicherheitsrahmenwerk (ISMM)	**Prozess „Durchführung“**	**Prozess „Steuerung“**	**Prozess „Einrichtung“**	**Prozess „Vorhersehbarkeit“**	**Prozess „Optimierung“**
Reifegradmodell für Cybersicherheitskapazitäten von Katar (Q-C2M2)	**Erste Schritte** Verwendet Ad-hoc-Cybersicherheitsverfahren und -prozesse in einigen Bereichen.	**Entwicklung** Eingeführte Leitlinien und Verfahren zur Entwicklung und Verbesserung der Cybersicherheitsaktivitäten in den Bereichen mit dem Ziel, neue Aktivitäten zur Einführung vorzuschlagen.	**Einführung** Verabschiedete Leitlinien zur Einführung aller Cybersicherheitsaktivitäten in den Bereichen mit dem Ziel, die Einführung zu einem bestimmten Zeitpunkt abzuschließen.	**Anpassung** Überdenken und Überprüfen der Cybersicherheitsaktivitäten und Annahme von Verfahren auf der Grundlage prädiktiver Indikatoren, die aus früheren Erfahrungen und Maßnahmen abgeleitet wurden.	**Agilität** Weiterführung der Anpassungsphase mit einem zusätzlichen Schwerpunkt auf Agilität und Geschwindigkeit bei der Einführung von Aktivitäten in den Bereichen.
Zertifizierung des Reifegradmodells für Cybersicherheit (CMMC)	**Prozesse: Durchführung** Weil die Organisation diese Verfahren möglicherweise nur ad-hoc ausführen kann und sich möglicherweise auf Dokumentation stützt (oder auch nicht), kann die Reife in Grad 1 nicht bewertet werden. **Verfahren: Grundlegende Cyberhygiene** Bei Reifegrad 1 steht der Schutz der FCI (Federal Contract Information – Vertragsinformationen des Bundes) im Mittelpunkt und es gibt nur Verfahren für grundlegende Sicherheitsanforderungen.	**Prozesse: Dokumentierung** Für Reifegrad 2 ist erforderlich, dass eine Organisation Verfahren und Leitlinien festlegt und dokumentiert, um die Umsetzung ihrer CMMC-Bemühungen zu steuern. Die Verfahrensdokumentation ermöglicht es Einzelpersonen, die Verfahren auf wiederholbare Weise durchzuführen. Organisationen entwickeln ausgereifte Fähigkeiten, indem sie ihre Prozesse dokumentieren und sie dann wie dokumentiert durchführen. **Verfahren: Mittlere Cyberhygiene** Reifegrad 2 ist der nächste Schritt nach Grad 1 und umfasst eine Teilmenge der in NIST SP 800-171 festgelegten Sicherheitsanforderungen sowie aus anderen Normen und Referenzen entnommene Verfahren.	**Prozesse: Steuerung** Bei Reifegrad 3 ist erforderlich, dass eine Organisation einen Plan erstellt, pflegt und mit Ressourcen ausstattet und so zeigt, dass sie die Aktivitäten für die Umsetzung der Verfahren steuert. Der Plan kann Informationen zu Aufgabenstellungen, Zielen, Projektplänen, Ressourcen, erforderlichen Schulungen und der Einbeziehung relevanter Interessenträger enthalten. **Verfahren: Gute Cyberhygiene** Bei Reifegrad 3 steht der Schutz der CUI (Controlled Unclassified Information – eingeschränkt zugängliche Informationen) im Mittelpunkt und er umfasst alle in NIST SP 800-171 festgelegten Sicherheitsanforderungen sowie zusätzliche aus anderen Normen und Referenzen entnommene Verfahren zur Minderung von Bedrohungen.	**Prozesse: Überprüfung.** Reifegrad 4 verlangt, dass eine Organisation Verfahren überprüft und auf ihre Wirksamkeit hin bewertet. Zusätzlich zur Wirksamkeitsbewertung der Verfahren können Organisationen in diesem Reifegrad bei Bedarf Korrekturmaßnahmen ergreifen und die Führungsebene regelmäßig über Status oder Schwierigkeiten informieren. **Verfahren: Proaktiv** Bei Reifegrad 4 geht es insbesondere um den Schutz von CUI und er umfasst eine Teilmenge der erweiterten Sicherheitsanforderungen. Diese Verfahren verbessern die Erkennungs- und Reaktionsfähigkeiten einer Organisation, um sich mit den sich ändernden Taktiken, Techniken und Verfahren zu befassen und sich entsprechend anzupassen.	**Prozesse: Optimierung** In Reifegrad 5 muss eine Organisation die Umsetzung der Prozesse in der gesamten Organisation standardisieren und optimieren. **Verfahren: Fortgeschritten/Proaktiv** Bei Reifegrad 5 steht der Schutz der CUI im Mittelpunkt. Die zusätzlichen Verfahren erhöhen die Tiefe und Komplexität der Cybersicherheitsfähigkeiten.

