EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RAMY OCENY ZDOLNOŚCI KRAJOWYCH

GRUDZIEŃ 2020 R.

INFORMACJE O ENISA

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. ENISA – utworzona w 2004 r. i wzmocniona unijnym aktem o cyberbezpieczeństwie – wnosi wkład w politykę cybernetyczną UE, zwiększa wiarygodność produktów, usług i procesów informacyjno-komunikacyjnych dzięki systemom certyfikacji cyberbezpieczeństwa, współpracuje z państwami członkowskimi i organami UE oraz pomaga przygotować Europę na przyszłe wyzwania cybernetyczne. Poprzez wymianę informacji, budowanie zdolności i zwiększanie świadomości, Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do gospodarki opartej na łączności i odporność unijnej infrastruktury oraz, w efekcie, zapewnić cyfrowe bezpieczeństwo społeczeństwa i mieszkańców Europy. Aby uzyskać więcej informacji, zob.: www.enisa.europa.eu.

DANE KONTAKTOWE

W celu skontaktowania się z autorami prosimy o skorzystanie z adresu team@enisa.europa.eu. Zapytania prasowe dotyczące tego dokumentu można kierować na adres press@enisa.europa.eu.

AUTORZY

Anna Sarri, Pinelopi Kyranoudi – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique – Wavestone

PODZIĘKOWANIA

ENISA pragnie podziękować i przekazać wyrazy uznania wszystkim ekspertom, którzy wzięli udział w opracowaniu niniejszego raportu i wnieśli do niego cenny wkład. Są to w szczególności, w porządku alfabetycznym:

Centralny Krajowy Urząd Rozwoju Społeczeństwa Cyfrowego (Chorwacja), Marin Ante Pivcevic

Centrum Cyberbezpieczeństwa (Belgia)

CFCS – Center for Cybersikkerhed (Dania), Thomas Wulff

Dział Polityki Cyberbezpieczeństwa, Departament Środowiska, Klimatu i Komunikacji (Irlandia), James Caffrey

Europejskie Centrum ds. Walki z Cyberprzestępczością – EC3, Adrian-Ionut Bobeica

Europejskie Centrum ds. Walki z Cyberprzestępczością – EC3, Alzofra Martinez Alvaro

Federalne Ministerstwo Spraw Wewnętrznych (Niemcy), Sascha-Alexander Lettgen

Krajowa Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Informacji (Czechy), Veronika Netolická

Krajowy Departament Bezpieczeństwa (Hiszpania), Maria Mar Lopez Gil

Krajowy Urząd Bezpieczeństwa (Słowacja)

Maltańska Agencja Technologii Informacyjnych (Malta), Katia Bonello i Martin Camilleri

Ministerstwo Polityki Cyfrowej (Grecja), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali i Sotiris Vasilos

Ministerstwo Spraw Gospodarczych i Komunikacji (Estonia), Anna-Liisa Pärnalaas

Ministerstwo Sprawiedliwości i Bezpieczeństwa Publicznego (Norwegia), Robin Bakke

NCTV, Ministerstwo Sprawiedliwości i Bezpieczeństwa (Niderlandy)

Portugalskie Krajowe Centrum Cyberbezpieczeństwa (Portugalia), Alexandre Leite i Pedro Matos

Rząd włoski (Włochy)

Uniwersytet Oksfordzki – Global Cyber Security Capacity Centre, Carolin Weisser Harris

Urząd ds. Bezpieczeństwa Informacji (Republika Słowenii), Marjan Kavčič

ENISA pragnie również podziękować za cenny wkład w niniejszą analizę wszystkim ekspertom, którzy przyczynili się do jej powstania, ale wolą zachować anonimowość.

ZASTRZEŻENIA PRAWNE

Należy zwrócić uwagę, że niniejsza publikacja przedstawia poglądy i interpretacje ENISA, o ile nie stwierdzono inaczej. Niniejsza publikacja nie powinna być interpretowana jako działanie prawne ENISA lub organów ENISA, chyba że została przyjęta zgodnie z rozporządzeniem (UE) nr 2019/881.
Niniejsza publikacja nie musi przedstawiać aktualnego stanu wiedzy i ENISA może ją okresowo aktualizować.

Źródła zewnętrzne zostały odpowiednio zacytowane. ENISA nie ponosi odpowiedzialności za treść źródeł zewnętrznych, w tym zewnętrznych stron internetowych, do których odniesienia znajdują się w niniejszej publikacji.

Niniejsza publikacja jest przeznaczona wyłącznie do celów informacyjnych. Musi ona być dostępna nieodpłatnie. Ani ENISA, ani żadna osoba działająca w jej imieniu nie ponoszą odpowiedzialności za wykorzystanie informacji zawartych w niniejszym sprawozdaniu.

INFORMACJA O PRAWACH AUTORSKICH

ISBN: 978-92-9204-488-6

DOI: 10.2824/601560

Numer katalogowy: TP-02-21-253-PL-N

1. SPIS TREŚCI

SŁOWNICZEK POJĘĆ

SKRÓT	DEFINICJA
AI	Sztuczna inteligencja (Artificial Intelligence)
B+R	Badania i rozwój
C2M2	Model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Cybersecurity Capability Maturity Model)
CCRA	Porozumienie w sprawie wspólnych kryteriów uznawania (Common Criteria Recognition Arrangement)
CCSMM	Społecznościowy model dojrzałości cyberbezpieczeństwa (The Community Cybersecurity Maturity Model)
CMM	Model zdolności w zakresie cyberbezpieczeństwa dla państw (Cybersecurity Capacity Maturity Model for Nations)
CMMC	Certyfikacja modelu dojrzałości cyberbezpieczeństwa (Cybersecurity Maturity Model Certification)
CPI	Indeks potęgi cybernetycznej (Cyber Power Index)
CSIRT	Zespoły reagowania na incydenty bezpieczeństwa komputerowego
CVD	Skoordynowane ujawnianie luk w zabezpieczeniach
DPA	Ustawa o ochronie danych
ECCG	Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa
ECSM	Europejski Miesiąc Cyberbezpieczeństwa
ECSO	Europejska Organizacja ds. Cyberbezpieczeństwa
EFTA	Europejskie Stowarzyszenie Wolnego Handlu
ERK	Europejskie ramy kwalifikacji
GCI	Globalny indeks cyberbezpieczeństwa (Global Cybersecurity Index)
GSD	Government Digital Service
IA-CM	Model audytu wewnętrznego dla sektora publicznego (Internal Audit Capability Model for the Public Sector)
ISMM	Model dojrzałości bezpieczeństwa informacji na potrzeby ram cyberbezpieczeństwa NIST (Information Security Maturity Model for NIST Cybersecurity Framework)
ITU	Międzynarodowy Związek Telekomunikacyjny
JRC	Jednolity rynek cyfrowy
KITI	Krytyczna infrastruktura teleinformatyczna
LEA	Organ ścigania

MŚP	Małe i średnie przedsiębiorstwa
NCSS	Krajowe strategie cyberbezpieczeństwa
NIS	Bezpieczeństwo sieci i informacji
NIST	Narodowy Instytut Standaryzacji i Technologii
NLO	Krajowi urzędnicy łącznikowi
OT	Technologia operacyjna
OUK	Operatorzy usług kluczowych
PC	Państwo członkowskie
PET	Technologie ochrony prywatności
PIMS	System zarządzania ochroną danych osobowych
PPP	Partnerstwa publiczno-prywatne
Q-C2M2	Katarski model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Qatar Cybersecurity Capability Maturity Model)
RODO	Ogólne rozporządzenie o ochronie danych
SOG-IS MRA	Umowa o wzajemnym uznawaniu przyjęta przez grupę wyższych urzędników ds. bezpieczeństwa systemów informatycznych (Senior Officers Group for Information Systems' Security, Mutual Recognition Agreement)
TIK	Technologie informacyjne i komunikacyjne
UE	Unia Europejska

STRESZCZENIE

W obliczu ciągłego poszerzania się krajobrazu cyberzagrożeń oraz nieustannie rosnącej intensywności i liczby ataków cybernetycznych, państwa członkowskie UE muszą skutecznie reagować, kontynuując opracowywanie swoich krajowych strategii cyberbezpieczeństwa (NCSS) oraz odpowiednio je dostosowując. Od 2012 r., kiedy to ENISA opublikowała pierwsze badania dotyczące krajowych strategii cyberbezpieczeństwa, państwa członkowskie UE i państwa EFTA poczyniły ogromne postępy w pracy nad swoimi strategiami i ich realizacji.

W niniejszym raporcie przedstawiono prace wykonane przez ENISA w celu stworzenia ram oceny zdolności krajowych (NCAF).

Zostały one opracowane w celu umożliwienia państwom członkowskim przeprowadzenia samooceny osiągniętego poziomu dojrzałości w drodze oceny celów krajowej strategii cyberbezpieczeństwa, co pomoże im wzmacniać i budować zdolności w zakresie cyberbezpieczeństwa na poziomie strategicznym i operacyjnym.

Przedstawiają one prosty, reprezentatywny obraz poziomu dojrzałości państwa członkowskiego w zakresie cyberbezpieczeństwa. Narzędzie NCAF pomaga państwom członkowskim:

- Uzyskać przydatne informacje do opracowania długoterminowej strategii (np. dobre praktyki, wytyczne);
- Określić, czego brakuje w krajowej strategii cyberbezpieczeństwa;
- Kontynuować budowanie zdolności w zakresie cyberbezpieczeństwa;
- Zapewniać rozliczalność działań o charakterze politycznym;
- Zyskiwać wiarygodność w oczach ogółu społeczeństwa i partnerów międzynarodowych;
- Wspierać działania informacyjne i poprawiać swój wizerunek publiczny jako przejrzyście działającej organizacji;
- Przewidywać nadchodzące problemy;
- Wyciągać wnioski i wskazywać najlepsze praktyki;
- Ustalić poziom bazowy dla zdolności w zakresie cyberbezpieczeństwa w całej UE dla ułatwienia rozmów; oraz
- Oceniać krajowe zdolności w zakresie cyberbezpieczeństwa.

Niniejsze ramy zostały opracowane z pomocą ekspertów merytorycznych z ENISA oraz przedstawicieli 19 państw członkowskich i państw EFTA[1]. Raport jest skierowany do decydentów, ekspertów i urzędników państwowych odpowiedzialnych za projektowanie,

[1] Przeprowadzono rozmowy z przedstawicielami następujących państw członkowskich i państw EFTA: Belgia, Chorwacja, Republika Czeska, Dania, Estonia, Niemcy, Grecja, Węgry, Irlandia, Włochy, Liechtenstein, Malta, Niderlandy, Norwegia, Portugalia, Słowacja, Słowenia, Hiszpania, Szwecja.

wdrażanie i ocenę krajowych strategii cyberbezpieczeństwa oraz – w szerszym ujęciu – zdolności w zakresie cyberbezpieczeństwa, a także uczestniczących w tych procesach.

Ramy oceny zdolności krajowych obejmują 17 celów strategicznych i można je podzielić na następujące cztery główne grupy:

- Grupa nr 1: Zarządzanie cyberbezpieczeństwem i normy w zakresie cyberbezpieczeństwa
    1. Opracowanie krajowego planu awaryjnego na wypadek cyberataku
    2. Określenie podstawowych środków bezpieczeństwa
    3. Ochrona tożsamości elektronicznej i budowanie zaufania do cyfrowych usług publicznych

- Grupa nr 2: Budowanie zdolności i zwiększanie świadomości
    4. Organizacja ćwiczeń w zakresie cyberbezpieczeństwa
    5. Zapewnienie możliwości reagowania na incydenty
    6. Zwiększanie świadomości użytkowników
    7. Udoskonalanie programów szkoleniowych i edukacyjnych
    8. Wspieranie badań i rozwoju
    9. Zachęcanie sektora prywatnego do inwestowania w środki bezpieczeństwa
    10. Poprawa cyberbezpieczeństwa w łańcuchu dostaw

- Grupa nr 3: Aspekty prawne i regulacyjne
    11. Ochrona krytycznej infrastruktury teleinformatycznej, OUK i DUC
    12. Walka z cyberprzestępczością
    13. Wprowadzenie mechanizmów zgłaszania incydentów
    14. Wzmocnienie prywatności i ochrony danych

- Grupa nr 4: Współpraca
    15. Ustanowienie partnerstwa publiczno-prywatnego
    16. Instytucjonalizacja współpracy między agencjami publicznymi
    17. Podejmowanie współpracy międzynarodowej

1. WPROWADZENIE

Dyrektywa w sprawie bezpieczeństwa sieci i informacji (NIS) opublikowana w lipcu 2016 r. zobowiązuje w art. 1 i 7 państwa członkowskie do przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, zwanej także NCSS (krajowa strategia cyberbezpieczeństwa). W tym kontekście krajową strategię cyberbezpieczeństwa definiuje się jako ramy, które określają strategiczne zasady, wytyczne, cele strategiczne, priorytety, odpowiednie polityki i środki regulacyjne. Zakładanym celem krajowej strategii cyberbezpieczeństwa jest osiągnięcie i utrzymanie wysokiego poziomu bezpieczeństwa sieci i systemów, a tym samym umożliwienie państwom członkowskim ograniczenia potencjalnych zagrożeń. Co więcej, krajowa strategia cyberbezpieczeństwa może również stać się motorem rozwoju przemysłowego oraz postępu gospodarczego i społecznego.

Zgodnie z unijnym aktem o cyberbezpieczeństwie, ENISA ma obowiązek pomagać w upowszechnianiu najlepszych praktyk w zakresie definiowania i wdrażania krajowych strategii cyberbezpieczeństwa, wspierając państwa członkowskie przy wdrażaniu dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz pozyskując od nich cenne informacje zwrotne o ich doświadczeniach. W tym celu ENISA opracowała szereg narzędzi, aby móc pomagać państwom członkowskim w opracowywaniu, wdrażaniu i ocenie krajowych strategii cyberbezpieczeństwa (NCSS).

W ramach swojego mandatu ENISA ma za zadanie opracować ramy samooceny zdolności krajowych w celu zmierzenia poziomu dojrzałości poszczególnych krajowych strategii cyberbezpieczeństwa. Celem niniejszego raportu jest zaprezentowanie badania przeprowadzonego w celu określenia ram dla samooceny.

1.1 ZAKRES I CELE BADANIA

Głównym celem niniejszego badania jest opracowanie ram samooceny zdolności krajowych, zwanych dalej NCAF, w celu zmierzenia poziomu dojrzałości zdolności państw członkowskich w zakresie cyberbezpieczeństwa. Dokładniej rzecz ujmując, ramy te powinny zwiększyć możliwości państw członkowskich w zakresie:

- Przeprowadzenia oceny krajowych zdolności w zakresie cyberbezpieczeństwa;
- Poszerzenia wiedzy o poziomie dojrzałości osiągniętym przez kraj;
- Wskazania obszarów wymagających poprawy; oraz
- Budowania zdolności w zakresie cyberbezpieczeństwa.

Ramy te powinny pomóc państwom członkowskim, a w szczególności krajowym decydentom, w przeprowadzeniu samooceny mającej na celu poprawę zdolności krajowych w zakresie cyberbezpieczeństwa.

1.2 PODEJŚCIE METODOLOGICZNE

Podejście metodologiczne zastosowane do opracowania ram samooceny zdolności krajowych składa się z czterech głównych etapów:

1. **Badanie źródeł wtórnych**: Pierwszy etap polegał na przeprowadzeniu szeroko zakrojonego przeglądu literatury w celu zgromadzenia najlepszych praktyk w zakresie opracowywania ram oceny dojrzałości dla krajowych strategii cyberbezpieczeństwa. Badanie źródeł wtórnych skupia się na systematycznej analizie odpowiednich dokumentów dotyczących budowania zdolności w zakresie cyberbezpieczeństwa i

kształtowania strategii, na już istniejących krajowych strategiach cyberbezpieczeństwa państw członkowskich oraz na porównaniu istniejących modeli dojrzałości w zakresie cyberbezpieczeństwa. Przeprowadzono analizę porównawczą istniejących modeli dojrzałości poprzez przyjęcie ram analitycznych opracowanych do celów niniejszego badania. Ramy analityczne zostały oparte na metodologii Beckera[2] służącej do opracowywania modeli dojrzałości, która określa ogólny, skonsolidowany model proceduralny do projektowania modeli dojrzałości i zawiera jednoznaczne wymogi dotyczące opracowywania takich modeli. Ramy analizy zostały dodatkowo zmodyfikowane pod kątem potrzeb niniejszego badania.

2. **Pozyskanie opinii ekspertów i zainteresowanych stron**: Wychodząc od danych zebranych w ramach badania źródeł wtórnych i związanych z nimi wstępnych wyników analizy, ta faza polegała na wskazaniu ekspertów mających doświadczenie w opracowywaniu i wdrażaniu krajowych strategii cyberbezpieczeństwa lub modeli dojrzałości oraz zaproszeniu ich do rozmowy. ENISA skontaktowała się ze swoją grupą ekspertów ds. krajowych strategii cyberbezpieczeństwa oraz z krajowymi urzędnikami łącznikowymi w celu wytypowania odpowiednich ekspertów w poszczególnych państwach członkowskich. Ponadto przeprowadzono rozmowy z wybranymi ekspertami uczestniczącymi w opracowywaniu modeli dojrzałości. Ogółem przeprowadzono 22 rozmowy, w tym 19 z przedstawicielami urzędów ds. cyberbezpieczeństwa z różnych państw członkowskich (i państw EFTA).
3. **Analiza danych z inwentaryzacji:** Dane zgromadzone w wyniku badania źródeł wtórnych i rozmów zostały następnie przeanalizowane w celu wskazania najlepszych praktyk w zakresie projektowania ram samooceny służących do pomiaru dojrzałości krajowej strategii cyberbezpieczeństwa, poznania potrzeb państw członkowskich oraz ustalenia, jakie dane można faktycznie zgromadzić w poszczególnych krajach Europy[3]. Analiza umożliwiła dopracowanie wstępnego modelu opracowanego na poprzednich etapach oraz udoskonalenie zestawu wskaźników zawartych w modelu, poziomów dojrzałości i wymiarów modelu.
4. **Ukończenie modelu:** Na kolejnym etapie zmodyfikowana wersja ram samooceny zdolności krajowych została zweryfikowana przez ekspertów merytorycznych z ENISA, a następnie dodatkowo zatwierdzona przez ekspertów przed publikacją podczas warsztatów, które odbyły się w październiku 2020 r.

1.3 ODBIORCY

Raport jest skierowany do decydentów, ekspertów i urzędników państwowych odpowiedzialnych za projektowanie, wdrażanie i ocenę krajowych strategii cyberbezpieczeństwa oraz – w szerszym ujęciu – zdolności w zakresie cyberbezpieczeństwa, a także uczestniczących w tych procesach. Ponadto zawarte w nim ustalenia mogą być przydatne dla ekspertów z dziedziny. polityki cyberbezpieczeństwa i naukowców na szczeblu krajowym lub europejskim.

[2] J. Becker, R. Knackstedt i J. Pöppelbuß, „Developing Maturity Models for IT Management: A Procedure Model and its Application", Business & Information Systems Engineering, tom 1, nr 3, s. 213–222, czerwiec 2009.
[3] Do celów niniejszego badania „kraje europejskie", o których mowa w raporcie, oznaczają 27 państw członkowskich UE.

2. KONTEKST

2.1 DOTYCHCZASOWE PRACE NAD CYKLEM ŻYCIA KRAJOWYCH STRATEGII CYBERBEZPIECZEŃSTWA

Zgodnie z postanowieniami unijnego aktu o cyberbezpieczeństwie, jednym z głównych celów ENISA jest pomoc dla państw członkowskich przy opracowywaniu krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, promowanie działań na rzecz upowszechniania tych strategii i monitorowanie ich wdrażania. W ramach swojego mandatu ENISA opracowała szereg dokumentów na ten temat w celu promowania wymiany dobrych praktyk i wspierania realizacji krajowych strategii cyberbezpieczeństwa w całej Unii Europejskiej:

- „Practical guide on the development and execution phase of NCSS”[4] opublikowany w 2012 r.
- „Setting the course for national efforts to strengthen security in cyberspace”[5] opublikowany w 2012 r.
- Pierwsze ramy ENISA do oceny krajowej strategii cyberbezpieczeństwa państwa członkowskiego opublikowane[6] w 2014 r.
- „Online NCSS Interactive Map”[7] opublikowany w 2014 r.
- „NCSS Good Practice Guide”[8] opublikowany w 2016 r.
- „National Cybersecurity Strategies Evaluation Tool” (narzędzie do oceny krajowych strategii cyberbezpieczeństwa)[9] opublikowany w 2018 r.
- „Good practices in innovation on Cybersecurity under the NCSS”[10] opublikowany w 2019 r.

ZAŁĄCZNIK A zawiera krótkie podsumowanie najważniejszych publikacji ENISA na ten temat.

Powyższe przewodniki i dokumenty zostały przeanalizowane w ramach badania źródeł wtórnych. Podstawowym elementem NCAF jest w szczególności „National Cybersecurity

[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, zaktualizowana w 2019 r.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Ten dokument stanowi aktualizację przewodnika z 2012 r.: 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
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

Strategies Evaluation Tool”[11]. NCAF opiera się na celach zawartych w internetowym narzędziu do oceny krajowych strategii cyberbezpieczeństwa.

2.2 WSPÓLNE CELE OKREŚLONE W EUROPEJSKICH KRAJOWYCH STRATEGIACH CYBERBEZPIECZEŃSTWA

Różnice między poszczególnymi państwami członkowskimi utrudniają wskazanie wspólnych działań lub planów działania ze względu na odmienne konteksty krajowe, ramy prawne i programy polityczne. Cele strategiczne zapisane w krajowych strategiach cyberbezpieczeństwa państw członkowskich często dotyczą jednak tych samych zagadnień. W związku z tym, w oparciu o wcześniejszy dorobek ENISA i analizy krajowych strategii cyberbezpieczeństwa państw członkowskich, określone zostały 22 cele strategiczne. 15 z nich zostało już wskazanych w ramach wcześniejszych prac ENISA, dwa z nich zostały dodane w tym badaniu, a pięć zostało wskazanych jako możliwe do uwzględnienia w przyszłości.

2.2.1 Typowe cele strategiczne uwzględnione przez państwa członkowskie

W oparciu o wcześniejsze prace ENISA, a konkretnie narzędzie do oceny krajowych strategii cyberbezpieczeństwa[12], w poniższej tabeli zamieszczono zestawienie wspomnianego powyżej zbioru 15 celów strategicznych, które są typowo uwzględniane w krajowych strategiach cyberbezpieczeństwa państw członkowskich. Cele te pozwalają dostrzec istotę ogólnej „filozofii krajowej” w tym zakresie. Więcej informacji na temat celów opisanych poniżej można znaleźć w raporcie ENISA „NCSS Good Practice Guide”[13].

Tabela 1: Typowe cele strategiczne uwzględnione przez państwa członkowskie w krajowych strategiach cyberbezpieczeństwa

Nr identyfikacyjny	Cele strategiczne NCSS	Cele
1	**Opracowanie krajowych planów awaryjnych na wypadek cyberataku**	▶ Przedstawienie i objaśnienie kryteriów, które należy stosować w celu stwierdzenia sytuacji kryzysowej; ▶ Określenie kluczowych procesów i działań mających na celu opanowanie kryzysu; oraz ▶ Jednoznaczne określenie ról i obowiązków różnych zainteresowanych stron podczas kryzysu w cyberprzestrzeni. ▶ Przedstawienie i objaśnienie kryteriów zakończenia kryzysu i/lub wskazanie osoby lub podmiotu posiadającego kompetencje, aby ogłosić koniec kryzysu.
2	**Określenie podstawowych środków bezpieczeństwa**	▶ Ujednolicenie różnych praktyk stosowanych przez organizacje w sektorze publicznym i prywatnym; ▶ Stworzenie wspólnego języka dla właściwych organów publicznych i organizacji, a także otwartych, bezpiecznych kanałów komunikacyjnych; ▶ Umożliwienie różnym zainteresowanym stronom sprawdzanie i porównywanie swoich zdolności w zakresie cyberbezpieczeństwa; ▶ Wymiana informacji na temat dobrych praktyk w dziedzinie cyberbezpieczeństwa w każdym sektorze przemysłu; oraz

[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
[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] Ten dokument stanowi aktualizację przewodnika z 2012 r.: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Nr identyfikacyjny	Cele strategiczne NCSS	Cele
		▶ Pomaganie zainteresowanym stronom w ustalaniu priorytetów dla inwestycji w dziedzinie bezpieczeństwa.
3	Organizacja ćwiczeń w zakresie cyberbezpieczeństwa	▶ Ustalenie, co wymaga przetestowania (plany i procesy, ludzie, infrastruktura, możliwości reagowania, możliwości współpracy, komunikacja itp.); ▶ Powołanie krajowego zespołu ds. planowania ćwiczeń w dziedzinie cyberbezpieczeństwa z jasno ustalonym zakresem kompetencji; oraz ▶ Włączenie ćwiczeń w dziedzinie cyberbezpieczeństwa do cyklu życia krajowej strategii cyberbezpieczeństwa lub krajowego planu awaryjnego na wypadek cyberataku.
4	Zapewnienie możliwości reagowania na incydenty	▶ Mandat – oznacza uprawnienia, role i obowiązki, które muszą zostać przydzielone zespołowi przez władze danego państwa; ▶ Portfel usług – obejmuje usługi, które zespół świadczy na swoim obszarze kompetencji lub wykorzystuje do swojego wewnętrznego funkcjonowania; ▶ Zdolności operacyjne – są to wymogi techniczne i operacyjne, których musi przestrzegać zespół; oraz ▶ Zdolności w zakresie współpracy – obejmują wymogi dotyczące wymiany informacji z innymi zespołami, które nie należą do trzech poprzednich kategorii, np. decydentami, wojskiem, organami regulacyjnymi, operatorami (krytycznej infrastruktury teleinformatycznej), organami ścigania.
5	Zwiększanie świadomości użytkowników	▶ Określanie braków w wiedzy na temat cyberbezpieczeństwa lub problematyki bezpieczeństwa informacji; oraz ▶ Uzupełnienie braków poprzez zwiększanie świadomości lub poszerzanie/wzmacnianie zasobu podstawowej wiedzy.
6	Udoskonalanie programów szkoleniowych i edukacyjnych	▶ Zwiększanie zdolności operacyjnych istniejącego personelu zajmującego się bezpieczeństwem informacji; ▶ Zachęcanie, a następnie przygotowywanie uczniów do pracy w branży cyberbezpieczeństwa; ▶ Wspieranie współpracy i zachęcanie do współpracy między środowiskami akademickimi zajmującymi się bezpieczeństwem informacji a branżą bezpieczeństwa informacji; ▶ Dostosowywanie szkoleń w zakresie cyberbezpieczeństwa do potrzeb przedsiębiorstw.
7	Wspieranie badań i rozwoju	▶ Określanie rzeczywistych przyczyn podatności zamiast usuwania ich skutków; ▶ Skupianie naukowców reprezentujących różne dyscypliny naukowe w celu poszukiwania rozwiązań wielowymiarowych i złożonych problemów, takich jak cyberzagrożenia fizyczne; ▶ Koordynowanie ze sobą potrzeb przemysłu i wyników badań naukowych, co ułatwia przechodzenie od teorii do praktyki; oraz ▶ Poszukiwanie sposobów nie tylko na utrzymanie, ale również na zwiększenie poziomu cyberbezpieczeństwa produktów i usług wspierających istniejącą infrastrukturę cybernetyczną.
8	Zachęcanie sektora prywatnego do inwestowania w środki bezpieczeństwa	▶ Określenie, w jaki sposób można zachęcać przedsiębiorstwa prywatne do inwestowania w środki bezpieczeństwa; oraz ▶ Zachęcanie przedsiębiorstw do inwestowania w bezpieczeństwo.
9	Ochrona krytycznej infrastruktury teleinformatycznej, OUK i DUC (KITI)	▶ Identyfikacja krytycznej infrastruktury teleinformatycznej; ▶ Określanie i ograniczanie istotnych zagrożeń dla KITI.
10	Walka z cyberprzestępczością	▶ Stanowienie prawa w obszarze cyberprzestępczości; oraz ▶ Zwiększenie skuteczności organów ścigania.
11	Wprowadzenie mechanizmów zgłaszania incydentów	▶ Poszerzanie wiedzy na temat ogólnego środowiska zagrożeń;

Nr identyfikacyjny	Cele strategiczne NCSS	Cele
		▶ Ocena skutków incydentów (np. naruszeń bezpieczeństwa, awarii sieci, przerw w świadczeniu usług); ▶ Poszerzanie wiedzy na temat istniejących i nowych podatności oraz rodzajów ataków; ▶ Odpowiednie dostosowywanie środków bezpieczeństwa; oraz ▶ Wdrożenie przepisów dyrektywy w sprawie bezpieczeństwa sieci i informacji dotyczących zgłaszania incydentów.
12	Wzmocnienie prywatności i ochrony danych	▶ Przyczynianie się do wzmacniania podstawowych praw w zakresie prywatności i ochrony danych.
13	Ustanowienie partnerstwa publiczno-prywatnego (PPP)	▶ Odstraszanie (w celu zniechęcania sprawców ataków); ▶ Ochrona (wykorzystuje badania nad nowymi zagrożeniami bezpieczeństwa); ▶ Wykrywanie (wykorzystuje wymianę informacji do przeciwdziałania nowym zagrożeniom); ▶ Reagowanie (w celu zapewnienia możliwości poradzenia sobie z początkowymi skutkami incydentu); oraz ▶ Przywracanie (w celu zapewnienia możliwości naprawienia ostatecznych skutków incydentu).
14	Instytucjonalizacja współpracy między agencjami publicznymi	▶ Zacieśnienie współpracy między agencjami publicznymi, których obowiązki i kompetencje są związane z cyberbezpieczeństwem; ▶ Unikanie powielania kompetencji i zasobów pomiędzy agencjami publicznymi; ▶ Poprawa i instytucjonalizacja współpracy między agencjami publicznymi w różnych obszarach cyberbezpieczeństwa.
15	Nawiązywanie współpracy międzynarodowej (nie tylko z państwami członkowskimi UE)	▶ Czerpanie korzyści z utworzenia wspólnej bazy wiedzy dla państw członkowskich UE; ▶ Stworzenie synergii pomiędzy krajowymi organami ds. cyberbezpieczeństwa; ▶ Umożliwienie i zintensyfikowanie walki z przestępczością transgraniczną.