Das Community-Reifegradmodell für Cybersicherheit (CCSMM)	**Sicherheitsbewusstsein** Das Hauptthema der Aktivitäten in diesem Reifegrad ist die Sensibilisierung von Einzelpersonen und Organisationen für die Bedrohungen, Schwierigkeiten und Fragestellungen im Zusammenhang mit der Cybersicherheit.	**Prozessentwicklung** Bei dieser Reifegradstufe geht es darum, Gemeinschaften dabei zu helfen, Sicherheitsprozesse einzuführen und zu verbessern, die erforderlich sind, um mit den Fragstellungen im Bereich der Cybersicherheit wirksam umzugehen.	**Informationsfluss** In dieser Reifegradstufe sollen die Mechanismen für den Informationsaustausch innerhalb der Gemeinschaft verbessert werden, damit die Gemeinschaft wirksame Verbindungen zwischen augenscheinlich nicht zusammengehörenden Informationselementen herstellen kann.	**Taktikentwicklung** Anhand der Elemente dieses Reifegrads sollen bessere und proaktivere Methoden entwickelt werden, um Angriffe zu erkennen und darauf zu reagieren zu können. In diesem Reifegrad sollten die meisten Präventionsmethoden vorhanden sein.	**Volle Einsatzfähigkeit in Bezug auf Cybersicherheit** Dieser Reifegrad stellt die Elemente dar, die vorhanden sein sollten, damit sich eine Organisation als voll einsatzfähig betrachtet, jeder Art von Cyberbedrohung zu begegnen.
Modell für interne Auditstellen (IA-CM) für den öffentlichen Sektor	**Erste Schritte** Keine nachhaltigen, wiederholbaren Fähigkeiten – abhängig von individuellen Anstrengungen	**Infrastruktur** Nachhaltige und wiederholbare Prozesse und Verfahren	**Integration** Management- und professionelle Verfahren werden einheitlich angewendet	**Steuerung** Es werden Informationen aus der gesamten Organisation berücksichtigt, um die Governance und das Risikomanagement zu verbessern	**Optimierung** Lernen innerhalb der Organisation sowie durch Input von außen zur kontinuierlichen Verbesserung