2.2.2 Dodatkowe cele strategiczne

Na podstawie analizy źródeł wtórnych i rozmów przeprowadzonych przez ENISA określono dodatkowe cele strategiczne. Państwa członkowskie w coraz większym stopniu uwzględniają te zagadnienia w swoich krajowych strategiach cyberbezpieczeństwa lub opracowują plany działania w tym zakresie. Przedstawiono również przykłady działań realizowanych przez państwa członkowskie. Jeżeli przykład pochodzi z publicznie dostępnego źródła, zamieszczono stosowny odnośnik. W przypadku gdy przykłady opierają się na poufnych rozmowach z urzędnikami państw członkowskich UE, nie zamieszczono żadnych odnośników.

Wskazano następujące dodatkowe cele strategiczne:

- Poprawa cyberbezpieczeństwa w łańcuchu dostaw; oraz
- Ochrona tożsamości elektronicznej i budowanie zaufania do cyfrowych usług publicznych.

Poprawa cyberbezpieczeństwa w łańcuchu dostaw

Małe i średnie przedsiębiorstwa (MŚP) stanowią fundament europejskiej gospodarki. Stanowią one 99% wszystkich przedsiębiorstw w UE[14], a w 2015 r. oszacowano, że MŚP stworzyły około 85% nowych miejsc pracy i zapewniały dwie trzecie wszystkich miejsc pracy w sektorze prywatnym w UE. Ponieważ MŚP świadczą usługi na rzecz dużych przedsiębiorstw i coraz częściej współpracują z administracją publiczną[15], należy także zauważyć, że w dzisiejszych czasach, gdy wszystko jest ze sobą połączone, to właśnie MŚP stanowią słabe ogniwo w przypadku cyberataków. MŚP są bowiem najbardziej narażone na cyberataki, ale często nie stać ich na to, aby zainwestować odpowiednie środki w cyberbezpieczeństwo[16]. W związku z tym poprawa cyberbezpieczeństwa w łańcuchu dostaw powinna być realizowana ze szczególnym uwzględnieniem MŚP.

Oprócz tego systemowego podejścia, państwa członkowskie mogą również położyć nacisk na działania na rzecz cyberbezpieczeństwa określonych usług i produktów ICT, które są uznawane niezbędne: technologii ICT stosowanych w krytycznej infrastrukturze teleinformatycznej, mechanizmów bezpieczeństwa stosowanych w sektorze telekomunikacji (mechanizmy kontroli po stronie dostawców usług internetowych itp.), usług zaufania zdefiniowanych w rozporządzeniu eIDAS oraz dostawców usług w chmurze. Na przykład Polska zobowiązała się w krajowej strategii cyberbezpieczeństwa[17] na lata 2019–2024 do opracowania krajowego systemu oceny i certyfikacji cyberbezpieczeństwa jako mechanizmu zapewniania jakości w łańcuchu dostaw. Ten system certyfikacji zostanie dostosowany do unijnych ram certyfikacji produktów, usług i procesów ICT ustanowionych w unijnym akcie o cyberbezpieczeństwie (2019/881).

Poprawa cyberbezpieczeństwa w łańcuchu dostaw ma wobec tego ogromne znaczenie. Można ją osiągnąć wprowadzając zdecydowaną politykę wspierania MŚP, udostępniając wytyczne dotyczące wymogów w zakresie cyberbezpieczeństwa w zamówieniach publicznych dla administracji publicznej, wspierając współpracę w sektorze prywatnym, budując partnerstwa publiczno-prywatne, promując mechanizmy skoordynowanego ujawniania luk w zabezpieczeniach (CVD)[18], tworząc program certyfikacji produktów, w tym elementy związane z cyberbezpieczeństwem w ramach inicjatyw cyfrowych skierowanych do MŚP, a także finansując podnoszenie kwalifikacji.

Ochrona tożsamości elektronicznej i budowanie zaufania do cyfrowych usług publicznych

W lutym 2020 r. Komisja przedstawiła swoją wizję transformacji cyfrowej UE w komunikacie zatytułowanym „Kształtowanie cyfrowej przyszłości Europy”[19], stawiając sobie za cel wprowadzanie integracyjnych technologii, które będą działały na rzecz ludzi i respektowały podstawowe wartości UE. W komunikacie stwierdzono w szczególności, że wspieranie transformacji cyfrowej administracji publicznej w całej Europie jest kwestią o zasadniczym znaczeniu. W tym względzie bardzo ważne jest budowanie zaufania do rządu w odniesieniu do tożsamości cyfrowej oraz zaufania do usług publicznych. O wadze tych zagadnień świadczy również fakt, że transakcje i wymiana danych w sektorze publicznym często mają wrażliwy charakter.

Wiele państw, między innymi Dania, Estonia, Francja, Luksemburg, Malta, Hiszpania, Niderlandy i Zjednoczone Królestwo, wyraziło zamiar uwzględnienia tej tematyki w krajowych

[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
[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] Kształtowanie cyfrowej przyszłości Europy, COM(2020) 67 final: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0067&qid=1614097887230&from=EN

strategiach cyberbezpieczeństwa. Niektóre z nich stwierdziły również, że ten strategiczny cel może zostać uwzględniony jako element szerszego planu:

- Estonia powiązała swój plan działania w tym zakresie zatytułowany „Bezpieczeństwo tożsamości cyfrowej i funkcji e-uwierzytelniania" z szerszą agendą cyfrową dla Estonii 2020.
- We francuskiej krajowej strategii cyberbezpieczeństwa wskazano, że sekretarz stanu odpowiedzialny za technologie cyfrowe nadzoruje opracowanie planu działania „w celu ochrony życia cyfrowego, prywatności i danych osobowych obywateli Francji".
- W niderlandzkiej krajowej strategii cyberbezpieczeństwa stwierdzono, że cyberbezpieczeństwo w administracji publicznej, a także usługi publiczne świadczone na rzecz obywateli i przedsiębiorstw, zostały bardziej szczegółowo omówione w ogólnej agendzie na rzecz administracji cyfrowej.
- Ponieważ rząd Zjednoczonego Królestwa przenosi kolejne usługi do internetu, powołał urząd Government Digital Service (GDS), którego zadaniem jest dopilnowanie, by wszystkie nowe usługi cyfrowe tworzone lub zamawiane przez rząd były zgodne z założeniami „secure by default" (domyślnie zapewnione bezpieczeństwo), przy wsparciu ze strony brytyjskiego Narodowego Centrum Cyberbezpieczeństwa (NCSC).

2.2.3 Inne rozpatrywane cele strategiczne

Na etapie badania źródeł wtórnych oraz w ramach rozmów przeprowadzanych przez ENISA badane były również inne cele strategiczne. Zdecydowano jednak, że nie zostaną one włączone do ram samooceny. ZAŁĄCZNIK C – Pozostałe cele objęte badaniem

zawiera definicje tych celów. Mogą one stać się przedmiotem dalszych rozmów dotyczących możliwości udoskonalania krajowych strategii cyberbezpieczeństwa.

Na potrzeby przyszłych rozważań wskazano następujące cele strategiczne:

- Opracowanie sektorowych strategii cyberbezpieczeństwa.
- Walka z kampaniami dezinformacyjnymi.
- Bezpieczeństwo najnowocześniejszych technologii (5G, sztuczna inteligencja, informatyka kwantowa itp.);
- Zapewnianie suwerenności danych; oraz
- Zachęcanie do rozwoju sektora ubezpieczeń cybernetycznych.

2.3 NAJWAŻNIEJSZE WNIOSKI Z ANALIZY PORÓWNAWCZEJ

Badanie źródeł wtórnych przeprowadzone na istniejących modelach dojrzałości związanych z cyberbezpieczeństwem miało na celu zebranie informacji i dowodów na potrzeby opracowania ram samooceny zdolności krajowych w obszarze krajowych strategii cyberbezpieczeństwa. W tym kontekście przeprowadzony został szeroko zakrojony przegląd literatury dotyczącej istniejących modeli, który uzupełnił wnioski ze wstępnych badań zakresowych dotyczących modeli dojrzałości w zakresie cyberbezpieczeństwa oraz istniejących krajowych strategii cyberbezpieczeństwa, szerzej opisany w punkcie 2.1 i 2.2. Ten przegląd systematyczny pomógł w wybraniu i uzasadnieniu poziomów dojrzałości do ram oceny oraz zdefiniowaniu różnych wymiarów i wskaźników.

W ramach przeglądu systematycznego modeli dojrzałości rozpatrzono i przeanalizowano 10 modeli na podstawie ich kluczowych cech. Ogólne zestawienie kluczowych cech poszczególnych modeli przeanalizowanych w ramach tego badania jest dostępne w Tabela 2: Zestawienie przeanalizowanych modeli dojrzałości, natomiast dokładniejszą analizę można znaleźć w ZAŁĄCZNIK A.

Tabela 2: Zestawienie przeanalizowanych modeli dojrzałości

Nazwa modelu	Liczba poziomów dojrzałości	Liczba atrybutów	Metoda oceny	Przedstawienie wyników
Model zdolności w zakresie cyberbezpieczeństwa dla państw (Cybersecurity Capacity Maturity Model for Nations, CMM)	5	5 głównych wymiarów	Współpraca z lokalną organizacją w celu dopracowania modelu przed zastosowaniem go w kontekście krajowym	Pięcioelementowy wykres radarowy
Model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Cybersecurity Capability Maturity Model, C2M2)	4	10 głównych dziedzin	Metodologia i zestaw narzędzi do samooceny	Karta oceny z wykresami kołowymi
Ramy na rzecz poprawy cyberbezpieczeństwa infrastruktury krytycznej (Framework for Improving Critical Infrastructure Cybersecurity)	nd. (4 poziomy)	5 podstawowych funkcji	Samoocena	nd.
Katarski model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Qatar Cybersecurity Capability Maturity Model, Q-C2M2)	5	5 głównych dziedzin	nd.	nd.
Certyfikacja modelu dojrzałości cyberbezpieczeństwa (Cybersecurity Maturity Model Certification, CMMC)	5	17 głównych dziedzin	Ocena dokonywana przez audytorów zewnętrznych	nd.
Społecznościowy model dojrzałości cyberbezpieczeństwa (The Community Cybersecurity Maturity Model, CCSMM)	5	6 głównych wymiarów	Ocena przeprowadzana wewnątrz społeczności z udziałem państwowych i federalnych organów ścigania	nd.
Model dojrzałości bezpieczeństwa informacji na potrzeby ram cyberbezpieczeństwa NIST (Information Security Maturity Model for NIST Cybersecurity Framework, ISMM)	5	23 oceniane obszary	nd.	nd.
Model audytu wewnętrznego (IA-CM) dla sektora publicznego (Internal Audit Capability Model (IA-CM) for the Public Sector)	5	6 elementów	Samoocena	nd.
Globalny indeks cyberbezpieczeństwa (Global Cybersecurity Index, GCI)	nd.	5 filarów	Samoocena	Tabela rankingowa
Indeks potęgi cybernetycznej (Cyber Power Index, CPI)	nd.	4 kategorie	Analiza porównawcza przeprowadzona przez Economist Intelligence Unit	Tabela rankingowa

Przeprowadzony przegląd systematyczny umożliwił wyciągnięcie wniosków na temat najlepszych praktyk przyjętych w istniejących modelach w celu wsparcia rozwoju modelu koncepcyjnego dla aktualnego modelu dojrzałości. Analiza porównawcza pomogła zwłaszcza w zdefiniowaniu poziomów dojrzałości, stworzeniu grup wymiarów oraz wyborze wskaźników, a także odpowiedniej metody wizualizacji wyników modelu. Najistotniejsze ustalenia dla każdego z tych elementów przedstawiono w Tabela 3.

Tabela 3: Najważniejsze wnioski z analizy porównawczej

Element	Najważniejszy wniosek
Poziomy dojrzałości	▶ Pięciostopniowa skala dojrzałości dla ram oceny zdolności w zakresie cyberbezpieczeństwa jest powszechnie przyjęta i umożliwia otrzymanie szczegółowych wyników oceny (Tabela 6 Porównanie poziomów dojrzałości zawiera wyczerpujące zestawienie definicji poziomów dojrzałości dla poszczególnych modeli); ▶ Wszystkie modele zawierają ogólną definicję poszczególnych poziomów dojrzałości, która jest następnie dostosowywana do różnych wymiarów lub grup wymiarów; ▶ W ramach pomiaru dojrzałości zdolności w zakresie cyberbezpieczeństwa ocenia się zazwyczaj dwa aspekty: dojrzałość strategii i dojrzałość procesów wprowadzonych w celu ich realizacji.
Atrybuty	▶ Wyniki analizy porównawczej atrybutów istniejących modeli dojrzałości są niejednorodne, przy czym średnia liczba atrybutów w jednym modelu wynosi od czterech do pięciu; ▶ Model oparty na około czterech lub pięciu atrybutach zapewnia krajom odpowiedni poziom szczegółowości danych, grupując odpowiednie wymiary i zapewniając czytelność wyników (zob. opis atrybutów dla poszczególnych modeli w Tabela 7: Porównanie atrybutów/ wymiarów); ▶ Najważniejsza zasada przyjęta we wszystkich modelach przy definiowaniu grup wymiarów dotyczy spójności elementów wchodzących w skład poszczególnych grup.
Metoda oceny	▶ Metody oceny stosowane w poszczególnych analizowanych modelach różnią się między sobą; ▶ Najczęściej występującą metodą oceny jest samoocena.
Przedstawienie wyników	▶ Ważne jest, aby wyniki były przedstawiane na różnych poziomach szczegółowości; ▶ Metodologia wizualizacji powinna być jasna i przystępna.

Model koncepcyjny został skonstruowany w oparciu o analizę porównawczą różnych modeli dojrzałości, a także istniejący dorobek ENISA. Podjęto również decyzję o zastosowaniu *interaktywnego narzędzia internetowego ENISA* do opracowania wskaźników dojrzałości wykorzystywanych dla poszczególnych atrybutów.

2.4 WYZWANIA ZWIĄZANE Z OCENĄ KRAJOWYCH STRATEGII CYBERBEZPIECZEŃSTWA

Przy budowie zdolności w zakresie cyberbezpieczeństwa państwa członkowskie muszą się mierzyć z wieloma wyzwaniami, zwłaszcza jeżeli chodzi o zapewnienie, aby zdolności te zawsze nadążały za zachodzącymi zmianami. Poniżej przedstawiono zestawienie wyzwań wskazanych przez państwa członkowskie i omówionych z nimi w ramach przeprowadzonego badania:

- **Trudności w koordynacji i współpracy:** Koordynowanie działań w zakresie cyberbezpieczeństwa na szczeblu krajowym w celu zapewnienia skutecznego reagowania na problemy cyberbezpieczeństwa może okazać się wyzwaniem ze względu na dużą liczbę zainteresowanych stron.
- **Brak zasobów do przeprowadzania oceny:** W zależności od kontekstu lokalnego i krajowej struktury zarządzania w zakresie cyberbezpieczeństwa, ocena krajowej strategii cyberbezpieczeństwa i jej celów może zająć nawet ponad 15 osobodni.
- **Brak wsparcia dla rozwoju zdolności w zakresie cyberbezpieczeństwa:** Niektóre państwa członkowskie poinformowały, że w celu uzasadnienia potrzeb budżetowych i uzyskania wsparcia dla rozwoju zdolności w zakresie cyberbezpieczeństwa, najpierw muszą zrealizować fazę oceny, która umożliwi określenie braków i ograniczeń.

- **Trudności w przypisywaniu sukcesów lub zmian do strategii:** Ponieważ codziennie pojawiają się nowe zagrożenia, a technologia idzie naprzód, plany działań muszą być stale dostosowywane w odpowiedzi na zmiany. Ocena krajowej strategii cyberbezpieczeństwa i przypisywanie zmian do samej strategii pozostają jednak żmudnym zadaniem. To z kolei utrudnia określanie ograniczeń i braków w krajowej strategii cyberbezpieczeństwa.
- **Trudności w pomiarze skuteczności krajowej strategii cyberbezpieczeństwa:** Do prowadzenia pomiarów w różnych obszarach, takich jak postępy, wdrażanie, dojrzałość i skuteczność, mogą być stosowane mierniki. Choć pomiar postępów i wdrażania jest stosunkowo prosty w porównaniu z pomiarem skuteczności, to właśnie skuteczność jest bardziej istotna dla oceny efektów i skutków krajowej strategii cyberbezpieczeństwa. Z rozmów przeprowadzonych przez ENISA wynika, że wiele państw członkowskich stwierdziło, iż ilościowa ocena skuteczności krajowej strategii cyberbezpieczeństwa jest istotna, ale jednocześnie stanowi bardzo wymagające zadanie, którego wykonanie bywa zupełnie niemożliwe.
- **Trudności z przyjęciem wspólnych ram:** Państwa członkowskie UE różnią się sytuacją w zakresie polityki, organizacji, kultury, struktury społecznej i dojrzałości krajowej strategii cyberbezpieczeństwa. Niektóre państwa członkowskie, z którymi przeprowadzono rozmowy w ramach tego badania, stwierdziły, że uzasadnienie i stosowanie uniwersalnych ram samooceny może okazać się trudne.

2.5 KORZYŚCI WYNIKAJĄCE Z OCENY ZDOLNOŚCI KRAJOWYCH

Od 2017 r. wszystkie państwa członkowskie UE posiadają krajową strategię cyberbezpieczeństwa[20]. Choć jest to pozytywne zjawisko, ważne jest również, aby państwa członkowskie potrafiły prawidłowo ocenić te strategie, zapewniając tym samym wartość dodaną dla planowania strategicznego i realizacji strategii.

Jednym z celów ram oceny zdolności krajowych jest ocena zdolności w zakresie cyberbezpieczeństwa w oparciu o priorytety określone w różnych krajowych strategiach cyberbezpieczeństwa. Zasadniczo ramy te oceniają poziom dojrzałości zdolności państw członkowskich w zakresie cyberbezpieczeństwa w dziedzinach zdefiniowanych przez cele tych strategii. Rezultaty zastosowania ram pomagają zatem decydentom z państw członkowskich w kształtowaniu krajowych strategii cyberbezpieczeństwa, dostarczając im danych na temat aktualnej sytuacji w kraju[21]. Nadrzędnym celem NCAF jest pomaganie państwom członkowskim we wskazywaniu obszarów wymagających poprawy oraz w budowaniu zdolności.

Ramy zostały opracowane w celu umożliwienia państwom członkowskim przeprowadzenia samooceny osiągniętego poziomu dojrzałości w drodze oceny celów krajowej strategii cyberbezpieczeństwa, co pomoże im wzmacniać i budować zdolności w zakresie cyberbezpieczeństwa na poziomie strategicznym i operacyjnym.

W bardziej praktycznym ujęciu, w rozmowach przeprowadzonych przez ENISA z kilkoma agencjami odpowiedzialnymi za dziedzinę cyberbezpieczeństwa w rożnych państwach członkowskich wskazywano i podkreślano następujące korzyści związane z ramami oceny zdolności krajowych:

- Uzyskanie przydatnych informacji do opracowania długoterminowej strategii (np. dobre praktyki, wytyczne);
- Pomoc we wskazaniu braków w krajowej strategii cyberbezpieczeństwa;

[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.

- Pomoc w dalszym budowaniu zdolności w zakresie cyberbezpieczeństwa;
- Zapewnienie rozliczalności działań o charakterze politycznym;
- Przydawanie wiarygodności w oczach ogółu społeczeństwa i partnerów międzynarodowych;
- Wspieranie działań informacyjnych i poprawa wizerunku publicznego jako przejrzyście działającej organizacji;
- Pomoc w przewidywaniu nadchodzących problemów;
- Pomoc w wyciąganiu wniosków i wskazywaniu najlepszych praktyk;
- Ustalenie poziomu bazowego dla zdolności w zakresie cyberbezpieczeństwa w całej UE dla ułatwienia rozmów; oraz
- Pomoc w ocenie krajowych zdolności w zakresie cyberbezpieczeństwa.

3. METODOLOGIA RAM OCENY ZDOLNOŚCI KRAJOWYCH

3.1 OGÓLNY CEL

Głównym celem NCAF jest pomiar poziomu dojrzałości zdolności **państw członkowskich** w zakresie cyberbezpieczeństwa, który umożliwi wsparcie tych państw przy przeprowadzaniu oceny krajowych zdolności w zakresie cyberbezpieczeństwa, zwiększanie świadomości na temat poziomu dojrzałości danego państwa, określanie obszarów wymagających poprawy oraz budowanie zdolności w zakresie cyberbezpieczeństwa.

3.2 POZIOMY DOJRZAŁOŚCI

Ramy opierają się na pięciu **poziomach dojrzałości**, które określają kolejne etapy pokonywane przez państwa członkowskie podczas budowania zdolności w zakresie cyberbezpieczeństwa w obszarach objętych poszczególnymi celami krajowych strategii cyberbezpieczeństwa. Każdy kolejny poziom oznacza wyższy stopień dojrzałości, począwszy od **poziomu 1**, na którym państwa członkowskie nie posiadają jasno określonego podejścia do budowania zdolności w zakresie cyberbezpieczeństwa w obszarach objętych celami krajowej strategii cyberbezpieczeństwa, a skończywszy na **poziomie 5**, gdzie strategia budowania zdolności w zakresie cyberbezpieczeństwa jest dynamiczna i można ją przystosowywać do zmian zachodzących w otoczeniu. Tabela 4 przedstawia skalę poziomów dojrzałości wraz z opisem poszczególnych poziomów dojrzałości.

Tabela 4: Pięciostopniowa skala dojrzałości ram oceny zdolności krajowych ENISA

POZIOM 1 – WSTĘPNY/DORAŹNY	POZIOM 2 – WCZESNA DEFINICJA	POZIOM 3 – USTANOWIENIE	POZIOM 4 – OPTYMALIZACJA	POZIOM 5 – ZDOLNOŚĆ ADAPTACJI
Państwo członkowskie nie posiada jasno określonego podejścia do budowania zdolności w zakresie cyberbezpieczeństwa w obszarach objętych celami krajowej strategii cyberbezpieczeństwa. Niemniej jednak mogło nakreślić pewne ogólne cele i przeprowadzić pewne badania (techniczne lub polityczne) w celu poprawy zdolności krajowych.	Określono krajowe podejście do budowania zdolności w obszarze objętym celami krajowej strategii cyberbezpieczeństwa. Istnieją plany działania lub prowadzone są działania mające na celu osiągnięcie rezultatów, ale są one mało zaawansowane. Ponadto mogły zostać wskazane lub zaangażowane aktywne zainteresowane strony.	Plan działania w zakresie budowania zdolności w obszarze objętym celami krajowej strategii cyberbezpieczeństwa został jasno zdefiniowany i ma poparcie odpowiednich zainteresowanych stron. Praktyki i działania są w jednolity sposób egzekwowane i wdrażane na szczeblu krajowym. Działania są definiowane i dokumentowane, przy czym określono jasny podział zasobów, sposób zarządzania i terminy realizacji.	Plan działania jest regularnie poddawany ocenie: wyznaczono w nim priorytety, został zoptymalizowany i jest trwały. Efektywność działań mających na celu budowanie zdolności w zakresie cyberbezpieczeństwa jest regularnie mierzona. Określono czynniki sukcesu, wyzwania i braki w realizacji działań.	Strategia budowania zdolności w zakresie cyberbezpieczeństwa jest dynamiczna i można ją przystosowywać do zmian. Nieustanne śledzenie zmian w otoczeniu (postępu technicznego, konfliktów światowych, nowych zagrożeń itp.) sprzyja sprawnemu podejmowaniu decyzji oraz możliwości szybkiego podejmowania działań na rzecz poprawy.

3.3 GRUPY ORAZ NADRZĘDNA STRUKTURA RAM SAMOOCENY

Ramy samooceny dzielą się na **cztery grupy**: (I) Zarządzanie cyberbezpieczeństwem i normy w zakresie cyberbezpieczeństwa, (II) Budowanie zdolności i zwiększanie świadomości, (III) Aspekty prawne i regulacyjne oraz (IV) Współpraca. Każda z tych grup obejmuje obszar tematyczny ważny dla budowania zdolności w zakresie cyberbezpieczeństwa w danym kraju oraz zawiera zbiór różnych celów, które mogą być uwzględniane przez państwa członkowskie w ich krajowych strategiach cyberbezpieczeństwa. W szczególności:

- **(I) Zarządzanie cyberbezpieczeństwem i normy w zakresie cyberbezpieczeństwa**: ta grupa mierzy zdolność państw członkowskich do wprowadzenia odpowiedniego sposobu zarządzania, norm i dobrych praktyk w dziedzinie cyberbezpieczeństwa. Wymiar ten uwzględnia różne aspekty cyberobrony i cyberodporności, a jednocześnie wspiera rozwój krajowego sektora cyberbezpieczeństwa i budowanie zaufania do władz państwowych;
- **(II) Budowanie zdolności i zwiększanie świadomości**: ta grupa ocenia zdolność państw członkowskich do budowania świadomości na temat ryzyka i zagrożeń dla cyberbezpieczeństwa oraz przeciwdziałania tym ryzykom i zagrożeniom. Ponadto wymiar ten mierzy zdolność kraju do ciągłego budowania zdolności w zakresie cyberbezpieczeństwa oraz do podnoszenia ogólnego poziomu wiedzy i umiejętności w tej dziedzinie. Uwzględnia on rozwój rynku cyberbezpieczeństwa oraz postępy działalności badawczo-rozwojowej w zakresie cyberbezpieczeństwa. Ta grupa reorganizuje wszystkie cele, tworząc fundamenty do budowania zdolności.
- **(III) Aspekty prawne i regulacyjne**: ta grupa mierzy zdolność państw członkowskich do wprowadzania niezbędnych instrumentów prawnych i regulacyjnych w celu reagowania na wzrost cyberprzestępczości i związanych z nią incydentów w

cyberprzestrzeni oraz przeciwdziałania ich wzrostowi, a także do ochrony krytycznej infrastruktury teleinformatycznej. Wymiar ten ocenia również zdolność państw członkowskich do stworzenia ram zapewniających ochronę dla obywateli i przedsiębiorstw, tak jak w przypadku zapewnienia równowagi między bezpieczeństwem a prywatnością; oraz

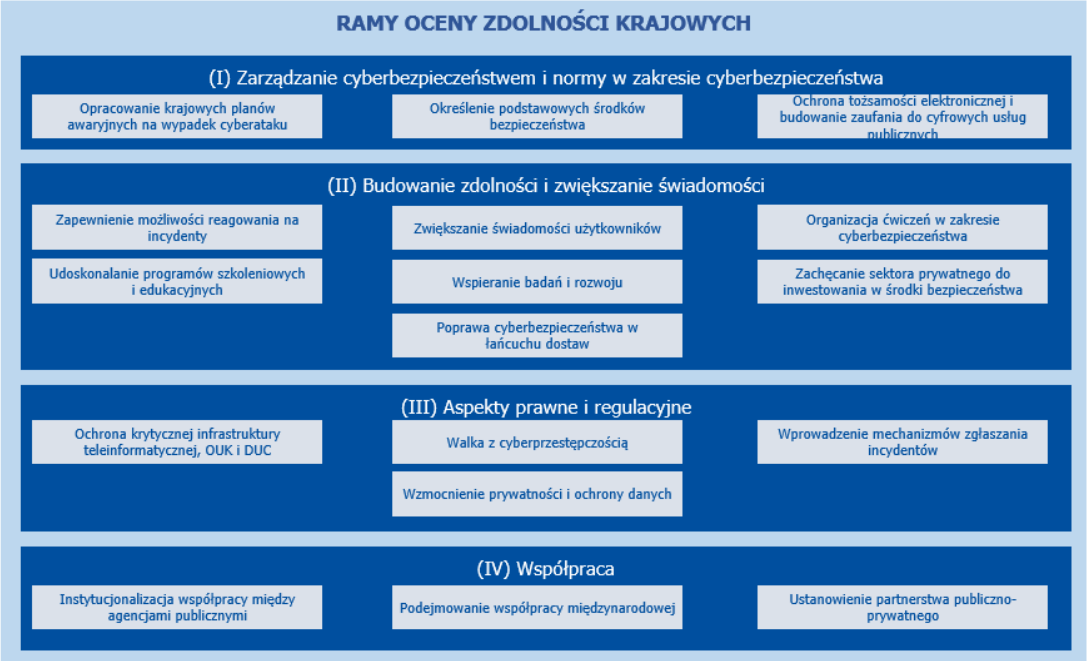
- **(IV) Współpraca:** ta grupa ocenia współpracę i wymianę informacji między różnymi grupami zainteresowanych stron na szczeblu krajowym i międzynarodowym, która stanowi ważne narzędzie, umożliwiające lepsze poznanie stale zmieniającego się środowiska zagrożeń i lepsze reagowanie na te zagrożenia.