Tabelle 7: Vergleich von Attributen/Dimensionen

	Reifegradmodell für Cybersicherheitskapazitäten für Nationen (CMM)	Reifegradmodell für Cybersicherheitskapazitäten (C2M2)	Reifegradmodell für Cybersicherheitskapazitäten von Katar (Q-C2M2)	Zertifizierung des Reifegradmodells für Cybersicherheit (CMMC)	Zertifizierung des Reifegradmodells für Cybersicherheit (CMMC)	Reifegradmodell für Informationssicherheit für das NIST-Cybersicherheitsregelwerk (ISMM)	Rahmen zur Verbesserung der Cybersicherheit kritischer Infrastrukturen	Der Globale Cybersicherheits-index (GCI)	Der Cyber Power Index (CPI)
Reifegrade	Fünf Dimensionen, die wiederum in mehrere Faktoren unterteilt sind, einschließlich einer Reihe von Aspekten und Indikatoren (Abbildung 4)	Zehn Bereiche, darunter ein einziges Managementziel und mehrere Konzeptziele (Abbildung 6)	Fünf Bereiche, unterteilt in Unterbereiche	Siebzehn Bereiche, die in Prozesse unterteilt sind und eine oder mehrere Fähigkeiten umfassen, denen wiederum Verfahren zugeordnet sind (Abbildung 9).	Sechs Haupt-dimensionen	23 bewertete Bereiche	Fünf Funktionen mit zugrunde liegenden Schlüsselkategorien und Unterkategorien (Abbildung 8).	Fünf Säulen mit mehreren Indikatoren	Vier Kategorien mit mehreren Indikatoren
Attribute/ Dimen-sionen	i Entwicklung einer Cybersicherheits-politik und -strategie ii Förderung einer verantwortungs-bewussten Cybersicherheits-kultur in der Gesellschaft iii Entwicklung von Cybersicherheits-wissen iv Schaffung von wirksamen rechtlichen und regulatorischen Rahmen v Risikokontrolle durch Normen, Organisationen und Technologien	i Risiko-management ii Anlagen-, Änderungs- und Konfigurations-management iii Identitäts- und Zugangs-management iv Bedrohungs- und Sicherheitslücken-management v Lagebewusstsein vi Reaktion auf Ereignisse und Sicherheitsvorfälle vii Lieferketten- und externes Abhängigkeits-management viii Personal-management ix Cybersicherheits-architektur x Verwaltung von Cybersicherheits-programmen	i Verstehen (Governance, Anlagen, Risiken und Schulung/ Ausbildung im Bereich Cybersicherheit) ii Sichern (Datensicherheit, Technologie-sicherheit, Sicherheit der Zugriffskontrolle, Kommunikations-sicherheit und Sicherheit des Personals) iii Exponieren (Überwachung, Vorfall-management, Erkennung, Analyse und Exposition) iv Reagieren (Reaktions-planung, Schadens-begrenzung und Reaktions-kommunikation) v Erhalten (Wieder-herstellungs-planung, Kontinuitäts-management, Verbesserung und	i Zugriffskontrolle ii Anlagen-management iii Prüfung und Rechenschafts-pflicht iv Sensibilisierung und Schulung/ Ausbildung v Konfigurations-management vi Identifizierung und Authentifizierung vii Reaktion auf Sicherheitsvorfälle viii Instandhaltung/ Pflege ix Medienschutz x Sicherheit des Personals xi Physische Schutz-maßnahmen xii Wiederherstellung xiii Risiko-management xiv Sicherheits-bewertung xv Lagebewusstsein xvi System- und Kommunikations-sicherheit xvii System- und Informations-integrität	i Erfasste Bedrohungen ii Parameter iii Informations-austausch iv Technologie v Schulung/ Ausbildung vi Test	i Anlagen-management ii Geschäftsumfeld iii Governance iv Risikobewertung v Risiko-management-strategie vi Bewertung der Einhaltung vii Zugriffskontrolle viii Sensibilisierung und Schulung/ Ausbildung ix Datensicherheit x Informations-schutzprozesse und -verfahren xi Instandhaltung/ Pflege xii Schutztechnologie xiii Abweichungen und Ereignisse xiv Kontinuierliche Sicherheits-überwachung xv Erkennungs-prozesse xvi Reaktionsplanung xvii Reaktions-kommunikation xviii Reaktionsanalyse xix Schadens-begrenzung xx Reaktions-verbesserungen	i Ermitteln ii Schützen iii Erkennen iv Reagieren v Wiederherstellen	i Recht ii Technik iii Organisation iv Kapazitätenaufbau v Zusammenarbeit	i Rechtlicher und regulatorischer Rahmen ii Wirtschaftlicher und gesellschaftlicher Kontext iii Technologie-Infrastruktur iv Anwendung in der Wirtschaft

			externe Abhängig-keiten)			xxi Wieder-herstellungs-planung xxii Wieder-herstellungs-verbesserungen xxiii Wieder-herstellungs-kommunikation			

ANHANG B – BIBLIOGRAPHIE DER SCHREIBTISCHSTUDIEN

Almuhammadi, S. und Alsaleh, M. (2017) „Information Security Maturity Model for Nist Cyber Security Framework“, in: Computer Science & Information Technology (CS & IT). Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. und Alsaleh, M. (2017) „Information Security Maturity Model for Nist Cyber Security Framework“, in: Computer Science & Information Technology (CS & IT). Abrufbar unter: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016) Stocktaking, analysis and recommendations on the protection of CIIs. Abrufbar unter: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009) Entwicklung von Reifegradmodellen für das IT-Management – Vorgehensmodell und praktische Anwendung. Abrufbar unter: https://link.springer.com/article/10.1007/s11576-009-0167-9.

Belgische Regierung (2012) Cybersicherheitsstrategie. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. et al. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide. RAND Corporation. Abrufbar unter: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012) „Introduction to Return on Security Investment“.

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019) „Cybersecurity Capability Maturity Model (C2M2)“ Version 2.0. Abrufbar unter https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019) Nationale Cybersicherheitsstrategien im Vergleich – Herausforderungen für die Schweiz. Abrufbar unter: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/MELANI%20Studie_final_AW_18M%C3%A4rz2019.pdf

Ministerrat (2019) Portugiesisches Amtsblatt, Serie 1 – Nr. 108 – Entschließung des Ministerrats Nr. 92/2019 (auf Englisch). Abrufbar unter: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016) Cybersecurity Capacity Maturity Model for Nations (CMM). Universität Oxford.