Cele uwzględnione w modelu są powszechnie przyjmowane przez państwa członkowskie i zostały wybrane spośród celów wymienionych w punkcie 2.2. W modelu ocenia się w szczególności następujące cele:

- 1. Opracowanie krajowych planów awaryjnych na wypadek cyberataku (I)
- 2. Określenie podstawowych środków bezpieczeństwa (I)
- 3. Ochrona tożsamości elektronicznej i budowanie zaufania do cyfrowych usług publicznych (I)
- 4. Zapewnienie możliwości reagowania na incydenty (II)
- 5. Zwiększanie świadomości użytkowników (II)
- 6. Organizacja ćwiczeń w zakresie cyberbezpieczeństwa (II)
- 7. Udoskonalanie programów szkoleniowych i edukacyjnych (II)
- 8. Wspieranie badań i rozwoju (II)
- 9. Zachęcanie sektora prywatnego do inwestowania w środki bezpieczeństwa (II)
- 10. Poprawa cyberbezpieczeństwa w łańcuchu dostaw (II)
- 11. Ochrona krytycznej infrastruktury teleinformatycznej, OUK i DUC (III)
- 12. Walka z cyberprzestępczością (III)
- 13. Wprowadzenie mechanizmów zgłaszania incydentów (III)
- 14. Wzmocnienie prywatności i ochrony danych (III)
- 15. Instytucjonalizacja współpracy między agencjami publicznymi (IV)
- 16. Podejmowanie współpracy międzynarodowej (IV)
- 17. Ustanowienie partnerstwa publiczno-prywatnego (IV)

W modelu połączono cztery grupy i należące do nich cele, aby uzyskać całościowy obraz dojrzałości zdolności państw członkowskich w zakresie cyberbezpieczeństwa. Rys. 1 przedstawia nadrzędną strukturę ram samooceny i pokazuje, w jaki sposób te elementy, czyli cele, grupy i ramy samooceny, są powiązane z oceną wyników dla danego kraju.

Rys. 1: Struktura ram samooceny



Dla każdego celu objętego ramami samooceny istnieje szereg wskaźników podzielonych pomiędzy pięć poziomów dojrzałości. Każdy wskaźnik opiera się na dychotomicznym pytaniu (odpowiedź tak/nie). Wskaźnik może być obowiązkowy lub nieobowiązkowy.

3.4 MECHANIZM OCENY PUNKTOWEJ

Mechanizm oceny punktowej zastosowany w ramach samooceny uwzględnia powyższe elementy oraz zasady wymienione w punkcie 3.5. W rzeczywistości ocena punktowa w modelu opiera się na wartości dwóch parametrów – **poziomu dojrzałości** oraz **wskaźnika pokrycia**. Każdy z tych parametrów można obliczyć na różnych poziomach: (i) dla każdego celu, (ii) dla grupy celów lub (iii) zbiorczo.

Ocena punktowa na poziomie celów

Ocena punktowa poziomu dojrzałości informuje o poziomie dojrzałości, pokazując, jakie zdolności i praktyki zostały wprowadzone. Ocenę punktową poziomu dojrzałości oblicza się jako najwyższy poziom, na którym respondent spełnił wszystkie wymogi (tj. udzielił odpowiedzi twierdzącej na wszystkie pytania obowiązkowe), spełniwszy również wszystkie wymogi dla poprzednich poziomów dojrzałości.

Wskaźnik pokrycia pokazuje zakres pokrycia wszystkich wskaźników, dla których udzielono odpowiedzi twierdzącej, niezależnie od ich poziomu. Jest to wartość uzupełniająca, uwzględniająca wszystkie wskaźniki mierzące dany cel. Wskaźnik pokrycia oblicza się jako stosunek łącznej liczby pytań w ramach danego celu do liczby pytań, na które udzielono odpowiedzi twierdzącej.

Należy wyjaśnić, że w pozostałej części dokumentu termin ***„ocena punktowa”*** może odnosić się zarówno do wartości poziomu dojrzałości, jak i do wskaźnika pokrycia.

Rys. 2 – Mechanizm oceny punktowej dla poszczególnych celów przedstawia wizualizację mechanizmu oceny opisanego w punkcie 3.1, który zostanie dokładniej opisany poniżej.

Rys. 2: Mechanizm oceny punktowej dla poszczególnych celów

Rys. 2 przedstawia przykład obliczenia poziomu dojrzałości dla celu.Warto zauważyć, że respondent spełnił wszystkie obowiązkowe wymogi dla pierwszych trzech poziomów dojrzałości, ale tylko częściowo spełnił te wymogi dla poziomu 4. Ocena punktowa wskazuje zatem na to, ***że poziom dojrzałości respondenta dla celu „Organizowanie ćwiczeń w dziedzinie cyberbezpieczeństwa" to poziom 3****.*

Jednakże w przykładzie przedstawionym na Rys. 2, poziom dojrzałości celu nie może uwzględnić informacji dostarczanych przez wskaźniki, dla których uzyskano wynik pozytywny, i które wykraczają ponad 3. poziom dojrzałości. W takim przypadku obraz wszystkich elementów wdrożonych przez respondenta, aby zrealizować cel, niezależnie od rzeczywistego poziomu dojrzałości, może zapewnić wskaźnik pokrycia. W tym przypadku stosunek łącznej liczby pytań w ramach celu do liczby pytań, na które udzielono odpowiedzi twierdzącej, wynosi 19/27, co oznacza, że ***wartość wskaźnika pokrycia wynosi 70%.***

Ponadto, aby uwzględnić specyfikę poszczególnych państw członkowskich, a jednocześnie zapewnić spójny obraz, wynik oblicza się na podstawie dwóch różnych prób na poziomie grupy i na poziomie zbiorczym:

- **Ogólna ocena punktowa:** jedna kompletna próba obejmująca wszystkie cele z danej grupy lub w całych ramach (od 1 do 17);
- **Szczegółowe oceny punktowe:** jedna, konkretna próba, obejmująca wyłącznie cele wybrane przez państwo członkowskie (zazwyczaj odpowiadające celom zawartym w krajowej strategii cyberbezpieczeństwa danego państwa) w danej grupie lub w całych ramach.

Ocena punktowa na poziomie grupy

Ogólny poziom dojrzałości dla poszczególnych grup oblicza się jako średnią arytmetyczną poziomu dojrzałości wszystkich celów w danej grupie.

Szczegółowy poziom dojrzałości dla poszczególnych grup oblicza się jako średnią arytmetyczną poziomu dojrzałości wszystkich celów w danej grupie, które państwo

członkowskie postanowiło ocenić (zazwyczaj odpowiadają one celom zawartym w krajowej strategii cyberbezpieczeństwa danego kraju).

Na przykład z rys. Rys. 1 wynika, że w skład grupy (I) Zarządzanie cyberbezpieczeństwem i normy w zakresie cyberbezpieczeństwa wchodzą trzy cele. Zakładając, że respondent zdecydował się ocenić tylko dwa pierwsze cele, pomijając trzeci, oraz że dwa pierwsze cele odpowiadają odpowiednio 2. i 4. poziomowi dojrzałości, poziom dojrzałości grupy z uwzględnieniem wszystkich celów to poziom 2 (ogólny poziom dojrzałości grupy (I) = (2 + 4)/3), natomiast poziom dojrzałości grupy uwzględniający jedynie konkretne cele wybrane przez oceniającego to poziom 3 (szczegółowy poziom dojrzałości grupy (I) = (2 + 4)/2).

Ogólny wskaźnik pokrycia dla poszczególnych grup oblicza się jako stosunek łącznej liczby pytań w ramach danej grupy do liczby pytań, na które udzielono odpowiedzi twierdzącej.

Szczegółowy wskaźnik pokrycia dla poszczególnych grup oblicza się jako stosunek łącznej liczby pytań w ramach danej grupy odnoszących się do celów, które państwo członkowskie zdecydowało się ocenić (zazwyczaj odpowiadających celom określonym w krajowej strategii bezpieczeństwa cybernetycznego danego państwa) do liczby pytań, na które udzielono odpowiedzi twierdzącej.

Oceny punktowe na poziomie zbiorczym

Zbiorczy ogólny poziom dojrzałości dla danego kraju oblicza się jako średnią arytmetyczną poziomu dojrzałości wszystkich celów objętych ramami oceny, od 1 do 17.

Zbiorczy szczegółowy poziom dojrzałości dla danego kraju oblicza się jako średnią arytmetyczną poziomu dojrzałości wszystkich celów w ramach oceny, które państwo członkowskie postanowiło ocenić (zazwyczaj odpowiadają one celom zawartym w krajowej strategii cyberbezpieczeństwa danego kraju).

Zbiorczy ogólny wskaźnik pokrycia dla danego kraju oblicza się jako stosunek łącznej liczby pytań w ramach wszystkich celów objętych ramami oceny (od 1 do 17) do liczby pytań, na które udzielono odpowiedzi twierdzącej.

Zbiorczy szczegółowy wskaźnik pokrycia dla danego kraju oblicza się jako stosunek łącznej liczby pytań odnoszących się do celów objętych ramami oceny, które państwo członkowskie zdecydowało się ocenić (zazwyczaj odpowiadających celom określonym w krajowej strategii bezpieczeństwa cybernetycznego danego państwa) do liczby pytań, na które udzielono odpowiedzi twierdzącej.

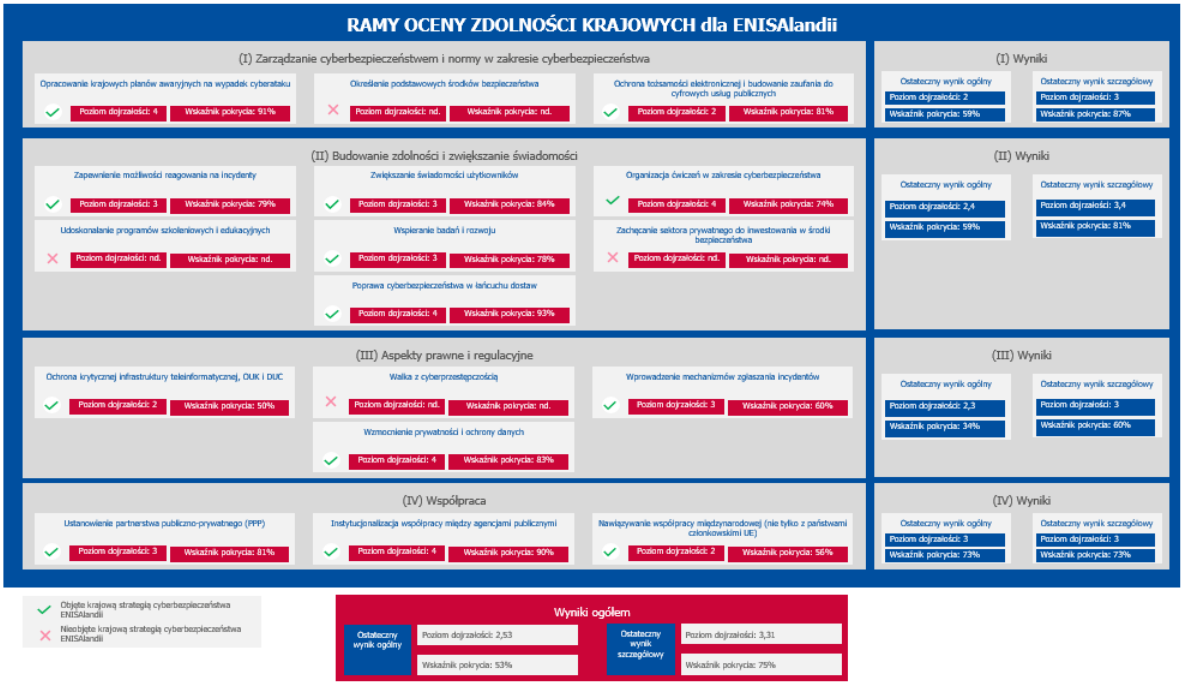
Przy każdym wskaźniku respondenci mogą wybrać w odpowiedzi trzecią możliwość „nie wiem/nie dotyczy". W takim przypadku wskaźnik nie jest uwzględniany przy obliczaniu łącznych wyników.