CSIRT Maturity – Self-assessment Tool (ohne Datum). Abrufbar unter: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

CyberCrime@IPA, Projekt des Europarates und der Europäischen Union, Globales Projekt zur Bekämpfung der Cyberkriminalität des Europarates und der Task Force Cyberkriminalität der

Europäischen Union (2011) Spezialisierte Einheiten für Cyberkriminalität – Studie über bewährte Verfahren. Abrufbar unter: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (ohne Datum). Abrufbar unter: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017) Public Private Partnerships (PPP).

Darra, E. (ohne Datum) „Welcome to the NCSS Training Tool“.

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting. Abrufbar unter: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014) Technical Guideline on Security Measures. Abrufbar unter: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015) Guideline on Threats and Assets. Abrufbar unter: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia (2016) Cybersicherheitsstrategie. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. et al. (2014) *Privacy and data protection by design - from policy to engineering.* Abrufbar unter: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Europäische Kommission (2012) Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52012PC0238&from=DE

Europäische Agentur für Netz- und Informationssicherheit (2012) NCSS: Practical Guide on Development and Execution. Heraklion. ENISA.

Europäische Agentur für Netz- und Informationssicherheit (2012) NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion. ENISA.

Europäische Agentur für Netz- und Informationssicherheit (2016) Guidelines for SMEs on the security of personal data processing.

Europäische Agentur für Netz- und Informationssicherheit (2016) NCSS good practice guide: designing and implementing national cyber security strategies. Heraklion. ENISA.

Europäische Agentur für Netz- und Informationssicherheit (2017) Handbook on security of personal data processing. Abrufbar unter: http://dx.publications.europa.eu/10.2824/569768

Europäische Agentur für Netz- und Informationssicherheit (2014) *ENISA CERT inventory inventory of CERT teams and activities in Europe*. Abrufbar unter: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Executive Office Of The President (2015) Memorandum for Heads of Executive Departments and Agencies. Abrufbar unter: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Bundeskanzleramt der Republik Österreich (2013) Österreichische Strategie für Cyber Sicherheit. Abrufbar unter: https://bmi.gv.at/504/files/130416_strategie_cybersicherheit_WEB.pdf

Bundesministerium des Innern (2011) Cybersicherheitsstrategie für Deutschland. Abrufbar unter: https://www.bmi.bund.de/cybersicherheitsstrategie/

Ferette, L. (2016) NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Abrufbar unter: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., Europäische Union und Agentur der Europäischen Union für Netz- und Informationssicherheit (2015) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations (Bericht über nationale und internationale Cybersicherheitsübungen: Umfrage, Analyse und Empfehlungen). Abrufbar unter: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Büro des französischen Premierministers (2014) Französische nationale Strategie für die digitale Sicherheit. Abrufbar unter: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_de.pdf

Galan Manso, C. et al. (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Abrufbar unter: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Universität Gent et al. (2017) „Evaluating Business Process Maturity Models“, Journal of the Association for Information Systems. Abrufbar unter: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Regierung von Bulgarien (2015) Nationale Cybersicherheitsstrategie – Cyberresistentes Bulgarien 2020.

Regierung von Kroatien (2015) Die nationale Cybersicherheitsstrategie der Republik Kroatien. Abrufbar unter: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Regierung von Griechenland (2017) Nationale Cybersicherheitsstrategie. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Regierung von Ungarn (2018) Strategie für Netz- und Informationssicherheit. Abrufbar unter: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Regierung von Irland (2019) Nationale Cybersicherheitsstrategie. Abrufbar unter: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Regierung von Spanien (2019) Nationale Cybersicherheitsstrategie. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Institute of Internal Auditors (Hrsg.) (2009) Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

Internationale Fernmeldeunion (ITU) (2018) Der Global Cybersecurity Index. Abrufbar unter: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Internationale Fernmeldeunion (ITU) (2018) Guide to developing a national cybersecurity strategy. Abrufbar unter: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B. (2019) „Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework“, International Review of Law.

Regierung von Lettland (2014) Cybersicherheitsstrategie Lettlands. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. et al. (2014) An evaluation framework for national cyber security strategies. Heraklion. ENISA. Abrufbar unter: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. et al. (2014) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.* Abrufbar unter: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Ministerium für Wettbewerbsfähigkeit und digitale, maritime und Dienstleistungswirtschaft (2016) Cybersicherheitsstrategie von Malta. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Ministerium für Wirtschaft und Kommunikation (2019) Cybersicherheitsstrategie – Republik Estland. Abrufbar unter: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministerium für Nationale Verteidigung der Republik Litauen (2018) Nationale Cybersicherheitsstrategie

Nationales Cybersicherheitszentrum (2015) Nationale Cybersicherheitsstrategie der Tschechischen Republik. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Nationale Cybersicherheitsstrategien – Interaktive Karte (ohne Datum). Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Bewertungsinstrument für nationale Cybersicherheitsstrategien (2018). Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. Abrufbar unter: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group (2008) Business Process Maturity Model. Abrufbar unter: https://www.omg.org/spec/BPMM/1.0/PDF

OECD, Europäische Union und Gemeinsame Forschungsstelle – Europäische Kommission (2008) Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. Abrufbar unter: https://www.oecd.org/sdd/42495745.pdf.

Büro des Kommissars für elektronische Kommunikation und Postvorschriften (2012) Cybersicherheitsstrategie der Republik Zypern.

Amtsblatt der Europäischen Union (2008) RICHTLINIE 2008/114/EG DES RATES vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32008L0114&from=DE

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) (2012) Cybersecurity policy making at a turning point. Abrufbar unter: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012) „National Cyber Security Strategies – Practical Guide on Development and Execution“.

Ouzounis, E. (2012) Good Practice Guide on National Exercises.

Portesi, S. (2017) Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects

Präsidium des Ministerrates (2017) Der italienische Aktionsplan für Cybersicherheit. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Rady Ministrów (2019) Dziennik Urzędowy Rzeczypospolitej Polskiej. Abrufbar unter: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Regierung von Rumänien (2013) Cybersicherheitsstrategie von Rumänien. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. und Agentur der Europäischen Union für Cybersicherheit (2019) Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Abrufbar unter: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Sekretariat des Sicherheitsausschusses (2019) Finnlands Cybersicherheitsstrategie 2019. Abrufbar unter: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Slowakische Regierung (2015) Cybersicherheitskonzept der Slowakischen Republik. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R. (2016) „Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016“.

Smith, R. (2016) „Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016“, in: Smith, R., Core EU Legislation. London: Macmillan Education. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148&from=DE.

Stavropoulos, V. (2017) European Cyber Security Month 2017.

Schwedische Regierung (2017) Nationell strategi för samhällets informations- och cybersäkerhet. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Dänische Regierung – Finanzministerium (2018) Dänische Strategie für Cyber- und Informationssicherheit. Abrufbar unter: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Der Bundesrat (2018) Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken.

Regierungsrat von Luxemburg (2018) Nationale Cybersicherheitsstrategie. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Niederländische Regierung (2018) Nationale Cybersicherheitsagenda. Abrufbar unter: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

The White House (2018) National Cyber Strategy of the United States of America. Abrufbar unter: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P., et al. (2011) Cyber Europe Report. Abrufbar unter: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. und Agentur der Europäischen Union für Netz- und Informationssicherheit (2013) *National-level risk assessments: an analysis report.* Abrufbar unter: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., et al. (2015) Report on cyber-crisis cooperation and management. Abrufbar unter: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A., et al. (2015) Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises. Abrufbar unter: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

Nationale Cybersicherheitsstrategie des Vereinigten Königreichs 2016-2021 (2016). Abrufbar unter: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Universität Innsbruck et al. (2009) Understanding Maturity Models.

Wamala, D. F. (2011) „ITU National Cybersecurity Strategy Guide“. Abrufbar unter: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007) „The Community Cyber Security Maturity Model“, in: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07)

ANHANG C – WEITERE UNTERSUCHTE ZIELE

Die nachstehend aufgeführten Ziele wurden im Rahmen der Schreibtischstudienphase und der von der ENISA durchgeführten Befragungen untersucht. Die folgenden Ziele sind nicht Teil des Rahmens zur Bewertung nationaler Fähigkeiten, beleuchten jedoch Themen, die es wert sind, erörtert zu werden. In jedem der folgenden Unterkapitel wird erläutert, warum das Ziel verworfen wurde.

- Entwicklung branchenspezifischer Cybersicherheitsstrategien
- Kampf gegen Desinformationskampagnen
- Sichere Spitzentechnologien (5G, KI, Quanteninformatik usw.)
- Sicherstellung der Datensouveränität
- Schaffung von Anreizen für die Entwicklung der Cyber-Versicherungsbranche.

Entwicklung branchenspezifischer Cybersicherheitsstrategien

Die Annahme sektorspezifischer Strategien, die auf sektorale Interventionen und Anreize abzielen, führt zweifellos zu einer stärker dezentralen Kapazität. Sie ist besonders geeignet für Mitgliedstaaten, deren Betreiber wesentlicher Dienste (OES) sich mit unterschiedlichen Rahmenbedingungen und Vorschriften befassen müssen und in denen aufgrund des transversalen Charakters der Cybersicherheit viele Abhängigkeiten bestehen. In der Tat ist es in mehreren Mitgliedstaaten üblich, dass es Dutzende nationaler Behörden und Regulierungsstellen gibt, die über Kenntnisse der Besonderheiten aller Sektoren verfügen und beauftragt sind, spezifische Vorschriften für jeden Sektor durchzusetzen.