Poziomy dojrzałości na poziomie grupy i na poziomie zbiorczym oblicza się za pomocą średniej arytmetycznej, aby wykazać, jakie postępy osiągnięto pomiędzy jedną oceną a drugą. Inna możliwość, polegająca na obliczeniu poziomów dojrzałości dla grupy i w ujęciu zbiorczym jako poziomu dojrzałości celu o najmniejszej dojrzałości – choć jest miarodajna z punktu widzenia dojrzałości – nie uwzględni postępów poczynionych w obszarach objętych innymi celami.

Ponieważ poziom grupy i poziom ogólny podlegają konsolidacji do celów sprawozdawczości, zdecydowano się na zastosowanie średniej arytmetycznej. Dla większej dokładności, na potrzeby sprawozdawczości należy posługiwać się ocenami punktowymi na poziomie celów.

Rys. 3 poniżej zawiera podsumowanie mechanizmów oceny punktowej na różnych poziomach modelu (cel, grupa, ujęcie zbiorcze).

Rys. 3: Ogólny mechanizm oceny punktowej



3.5 WYMOGI DOTYCZĄCE RAM SAMOOCENY

Ramy oceny zdolności krajowych przedstawione w tym punkcie opierają się na potrzebach wskazanych przez państwa członkowskie i zostały skonstruowane na podstawie zbioru następujących wymogów:

- Ramy NCAF są dobrowolnie wprowadzane przez państwo członkowskie jako ramy samooceny;
- Zadaniem NCAF jest mierzenie zdolności państw członkowskich w zakresie cyberbezpieczeństwa w odniesieniu do 17 celów. Państwo członkowskie może jednak wybrać cele do przeprowadzenia oceny i przeprowadzić ocenę w oparciu o podzbiór tych 17 celów;
- Ramy samooceny służą do pomiaru poziomu dojrzałości zdolności państwa członkowskiego w zakresie cyberbezpieczeństwa;
- Wyniki oceny nie zostaną opublikowane, chyba że państwo członkowskie zdecyduje o tym z własnej inicjatywy;
- Państwo członkowskie może przedstawiać wyniki oceny, prezentując poziom dojrzałości swoich zdolności w zakresie cyberbezpieczeństwa, grupy celów lub nawet jednego celu;
- Wszystkie oceniane cele są jednakowo istotne w ramach oceny, w związku z czym są tak samo ważne. To samo odnosi się do wskaźników stosowanych w ramach oceny; oraz
- Państwo członkowskie jest w stanie monitorować postępy w czasie.

Ramy samooceny służą wspieraniu państw członkowskich w budowaniu zdolności w zakresie cyberbezpieczeństwa. Dlatego obejmują one również zbiór zaleceń lub wytycznych, które mają pomóc państwom europejskim w osiągnięciu wyższego poziomu dojrzałości.

Uwaga: te zalecenia lub wytyczne mają charakter ogólny i opierają się na publikacjach ENISA oraz doświadczeniach zdobytych w innych krajach, oraz będą się opierać na wynikach samooceny.

4. WSKAŹNIKI NCAF

4.1 WSKAŹNIKI RAMOWE

W tym punkcie zostały przedstawione wskaźniki ram oceny zdolności krajowych ENISA. Poniższe punkty zostały podzielone według grup.

Dla każdej grupy przedstawiono w tabeli pełny zestaw wskaźników w formie pytań reprezentatywnych dla danego poziomu dojrzałości. Głównym narzędziem samooceny jest ankieta. Dla każdego celu istnieją dwa zestawy wskaźników:

- Zestaw ogólnych pytań dotyczących dojrzałości strategii (9 pytań ogólnych), oznaczonych od „a" do „c" dla każdego poziomu dojrzałości, takich samych dla każdego celu; oraz
- Zestaw pytań dotyczących zdolności w zakresie cyberbezpieczeństwa (319 pytań dotyczących zdolności w zakresie cyberbezpieczeństwa), ponumerowanych od „1" do „10" dla każdego poziomu dojrzałości, innych dla każdego obszaru objętego celem.

Każde pytanie jest opatrzone znacznikiem (0-1) wskazującym, czy pytanie jest wskaźnikiem obowiązkowym (1) czy nieobowiązkowym (0) dla danego poziomu dojrzałości.

Każde pytanie jest oznaczone numerem identyfikacyjnym, na który składają się:

- Numer celu;
- Poziom dojrzałości; oraz
- Numer pytania.

Na przykład pytanie ID 1.2.4 to czwarte pytanie dla poziomu dojrzałości 2 i celu strategicznego (I) „Opracowanie krajowych planów awaryjnych na wypadek cyberataku".

Należy pamiętać, że w całej ankiecie zakres pytań dotyczy szczebla krajowego, o ile nie wskazano inaczej. We wszystkich pytaniach zwrot „Państwo" dotyczy ogólnie państwa członkowskiego i nie odnosi się do osoby lub organu rządowego przeprowadzającego ocenę.

Definicje poszczególnych celów znajdują się w punkcie 2.2 – Wspólne cele określone w europejskich krajowych strategiach cyberbezpieczeństwa.

4.1.1 Grupa nr 1: Zarządzanie cyberbezpieczeństwem i normy w zakresie cyberbezpieczeństwa

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
1 – Opracowanie krajowych planów awaryjnych na wypadek cyberataku	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy przystąpili Państwo do prac nad planami awaryjnymi na wypadek cyberataku, np. określili ogólne cele, zakres lub zasady dla planów awaryjnych itp.?	1	Czy posiadają Państwo doktrynę/strategię krajową, w której cyberbezpieczeństwo zostało uwzględnione jako czynnik kryzysu (tj. protokół, politykę itp.)?	1	Czy posiadają Państwo ogólnokrajowy plan zarządzania na wypadek cyberkryzysu?	1	Czy są Państwo zadowoleni z liczby lub odsetka krytycznych sektorów uwzględnionych w krajowym planie awaryjnym na wypadek cyberataku?	1	Czy funkcjonuje u Państwa proces wyciągania wniosków z przeprowadzonych ćwiczeń w dziedzinie cyberbezpieczeństwa lub rzeczywistych kryzysów na szczeblu krajowym?	1
	2	Czy panuje powszechna zgoda co do tego, że cyberincydenty stanowią czynnik kryzysu, który może zagrażać bezpieczeństwu narodowemu?	0	Czy dysponują Państwo węzłem służącym do pozyskiwania informacji i przekazywania ich decydentom, tj. jakimikolwiek metodami, platformami lub lokalizacjami zapewniającymi wszystkim uczestnikom reagowania kryzysowego dostęp do tych samych informacji dotyczących cyberkryzysu w czasie rzeczywistym?	1	Czy posiadają Państwo specjalne ogólnokrajowe procedury na wypadek cyberkryzysu?	1	Czy organizują Państwo wystarczająco często działania (tj. ćwiczenia) związane z planowaniem awaryjnym na szczeblu krajowym na wypadek cyberataku?	1	Czy posiadają Państwo procedurę regularnego testowania planu krajowego?	1
	3	Czy przeprowadzono badania (techniczne, operacyjne, polityczne) w zakresie planowania awaryjnego na wypadek cyberataku?	0	Czy do nadzoru nad opracowywaniem i realizacją krajowych planów awaryjnych na wypadek cyberataku zostały zaangażowane odpowiednie zasoby?	1	Czy dysponują Państwo zespołem ds. komunikacji specjalnie przeszkolonym w zakresie reagowania na cyberkryzysy i informowania społeczeństwa?	1	Czy dysponują Państwo wystarczającą liczbą personelu zajmującego się planowaniem kryzysowym, analizowaniem zdobytych doświadczeń i wprowadzaniem zmian?	1	Czy dysponują Państwo odpowiednimi narzędziami i platformami do budowania orientacji sytuacyjnej?	1

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	4	-		Czy posiadają Państwo na szczeblu krajowym metodologię oceny cyberzagrożeń, która uwzględniałaby procedury oceny skutków?	0	Czy angażują Państwo wszystkie zainteresowane podmioty w kraju (bezpieczeństwo narodowe, obrona, ochrona ludności, egzekwowanie prawa, ministerstwa, władze itp.)?	1	Czy dysponują Państwo odpowiednią liczbą osób przeszkolonych w zakresie reagowania na cyberkryzysy na szczeblu krajowym?	1	Czy wykorzystują Państwo określony model dojrzałości do monitorowania i udoskonalania planu awaryjnego na wypadek cyberataku?	0
	5	-		-		Czy dysponują Państwo odpowiednimi obiektami i centrami sytuacyjnymi do zarządzania kryzysowego?	1	-		Czy dysponują Państwo zasobami wyspecjalizowanymi w przewidywaniu zagrożeń lub pracującymi nad zapewnieniem cyberbezpieczeństwa w przyszłości, które umożliwią opanowanie przyszłych kryzysów lub wyzwań?	0
	6	-		-		Czy w razie potrzeby współpracują Państwo z zagranicznymi zainteresowanymi stronami w UE?	0	-		-	
	7	-		-		Czy w razie potrzeby współpracują Państwo z zagranicznymi zainteresowanymi stronami spoza UE?	0	-		-	
2 – Określenie podstawowych środków bezpieczeństwa	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	1	Czy przeprowadzili Państwo badanie mające na celu określenie wymogów i luk dla organizacji **publicznych** w oparciu o międzynarodowe normy, *np.* ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS itp.?	1	Czy środki bezpieczeństwa zostały opracowane zgodnie z normami międzynarodowymi/krajowymi?	1	Czy podstawowe środki bezpieczeństwa są obowiązkowe?	1	Czy istnieje proces zapewniający częstą aktualizację podstawowych środków bezpieczeństwa?	1	Czy funkcjonuje u Państwa proces wzmacniania odporności ICT w przypadku, gdy środki nie umożliwiają opanowania incydentów?	1
	2	Czy przeprowadzili Państwo badanie mające na celu określenie wymogów i luk dla organizacji **prywatnych** w oparciu o międzynarodowe normy, np. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS itp.?	1	Czy przy określaniu podstawowych środków bezpieczeństwa przeprowadzane są konsultacje z sektorem prywatnym i innymi zainteresowanymi stronami?	1	Czy wdrażają Państwo horyzontalne środki bezpieczeństwa we wszystkich krytycznych sektorach?	1	Czy istnieje mechanizm monitorowania umożliwiający badanie upowszechniania się podstawowych środków bezpieczeństwa?	1	Czy oceniają Państwo istotność nowych norm opracowywanych w odpowiedzi na zmiany zachodzące w krajobrazie zagrożeń?	1
	3	-		-		Czy wdrażają Państwo sektorowe środki bezpieczeństwa we wszystkich krytycznych sektorach?	1	Czy istnieje organ krajowy, który kontroluje, czy podstawowe środki bezpieczeństwa są stosowane?	1	Czy posiadają lub wspierają Państwo krajowy proces skoordynowanego ujawniania luk w zabezpieczeniach (CVD)?	1
	4	-				Czy podstawowe środki bezpieczeństwa są zgodne z odpowiednimi systemami certyfikacji?	1	Czy istnieje procedura wskazywania organizacji nieprzestrzegających wymogów w określonym czasie?	1	-	
	5	-		-		Czy istnieje proces samooceny ryzyka dla podstawowych środków bezpieczeństwa?	1	Czy istnieje proces audytu weryfikujący prawidłowe stosowanie środków bezpieczeństwa?	1	-	

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
2 – Określenie podstawowych środków bezpieczeństwa	6	-		-		Czy dokonują Państwo weryfikacji obowiązkowych podstawowych środków bezpieczeństwa w procesie udzielania zamówień przez organy rządowe?	0	Czy określają Państwo bezpieczne normy w zakresie opracowywania krytycznych produktów IT/OT (sprzętu medycznego, pojazdów podłączonych do sieci (connected) i autonomicznych, profesjonalnych urządzeń radiowych, maszyn dla przemysłu ciężkiego itp.) lub aktywnie zachęcają do ich przyjmowania?	0	-	
3 – Ochrona tożsamości elektronicznej i budowanie zaufania do cyfrowych usług publicznych	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy przeprowadzili Państwo badania lub analizy luk w celu określenia potrzeb w zakresie zapewnienia cyfrowych usług publicznych dla obywateli i przedsiębiorstw?	1	Czy przeprowadzają Państwo analizy ryzyka w celu określenia profilu ryzyka aktywów lub usług przed przeniesieniem ich do chmury obliczeniowej lub w celu uruchomienia jakichkolwiek projektów w zakresie transformacji cyfrowej?	1	Czy promują Państwo stosowanie metod uwzględniania ochrony prywatności już w fazie projektowania we wszystkich projektach z zakresu e-administracji?	1	Czy gromadzą Państwo wskaźniki dotyczące cyberincydentów związanych z naruszeniem bezpieczeństwa cyfrowych usług publicznych?	1	Czy uczestniczą Państwo w pracach europejskich grup roboczych nad utrzymaniem norm lub opracowaniem nowych wymogów dotyczących elektronicznych usług zaufania (podpisy elektroniczne, pieczęcie elektroniczne, usługi rejestrowanych doręczeń elektronicznych, oznaczanie czasu, uwierzytelnianie witryn internetowych), np. ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU itp.?	1
	2	-		Czy posiadają Państwo strategię tworzenia lub promowania bezpiecznych krajowych systemów identyfikacji elektronicznej (eID) dla obywateli i przedsiębiorstw?	1	Czy umożliwiają Państwo zainteresowanym stronom z sektora prywatnego udział w projektowaniu i świadczeniu bezpiecznych cyfrowych usług publicznych?	1	Czy wdrożyli Państwo wzajemne uznawanie środków identyfikacji elektronicznej z innymi państwami członkowskimi?	1	Czy uczestniczą Państwo aktywnie we wzajemnych ocenach w ramach zgłaszania systemów identyfikacji elektronicznej do Komisji Europejskiej?	1

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
3 – Ochrona tożsamości elektronicznej i budowanie zaufania do cyfrowych usług publicznych	3	-		Czy posiadają Państwo strategię tworzenia lub promowania bezpiecznych krajowych elektronicznych usług zaufania (podpisy elektroniczne, pieczęcie elektroniczne, usługi rejestrowanych doręczeń elektronicznych, oznaczanie czasu, uwierzytelnianie witryn internetowych) dla obywateli i przedsiębiorstw?	1	Czy wdrażają Państwo minimalne wymogi bezpieczeństwa dla wszystkich cyfrowych usług publicznych?	1	-		-	
	4	-		Czy posiadają Państwo strategię dotyczącą rządowej chmury obliczeniowej (strategia chmury obliczeniowej skierowana do rządu i organów publicznych, takich jak ministerstwa, agencje rządowe i administracja publiczna itp.), która uwzględniałaby implikacje dla bezpieczeństwa?	0	Czy obywatele i przedsiębiorstwa mają dostęp do jakichkolwiek systemów identyfikacji elektronicznej o średnim lub wysokim poziomie bezpieczeństwa w rozumieniu załącznika do rozporządzenia (UE) nr 910/2014 (eIDAS)?	1	-		-	
	5	-		-		Czy posiadają Państwo cyfrowe usługi publiczne wymagające stosowania systemów identyfikacji elektronicznej o średnim lub wysokim poziomie bezpieczeństwa w rozumieniu załącznika do rozporządzenia (UE) nr 910/2014 (eIDAS)?	1	-		-	
	6	-		-		Czy mają Państwo dostawców usług zaufania dla obywateli i przedsiębiorstw (podpisy elektroniczne, pieczęcie elektroniczne, usługi rejestrowanych doręczeń elektronicznych, oznaczanie czasu, uwierzytelnianie witryn internetowych)?	1	-		-	
	7	-		-		Czy wspierają Państwo przyjmowanie podstawowych środków bezpieczeństwa w odniesieniu do wszystkich modeli wdrażania chmury obliczeniowej (np. prywatnych, publicznych, hybrydowych, IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Grupa nr 2: Budowanie zdolności i zwiększanie świadomości

Cel NCSS	Lp.	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
4 – Zapewnienie możliwości reagowania na incydenty	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy dysponują Państwo nieformalnymi możliwościami reagowania na incydenty zarządzanymi w ramach sektora publicznego, prywatnego lub obu tych sektorów?	1	Czy posiadają Państwo co najmniej jeden oficjalny krajowy zespół reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)?	1	Czy dysponują Państwo możliwościami reagowania na incydenty w sektorach, o których mowa w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji?	1	Czy zdefiniowali Państwo i wspierają Państwo ujednolicone praktyki w zakresie procedur reagowania na incydenty i systemów klasyfikacji incydentów?	1	Czy posiadają Państwo jakiekolwiek mechanizmy wczesnego wykrywania podatności typu zero-day, ich identyfikacji, zapobiegania im, reagowania na nie oraz ich ograniczania?	1
	2	-		Czy Państwa krajowe zespoły CSIRT mają jasno określony zakres interwencji, np. w zależności od sektora stanowiącego cel, rodzajów incydentów, skutków?	1	Czy w Państwa kraju istnieje mechanizm współpracy z zespołem CSIRT w zakresie reagowania na incydenty?	1	Czy przeprowadzają Państwo ocenę możliwości reagowania na incydenty, aby mieć pewność, że dysponują Państwo odpowiednimi zasobami i kwalifikacjami do wykonywania zadań określonych w pkt 2 załącznika I do dyrektywy w sprawie bezpieczeństwa sieci i informacji?	1	-	

Cel NCSS	Lp.	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
4 – Zapewnienie możliwości reagowania na incydenty	3	-		Czy Państwa krajowe zespoły CSIRT mają jasno określone relacje z pozostałymi krajowymi zainteresowanymi stronami w odniesieniu do krajowego krajobrazu cyberbezpieczeństwa i praktyki reagowania na incydenty (np. z organami ścigania, wojskiem, dostawcami usług internetowych, narodowym centrum cyberbezpieczeństwa)?	0	Czy Państwa krajowe zespoły CSIRT mają możliwości reagowania na incydenty przewidziane w załączniku I do dyrektywy w sprawie bezpieczeństwa sieci i informacji? Tj. dostępność, bezpieczeństwo fizyczne, ciągłość działania, współpraca międzynarodowa, monitorowanie incydentów, przekazywanie wczesnych ostrzeżeń i ogłaszania alarmów, reagowanie na incydenty, analiza ryzyka i orientacji sytuacyjnej, współpraca z sektorem prywatnym, standardowe praktyki itp.	1	-		-	
	4	-				Czy istnieje mechanizm współpracy z pozostałymi sąsiednimi krajami w związku z incydentami?	1	-		-	
	5	-		-		Czy określili Państwo w sposób formalny jasne zasady i procedury postępowania w przypadku incydentu?	1	-		-	
	6	-		-		Czy Państwa krajowy zespół lub krajowe zespoły CSIRT uczestniczą w ćwiczeniach w dziedzinie bezpieczeństwa cybernetycznego na szczeblu krajowym oraz międzynarodowym?	1	-		-	
	7	-		-		Czy Państwa krajowy zespół lub krajowe zespoły CSIRT należą do FIRST (Forum Zespołów Reagowania na Incydenty i Bezpieczeństwa)?	0	-		-	
5 – Zwiększanie świadomości użytkowników	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1

Cel NCSS	Lp.	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
5 – Zwiększanie świadomości użytkowników	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy rząd, sektor prywatny lub ogół użytkowników choćby w minimalnym stopniu dostrzegają potrzebę zwiększania świadomości w zakresie cyberbezpieczeństwa i prywatności?	1	Czy określili Państwo konkretną grupę docelową, w której warto zwiększyć świadomość użytkowników, np. ogół użytkowników, osoby młode, użytkownicy biznesowe (których z kolei można podzielić na MŚP, OUK, DUC itp.)?	1	Czy opracowali Państwo plany/strategię komunikacji na potrzeby kampanii?	1	Czy opracowują Państwo mierniki do oceny swojej kampanii na etapie planowania?	1	Czy dysponują Państwo mechanizmami, dzięki którym kampanie informacyjne są stale aktualne w odniesieniu do postępu technicznego, zmian w krajobrazie zagrożeń, regulacji prawnych i krajowych przepisów dotyczących bezpieczeństwa?	1
	2	Czy agencje publiczne prowadzą doraźne kampanie informacyjne na temat cyberbezpieczeństwa w ramach swoich organizacji, np. w następstwie cyberincydentu?	0	Czy sporządzają Państwo plan projektu mający na celu zwiększanie świadomości zagadnień bezpieczeństwa informacji i prywatności?	1	Czy istnieje u Państwa proces opracowywania materiałów na szczeblu rządowym?	1	Czy oceniają Państwo swoje kampanie po ich zrealizowaniu?	1	Czy przeprowadzają Państwo okresową ocenę lub badanie w celu pomiaru zmiany postaw lub zachowań w stosunku do spraw cyberbezpieczeństwa i prywatności w sektorze prywatnym i publicznym?	1
	3	Czy agencje publiczne prowadzą doraźne kampanie informacyjne na temat cyberbezpieczeństwa skierowane do ogółu społeczeństwa, np. w następstwie cyberincydentu?	0	Czy dysponują Państwo dostępnymi i łatwymi do odszukania materiałami (np. jeden portal internetowy, pakiety informacyjne) dla wszystkich użytkowników, którzy starają się dokształcać w zakresie cyberbezpieczeństwa i prywatności?	1	Czy dysponują Państwo jakimikolwiek mechanizmami służącymi do określania obszarów, w których warto zwiększać świadomość (np. krajobraz zagrożeń ENISA, krajobrazy krajowe, krajobrazy międzynarodowe, informacje zwrotne od krajowych ośrodków ds. walki z cyberprzestępczością itp.)?	1	Czy posiadają Państwo jakiekolwiek mechanizmy służące do wybierania właściwych środków przekazu lub kanałów komunikacji w zależności od grupy docelowej w celu uzyskania jak największego zasięgu i zainteresowania, np. różnego rodzaju media cyfrowe, broszury, e-maile, materiały dydaktyczne, plakaty w uczęszczanych miejscach, telewizja, radio itp.?	1	Czy konsultują się Państwo z ekspertami w dziedzinie behawiorystyki w celu dostosowywania kampanii do odbiorców docelowych?	1
	4	-		-		Czy inicjują Państwo współpracę między zainteresowanymi stronami a ekspertami i zespołami ds. komunikacji w celu opracowywania materiałów?	1			-	

Cel NCSS	Lp.	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	5	-		-		Czy umożliwiają Państwo udział sektora prywatnego w działaniach informacyjnych i angażują go w takie działania, aby promować i rozpowszechniać przekaz wśród szerszego grona odbiorców?	1	-		-	
	6	-		-		Czy przygotowują Państwo specjalne inicjatywy informacyjne skierowane do kadry zarządzającej w sektorze publicznym, prywatnym, akademickim lub społeczeństwa obywatelskiego?	1	-		-	
	7	-		-		Czy uczestniczą Państwo w kampaniach Europejskiego Miesiąca Cyberbezpieczeństwa (ESCM) organizowanych przez ENISA?	0	-		-	
6 – Organizacja ćwiczeń w zakresie cyberbezpieczeństwa	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
6 – Organizacja ćwiczeń w zakresie cyberbezpieczeństwa	1	Czy przeprowadzają Państwo ćwiczenia kryzysowe w innych (niż cyberbezpieczeństwo) sektorach na szczeblu krajowym lub ogólnoeuropejskim?	1	Czy posiadają Państwo program ćwiczeń w zakresie cyberbezpieczeństwa na szczeblu krajowym?	1	Czy angażują Państwo wszystkie właściwe organy administracji publicznej (nawet jeśli scenariusz dotyczy konkretnego sektora)?	1	Czy sporządzają Państwo raporty z wykonania działań/raporty ewaluacyjne?	1	Czy mają Państwo możliwość analizowania doświadczeń zdobytych w dziedzinie cyberbezpieczeństwa (procesy sprawozdawcze, analiza, łagodzenie skutków)?	1

Cel NCSS	Lp.	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	2	Czy przydzielili Państwo zasoby do opracowywania i planowania ćwiczeń zarządzania kryzysowego?	1	Czy przeprowadzają Państwo lub priorytetowo traktują ćwiczenia zarządzania kryzysowego dotyczące podstawowych funkcji społecznych i infrastruktury krytycznej?	1	Czy angażują Państwo sektor prywatny w planowanie i realizację ćwiczeń?	1	Czy testują Państwo ogólnokrajowe plany i procedury?	1	Czy posiadają Państwo ugruntowany proces wyciągania wniosków?	1
	3	-		Czy wskazali Państwo jednostkę koordynującą do nadzorowania opracowywania i planowania ćwiczeń w dziedzinie cyberbezpieczeństwa (agencja publiczna, firma doradcza itp.)?	0	Czy organizują Państwo ćwiczenia sektorowe na szczeblu krajowym lub międzynarodowym?	1	Czy uczestniczą Państwo w ćwiczeniach w dziedzinie cyberbezpieczeństwa na szczeblu ogólnoeuropejskim?	1	Czy modyfikują Państwo scenariusze ćwiczeń w związku z zachodzącymi zmianami (postęp techniczny, globalne konflikty, krajobraz zagrożeń itp.)?	1
	4	-		-		Czy organizują Państwo ćwiczenia we wszystkich sektorach krytycznych wymienionych w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji?	1	-		Czy ujednolicają Państwo swoje procedury zarządzania kryzysowego z innymi państwami członkowskimi w celu zapewnienia skutecznego ogólnoeuropejskiego zarządzania kryzysowego?	1
	5	-		-		Czy organizują Państwo międzysektorowe lub wielosektorowe ćwiczenia w dziedzinie cyberbezpieczeństwa?	1	-		Czy posiadają Państwo mechanizm umożliwiający szybkie modyfikowanie strategii, planów i procedur w oparciu o doświadczenia zdobyte podczas ćwiczeń?	0
	6	-		-		Czy organizują Państwo ćwiczenia w dziedzinie cyberbezpieczeństwa właściwe dla różnych szczebli (szczebel techniczny i operacyjny, szczebel proceduralny, szczebel decyzyjny, szczebel polityczny itp.)?	0	-		-	
7 – Udoskonalanie programów szkoleniowych i edukacyjnych	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		

Cel NCSS	Lp.	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy rozważają Państwo możliwość opracowywania programów szkoleniowych i edukacyjnych w dziedzinie cyberbezpieczeństwa?	1	Czy organizują Państwo kursy poświęcone cyberbezpieczeństwu?	1	Czy Państwa kraj uwzględnia kulturę cyberbezpieczeństwa na wczesnym etapie kształcenia uczniów? Na przykład czy opowiadają się Państwo za poruszaniem tematyki cyberbezpieczeństwa w gimnazjach i szkołach średnich?	1	Czy nakłaniają Państwo pracowników sektora prywatnego i publicznego do uzyskiwania akredytacji lub certyfikatów?	1	Czy wprowadzili Państwo mechanizmy, dzięki którym szkolenia i programy edukacyjne są stale aktualne w odniesieniu do bieżących i nowo pojawiających się zmian technologicznych, zmian w krajobrazie zagrożeń, regulacji prawnych i krajowych przepisów dotyczących bezpieczeństwa?	1
	2	-		Czy uczelnie wyższe w Państwa kraju oferują studia doktoranckie w dziedzinie cyberbezpieczeństwa jako niezależną dyscyplinę, a nie jako przedmiot realizowany w ramach informatyki?	1	Czy posiadają Państwo krajowe laboratoria badawcze i instytucje oświatowe specjalizujące się w cyberbezpieczeństwie?	1	Czy w Państwa kraju opracowano programy szkoleń lub mentoringu w dziedzinie cyberbezpieczeństwa w celu wspierania krajowych start-upów i MŚP?	1	Czy zakładają Państwo akademickie centra doskonałości w dziedzinie cyberbezpieczeństwa pełniące funkcje ośrodków badań naukowych i kształcenia?	1
	3	-		Czy zamierzają Państwo szkolić pedagogów, niezależnie od ich specjalizacji, w zakresie bezpieczeństwa informacji i prywatności, np. bezpieczeństwa w internecie, ochrony danych osobowych, cyberprzemocy?	1	Czy zachęcają Państwo do organizowania specjalnych kursów lub finansują specjalne kursy z zakresu cyberbezpieczeństwa i programy szkoleń dla pracowników agencji pośrednictwa pracy w państwach członkowskich?	1	Czy aktywnie wspierają Państwo wprowadzanie kursów z zakresu bezpieczeństwa informacji w szkolnictwie wyższym, nie tylko dla studentów informatyki, ale również dla innych specjalności zawodowych, np. kursów dostosowanych do potrzeb danego zawodu?	1	Czy w ważnych rozmowach dotyczących edukacji i badań w dziedzinie cyberbezpieczeństwa na szczeblu międzynarodowym uczestniczą instytucje akademickie?	0
	4	-		-		Czy posiadają Państwo kursy lub specjalistyczny program nauczania z zakresu cyberbezpieczeństwa na poziomach 5-8 ERK (europejskich ram kwalifikacji)?	1	Czy regularnie przeprowadzają Państwo ocenę luki kompetencyjnej (braku pracowników wykwalifikowanych w zakresie cyberbezpieczeństwa) w dziedzinie bezpieczeństwa informacji?	1	-	
	5	-		-		Czy zachęcają Państwo do podejmowania inicjatyw lub wspierają inicjatywy mające na celu włączenie kursów z zakresu bezpieczeństwa w internecie do kształcenia na poziomie podstawowym i średnim?	1	Czy wspierają Państwo tworzenie sieci kontaktów i wymianę informacji między placówkami naukowymi, zarówno na szczeblu krajowym, jak i międzynarodowym?	1		