Dänemark hat beispielsweise sechs gezielte Strategien gestartet, die sich mit den Cyber- und Informationssicherheitsbemühungen der kritischsten Sektoren befassen, um eine stärkere dezentrale Kapazität im Bereich Cyber- und Informationssicherheit zu entwickeln. Jede „sektorale Einheit“ wird unter anderem zu Bedrohungsbewertungen auf sektoraler Ebene, Überwachung, Übungen zur Abwehrbereitschaft, Einrichtung von Sicherheitssystemen, Wissensaustausch und Anweisungen beitragen. Sektorspezifische Strategien gibt es für folgende Sektoren:

- Energie
- Gesundheitswesen
- Transport
- Telekommunikation
- Finanzwesen
- Seeverkehr

Andere Mitgliedstaaten haben Interesse bekundet, sektorspezifische Cybersicherheitsstrategien zu erwägen, um alle rechtlichen Anforderungen widerzuspiegeln. Es ist jedoch zu beachten, dass ein solches Ziel je nach Größe, nationaler Politik und Reife möglicherweise nicht für alle Mitgliedstaaten geeignet ist. Die große Schwierigkeit, die darin besteht, sicherzustellen, dass der Rahmen alle Besonderheiten berücksichtigen kann, führte dazu, dass die ENISA dieses Ziel nicht in den Rahmen aufgenommen hat.

Kampf gegen Desinformationskampagnen

Die Mitgliedstaaten nehmen den Schutz grundlegender Grundsätze wie Menschenrechte, Transparenz und öffentliches Vertrauen in ihre nationalen Cybersicherheitsstrategien auf. Dies ist besonders wichtig in Bezug auf Falschinformationen, die über traditionelle Nachrichtenmedien oder Social-Media-Plattformen verbreitet werden. Darüber hinaus stellt die Cybersicherheit derzeit eine der größten Herausforderungen bei Wahlen dar. In der Tat wurden im Vorfeld wichtiger Wahlen in verschiedenen Ländern Aktivitäten wie das Verbreiten von Falschinformationen oder Negativpropaganda beobachtet. Diese Bedrohung kann den demokratischen Prozess der EU untergraben. Auf europäischer Ebene hat die Kommission einen Aktionsplan[32] ausgearbeitet, um die Bemühungen zur Bekämpfung von Desinformation in Europa zu verstärken: Dieser Plan konzentriert sich auf vier Schlüsselbereiche (Erkennung, Zusammenarbeit, Zusammenwirken mit Online-Plattformen und Sensibilisierung) und dient dem Aufbau der Fähigkeiten der EU und der Stärkung der Zusammenarbeit zwischen den Mitgliedstaaten.

4 von 19 befragten Ländern haben ihre Absicht zum Ausdruck gebracht, das Problem der Desinformation und Propaganda in ihrer NCSS in Angriff zu nehmen.

So heißt es in der französischen NCSS[33]: „Es obliegt dem Staat, die Bürger über die Manipulationsrisiken und Propagandatechniken Krimineller im Internet zu informieren Nach den Attentaten in Frankreich im Januar 2015 hat die Regierung eine Informationsplattform zu den Risiken der islamistischen Radikalisierung über die elektronischen Kommunikationsnetzwerke eingerichtet. « Stop-djihadisme.gouv.fr ». Dieser Ansatz könnte auf andere Propaganda- oder Destabilisierungsphänomene ausgeweitet werden."

In einem anderen Beispiel, in Polens NCSS[34] 2019-2024, steht Folgendes: Gegen manipulative Aktivitäten wie Desinformationskampagnen sind systemische Maßnahmen erforderlich, um die Bürger dafür zu sensibilisieren, die Echtheit von Informationen zu überprüfen und auf Versuche, sie zu verfälschen, zu reagieren.

In von der ENISA durchgeführten Befragungen teilten mehrere Mitgliedstaaten jedoch mit, dass sie das Problem nicht im Rahmen ihrer NCSS als Cybersicherheitsbedrohung behandeln, sondern es auf einer breiteren gesellschaftlichen Ebene, beispielsweise über politische Initiativen, angehen.

[32] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018JC0036&from=de
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_de.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Sichere Spitzentechnologien (5G, KI, Quanteninformatik usw.)

Da die derzeitige Cyberbedrohungslandschaft sich weiter ausdehnt, wird die Entwicklung neuer Technologien höchstwahrscheinlich zu einer Zunahme der Intensität und der Anzahl von Cyberangriffen sowie zu einer Diversifizierung der Methoden, Mittel und Ziele der Bedrohungsakteure führen. In der Zwischenzeit können diese neuen technologischen Lösungen in Form von Spitzentechnologien zu Bausteinen des europäischen digitalen Marktes werden. Um die wachsende digitale Abhängigkeit der Mitgliedstaaten zu schützen und das Aufkommen neuer Technologien zu gewährleisten, sollten Anreize und umfassende Strategien geschaffen werden, um die sichere und vertrauenswürdige Entwicklung und den Einsatz dieser Technologien in der EU zu unterstützen.

Während der Schreibtischstudien über die NCSS der Mitgliedstaaten wurden die folgenden Spitzentechnologien als für die Mitgliedstaaten von Interesse vorgeschlagen: 5G, KI, Quanteninformatik, Kryptotechnik, Edge-Computing, verbundene und autonome Fahrzeuge, Big Data und Smart Data, Blockchain, Robotik und IoT.

Insbesondere veröffentlichte die Europäische Kommission Anfang 2020 eine Mitteilung, in der die Mitgliedstaaten aufgefordert wurden, Schritte zur Umsetzung der in den Schlussfolgerungen des 5G-Instrumentariums empfohlenen Maßnahmen zu unternehmen.[35] Dieses 5G-Instrumentarium wurde im Anschluss an die Empfehlung (EU) 2019/534 Cybersicherheit der 5G-Netze von der Kommission im Jahr 2019 verabschiedet, in der ein einheitliches europäisches Konzept für die Cybersicherheit von 5G-Netzen gefordert wurde.[36]

In von der ENISA durchgeführten Befragungen wurde hervorgehoben, dass dieses Thema eher ein Querschnittsthema sei, das in der gesamten NCSS behandelt werde, als ein spezifisches Ziel.

Sicherstellung der Datensouveränität

Einerseits kann der Cyberspace als ein beeindruckender globaler gemeinsamer Raum angesehen werden, der leicht zugänglich ist, ein hohes Maß an Konnektivität bietet und große Chancen für sozioökonomisches Wachstum bieten kann. Andererseits kennzeichnen den Cyberspace auch seine schwache Gerichtsbarkeit, die Schwierigkeit, Aktionen zuzuordnen, fehlende Grenzen und miteinander verbundene Systeme, die durchlässig sein können und deren Daten von anderen Staaten gestohlen werden oder sogar abgerufen werden können. Zusätzlich zu diesen beiden Perspektiven ist das digitale Ökosystem durch die Konzentration von Online-Serviceplattformen und -Infrastruktur in den Händen sehr weniger Interessenträger gekennzeichnet. Alle vorstehend genannten Aspekte veranlassen die Mitgliedstaaten, die digitale Souveränität zu fördern. Die Erlangung digitaler Souveränität bedeutet, dass Bürger und Unternehmen in der Lage sind, sich voll und ganz zu entfalten, indem sie vertrauenswürdige digitale Dienste und IKT-Produkte nutzen, ohne Angst um ihre persönlichen Daten oder digitalen Vermögenswerte, ihre wirtschaftliche Autonomie oder ihren politischen Einfluss haben zu müssen.

Die Datensouveränität oder digitale Souveränität wird von den Mitgliedstaaten auf nationaler und europäischer Ebene befürwortet. Während die Mitgliedstaaten das Problem nicht direkt in

[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission

[36] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019H0534

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

ihrer NCSS als spezifisches Ziel zu behandeln scheinen, gehen sie darauf entweder als Querschnittsprinzip ein oder sie stellen ihre Absicht, die digitale Souveränität auf nationaler Ebene zu gewährleisten, in Ad-hoc-Veröffentlichungen dar und stellen dabei Schlüsseltechnologien in den Vordergrund. In der französischen strategischen Überprüfung der Cyberabwehr im Jahr 2018 heißt es beispielsweise: Die Kontrolle der folgenden Technologien ist von größter Bedeutung, um die digitale Souveränität sicherzustellen: Kommunikationsverschlüsselung, Erkennung von Cyberangriffen, Betriebsfunk, Cloud-Computing und künstliche Intelligenz.[37]

Auf europäischer Ebene beteiligen sich die Mitgliedstaaten aktiv an der Festlegung der europäischen Datenstrategie (COM/2020/66 final) und am Aufbau des EU-Zertifizierungsrahmens für digitale IKT-Produkte, -Dienste und -Prozesse, der durch den EU-Rechtsakt zur Cybersicherheit (2019/881) festgelegt wurde, um eine strategische digitale Autonomie auf europäischer Ebene zu gewährleisten.

Die Phase der Befragung der Mitgliedstaaten hat gezeigt, dass das Thema der digitalen Souveränität häufig als umfassenderes Thema betrachtet wird und nicht als eines, das auf die Cybersicherheit beschränkt ist. Daher behandeln die Mitgliedstaaten das Thema nicht im Rahmen ihrer NCSS, und die wenigen, die dies tun, betrachten sie nicht als spezifisches Ziel.

Schaffung von Anreizen für die Entwicklung der Cyber-Versicherungsbranche

Der aktuelle Zustand der Cyber-Versicherungsbranche zeigt, dass der Weltmarkt unbestritten gewachsen ist. Die Branche befindet sich jedoch noch in ihren Anfängen, da Daten gesammelt und viele Präzedenzfälle geschaffen werden müssen (z. B. in Bezug auf nicht explizit vom Versicherungsschutz ein- oder ausgeschlossene Versicherungsrisiken, systemische Cyberrisiken usw.). Darüber hinaus liegen die geschätzten Verluste, die durch Cyberangriffe weltweit aggregiert werden, mehrere Größenordnungen über der derzeitigen Abdeckungskapazität der Cyber-Versicherungsbranche (IWF-Arbeitspapier WP/18/143: Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment). Die Entwicklung der Cyber-Versicherungsbranche kann jedoch sicherlich Vorteile bringen und den Grundstein für vorteilhafte Mechanismen legen. So können Cyber-Versicherungsmechanismen bei Folgendem helfen:

- Sensibilisierung für Cybersicherheitsrisiken in Unternehmen
- Quantitative Bewertung der Exposition gegenüber Cyberrisiken
- Verbesserung des Risikomanagements für Cybersicherheit
- Unterstützung von Organisationen, die Cyberangriffen zum Opfer fallen
- Deckung des durch einen Cyberangriff verursachten Schadens (Sach- und andere Schäden)

Einige Mitgliedstaaten haben begonnen, sich mit diesem Thema zu befassen. Beispiele:

- Estland verfolgte in seiner NCSS einen „abwartenden" Ansatz: Um die Cyberrisiken im privaten Sektor im Allgemeinen zu mindern, werden Angebot und Nachfrage nach Cyber-Versicherungsdienstleistungen in Estland analysiert und es werden auf dieser Grundlage kooperative Grundsätze für verbundene Parteien vereinbart, einschließlich Informationsaustausch, Vorbereitung der Risikobewertung usw. Heutzutage gibt es auf dem estnischen Markt nur wenige Anbieter von Cyber-Versicherungsdienstleistungen,

[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

und es muss zunächst ermittelt werden, wer was anbietet. Die Komplexität des Versicherungsschutzes wird häufig als Hindernis für die Entwicklung des Cyber-Versicherungsmarktes angesehen.

- Luxemburg unterstützt in seiner NCSS ausdrücklich die Entwicklung der Cyber-Versicherungsbranche: Ziel 1: Schaffung neuer Produkte und Dienstleistungen. Um Risiken zu bündeln und Opfer digitaler Cybervorfälle zu ermutigen, sich an Fachleute zu wenden, um den Vorfall zu bewältigen und ein von einer böswilligen Handlung betroffenes System wiederherzustellen, werden Versicherungsunternehmen aufgefordert, spezifische Produkte für den Bereich der Cyber-Versicherung zu entwickeln.

Die Rückmeldungen der Befragten zu diesem Thema waren sehr unterschiedlich: Einige Mitgliedstaaten gaben an, dass das Thema Cyber-Versicherung in letzter Zeit Gegenstand von Diskussionen geworden sei, während andere mitteilten, dass das Thema zwar vielversprechend, die Branche jedoch noch nicht ausgereift genug sei. Eine große Anzahl von Befragten erklärte jedoch, dass das Thema nicht als Teil der NCSS behandelt werde, entweder weil es als zu spezifisch angesehen werde oder nicht unter die NCSS falle.

TP-02-21-253-DE-N

Über die Agentur der Europäischen Union für Cybersicherheit

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Die Agentur wurde im Jahr 2004 errichtet und durch den Rechtsakt zur Cybersicherheit in ihrem Mandat weiter gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von IKT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, kooperiert mit den Mitgliedstaaten und Organen und Einrichtungen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Kapazitätenaufbau und Sensibilisierung im Bereich der Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürgerinnen und Bürger Europas zu gewährleisten. Nähere Informationen sind zu finden unter www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-477-0
DOI: 10.2824/678327