Cel NCSS	Lp.	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
7 - Udoskonalanie programów szkoleniowych i edukacyjnych	6	-		-		Czy finansują lub oferują Państwo bezpłatnie szkolenia dla obywateli z zakresu cyberbezpieczeństwa?	0	Czy w jakikolwiek sposób angażują Państwo sektor prywatny w inicjatywy edukacyjne w zakresie cyberbezpieczeństwa, np. projektowanie i realizację kursów, staże, praktyki itp.?	1	-	
	7	-		-		Czy organizują Państwo doroczne imprezy związane z bezpieczeństwem informacji (np. turnieje hakerskie lub hakatony)?	0	Czy wdrażają Państwo mechanizmy finansowania zachęcające do uzyskiwania stopni naukowych w dziedzinie cyberbezpieczeństwa, np. stypendia, gwarantowane przygotowanie zawodowe/praktyki, gwarantowane miejsca pracy w konkretnej branży lub stanowiska w sektorze publicznym?	0	-	
8 – Wspieranie badań i rozwoju	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy przeprowadzili Państwo badania lub analizy mające na celu określenie priorytetów w zakresie badań i rozwoju w dziedzinie cyberbezpieczeństwa?	1	Czy posiadają Państwo proces wskazywania priorytetów w zakresie badań i rozwoju (np. nowych zagadnień dotyczących zapobiegania nowym rodzajom cyberataków, ochrony przed nimi, wykrywania ich i dostosowywania się do nich)?	1	Czy istnieje plan powiązania przedsięwzięć badawczo-rozwojowych z gospodarką realną?	1	Czy przedsięwzięcia w zakresie cyberbezpieczeństwa w dziedzinie badań i rozwoju są skoordynowane z odpowiednimi celami strategicznymi, takimi jak JRC, „Horyzont 2020”, „Cyfrowa Europa”, europejska strategia bezpieczeństwa cybernetycznego?	1	Czy prowadzą Państwo współpracę na szczeblu krajowym z jakimikolwiek międzynarodowymi inicjatywami w zakresie badań naukowych i innowacji związanymi z cyberbezpieczeństwem?	1

Cel NCSS	Lp.	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	2	-		Czy sektor prywatny uczestniczy w ustalaniu priorytetów w zakresie badań i rozwoju?	1	Czy funkcjonują u Państwa jakiekolwiek krajowe projekty związane z cyberbezpieczeństwem?	1	Czy istnieje system oceny inicjatyw badawczo-rozwojowych?	1	Czy priorytety w zakresie badań i rozwoju są skoordynowane z obowiązującymi lub planowanymi do wprowadzenia przepisami (na szczeblu krajowym)?	1
8 – Wspieranie badań i rozwoju	3	-		Czy w ustalaniu priorytetów w zakresie badań i rozwoju uczestniczy środowisko akademickie?	1	Czy dysponują Państwo lokalnymi/regionalnymi ekosystemami start-upów i innymi kanałami tworzenia sieci współpracy (np. parkami technologicznymi, klastrami innowacyjnymi, wydarzeniami/platformami służącymi tworzeniu sieci kontaktów) umożliwiającymi wspieranie innowacji (w tym dla start-upów z branży cyberbezpieczeństwa)?	1	Czy zawarli Państwo jakiekolwiek umowy o współpracy z uczelniami wyższymi i innymi ośrodkami badawczymi?	1	Czy uczestniczą Państwo w ważnych rozmowach nad jednym lub wieloma przełomowymi zagadnieniami w zakresie badań i rozwoju na szczeblu międzynarodowym?	0
	4	-		Czy istnieją jakieś krajowe inicjatywy badawczo-rozwojowe związane z cyberbezpieczeństwem?	0	Czy w środowisku akademickim i sektorze prywatnym inwestuje się w programy badawczo-rozwojowe w dziedzinie cyberbezpieczeństwa?	1	Czy istnieje uznany organ instytucjonalny nadzorujący działalność badawczo-rozwojową w dziedzinie cyberbezpieczeństwa?	0	-	
	5	-		-		Czy posiadają Państwo katedry badań przemysłowych na uczelniach wyższych umożliwiające dostosowywanie tematyki badań do potrzeb rynku?	1	-		-	
	6	-		-		Czy posiadają Państwo specjalne programy finansowania badań i rozwoju w dziedzinie cyberbezpieczeństwa?	0	-		-	
9 – Zachęcanie sektora prywatnego do inwestowania w środki bezpieczeństwa	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		

Cel NCSS	Lp.	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy istnieje polityka przemysłowa lub wola polityczna w zakresie wspierania rozwoju sektora cyberbezpieczeństwa?	1	Czy w opracowywaniu zachęt uczestniczy sektor prywatny?	1	Czy istnieją zachęty ekonomiczne/regulacyjne lub inne rodzaje zachęt do inwestowania w cyberbezpieczeństwo?	1	Czy jakiekolwiek podmioty prywatne reagują na zachęty, inwestując w środki bezpieczeństwa, np. inwestorzy specjalizujący się w cyberbezpieczeństwie i inwestorzy niewyspecjalizowani?	1	Czy zagadnienia w dziedzinie cyberbezpieczeństwa, których dotyczą zachęty, są przez Państwa wybierane na podstawie zmian zachodzących w zakresie zagrożeń?	1
9 – Zachęcanie sektora prywatnego do inwestowania w środki bezpieczeństwa	2	-		Czy wskazali Państwo konkretne zagadnienia cyberbezpieczeństwa, które powinny być rozwijane, jak np. kryptografia, prywatność, nowa forma uwierzytelniania, AI na potrzeby cyberbezpieczeństwa itp.?	0	Czy udzielają Państwo wsparcia (np. zachęty podatkowe) dla start-upów i MŚP w sektorze cyberbezpieczeństwa?	1	Czy stosują Państwo zachęty dla sektora prywatnego, aby skłonić go do skupienia się na bezpieczeństwie najnowocześniejszych technologii, np. 5G, sztucznej inteligencji, internetu rzeczy (IoT), informatyki kwantowej itp.?	1	-	
	3	-		-		Czy stosują Państwo zachęty podatkowe lub inne zachęty finansowe dla inwestorów z sektora prywatnego w start-upach w sektorze cyberbezpieczeństwa?	1	-		-	
	4	-		-		Czy ułatwiają Państwo start-upom i MŚP w sektorze cyberbezpieczeństwa dostęp do procedur zamówień publicznych?	0	-		-	
	5	-		-		Czy przewidziano środki w budżecie na zachęty dla sektora prywatnego?	0	-		-	
10 – Poprawa cyberbezpieczeństwa w łańcuchu dostaw	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		

Cel NCSS	Lp.	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
10 – Poprawa cyberbezpieczeństwa w łańcuchu dostaw	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy przeprowadzili Państwo badanie dotyczące dobrych praktyk w zakresie bezpieczeństwa dla zarządzania łańcuchem dostaw stosowanych w zamówieniach publicznych w różnych segmentach branżowych lub w sektorze publicznym?	1	Czy przeprowadzają Państwo oceny cyberbezpieczeństwa na wszystkich etapach łańcucha dostaw usług i produktów ICT w sektorach krytycznych (wskazanych w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji (2016/1148))?	1	Czy korzystają Państwo z systemu certyfikacji bezpieczeństwa produktów i usług opartych na ICT, np. SOG-IS MRA w Europie (umowa o wzajemnym uznaniu przyjęta przez grupę wyższych urzędników ds. bezpieczeństwa systemów informatycznych), porozumienie w sprawie uznawania Common Criteria (CCRA), inicjatywy krajowe, inicjatywy sektorowe itp.?	1	Czy posiadają Państwo procedurę aktualizacji oceny cyberbezpieczeństwa łańcucha dostaw usług i produktów ICT w sektorach krytycznych (wskazanych w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji (2016/1148))?	1	Czy posiadają Państwo mechanizmy umożliwiające wykrywanie wczesnych sygnałów naruszenia bezpieczeństwa w kluczowych elementach łańcucha dostaw, np. mechanizmy kontroli bezpieczeństwa na poziomie dostawców usług internetowych, mechanizmy wykrywania zagrożeń w najważniejszych elementach infrastruktury itp.?	1
	2	-		Czy w polityce zamówień publicznych administracji publicznej stosują Państwo normy zapewniające spełnianie podstawowych wymogów w zakresie bezpieczeństwa informacji przez dostawców produktów lub usług ICT, np. ISO/IEC 27001 i 27002, ISO/IEC 27036 itp.?	1	Czy wspierają Państwo czynnie stosowanie najlepszych praktyk w zakresie bezpieczeństwa i ochrony prywatności już w fazie projektowania przy opracowywaniu produktów i usług ICT, np. bezpiecznego cyklu życia oprogramowania (SSDLC), cyklu życia internetu rzeczy (IoT lifecycle)?	1	Czy posiadają Państwo procedurę identyfikacji słabych ogniw cyberbezpieczeństwa w łańcuchu dostaw w sektorach krytycznych (wskazanych w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji (2016/1148))?	1	-	
	3	-		-		Czy opracowują Państwo i udostępniają centralne katalogi zawierające rozszerzone informacje na temat istniejących norm w zakresie bezpieczeństwa informacji i prywatności, które są skalowalne dla MŚP i mogą być przez nie stosowane?	1	Czy dysponują Państwo mechanizmami zapewniającymi, aby produkty i usługi ICT, które mają kluczowe znaczenie dla OUK, były odporne na cyberzagrożenia (tj. cechowały się zdolnością do utrzymania dostępności i odpornością na cyberincydenty), np. poprzez testowanie, przeprowadzanie regularnych ocen, wykrywanie elementów, których bezpieczeństwo zostało naruszone itp.?	1	-	

Cel NCSS	Lp.	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	4	-				Czy uczestniczą Państwo czynnie w opracowywaniu unijnych ram certyfikacji cyfrowych produktów, usług i procesów ICT przewidzianych w unijnym akcie o cyberbezpieczeństwie (rozporządzenie (UE) 2019/881), np. w pracach Europejskiej Grupy ds. Certyfikacji Bezpieczeństwa Cybernetycznego (ECCG), promowaniu norm i procedur technicznych dotyczących bezpieczeństwa produktów/usług ICT?	0	Czy wspierają Państwo rozwój systemów certyfikacji przeznaczonych dla MŚP w celu zwiększania bezpieczeństwa informacji i przyspieszenia przyjmowania norm w zakresie prywatności?	0	-	
	5	-		-		Czy stosują Państwo jakieś zachęty dla MŚP do przyjmowania norm w zakresie bezpieczeństwa i prywatności?	0	Czy wprowadzili Państwo środki zachęcające duże przedsiębiorstwa do zwiększania cyberbezpieczeństwa małych przedsiębiorstw należących do ich łańcuchów, np. ośrodki cyberbezpieczeństwa, szkolenia i kampanie informacyjne itp.?	0	-	
	6	-		-		Czy zachęcają Państwo dostawców oprogramowania do wspierania MŚP poprzez zapewnienie bezpiecznych domyślnych konfiguracji w produktach przeznaczonych dla małych organizacji?	0	-		-	

4.1.3 Grupa nr 3: Aspekty prawne i regulacyjne

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
11 – Ochrona krytycznej infrastruktury teleinformatycznej, OUK i DUC	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy panuje powszechna zgoda co do tego, że operatorzy KITI przyczyniają się do zapewnienia bezpieczeństwa narodowego?	1	Czy posiadają Państwo metodologię określania usług kluczowych?	1	Czy wdrożyli Państwo dyrektywę w sprawie bezpieczeństwa sieci i informacji (2016/1148)?	1	Czy posiadają Państwo procedurę aktualizacji rejestru ryzyka?	1	Czy sporządzają i aktualizują Państwo przeglądy zagrożeń (threat landscape reports)?	1
	2	-		Czy posiadają Państwo metodologię identyfikacji KITI?	1	Czy wdrożyli Państwo dyrektywę ECI (2008/114) w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony?	1	Czy posiadają Państwo inne mechanizmy służące do weryfikowania, czy środki techniczne i organizacyjne wprowadzane przez OUK umożliwiają prawidłowe zarządzanie ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, np. regularne audyty cyberbezpieczeństwa, krajowe ramy wdrażania standardowych środków, narzędzia techniczne zapewniane przez rząd, takie jak mechanizmy wykrywania lub weryfikacja konfiguracji dla poszczególnych systemów?	1	Czy w zależności od zmian zachodzących w krajobrazie zagrożeń są Państwo w stanie uwzględnić nowy sektor w swoim planie działania w zakresie ochrony krytycznej infrastruktury teleinformatycznej?	1
	3	-		Czy posiadają Państwo metodologię identyfikacji OUK?	1	Czy posiadają Państwo krajowy rejestr OUK zidentyfikowanych w poszczególnych krytycznych sektorach?	1	Czy co najmniej raz na dwa lata przeprowadzają Państwo przegląd wykazu zidentyfikowanych OUK, a następnie go uaktualniają?	1	Czy w zależności od zmian zachodzących w krajobrazie zagrożeń są Państwo w stanie uwzględniać nowe wymagania w swoim planie działania w zakresie ochrony krytycznej infrastruktury teleinformatycznej?	1

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
11 – Ochrona krytycznej infrastruktury teleinformatycznej, OUK i DUC	4	-		Czy posiadają Państwo metodologię identyfikacji dostawców usług cyfrowych?	1	Czy posiadają Państwo krajowy rejestr zidentyfikowanych dostawców usług cyfrowych?	1	Czy posiadają Państwo inne mechanizmy służące do weryfikowania, czy środki techniczne i organizacyjne wprowadzane przez dostawców usług cyfrowych umożliwiają prawidłowe zarządzanie ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, np. regularne audyty cyberbezpieczeństwa, krajowe ramy wdrażania standardowych środków, narzędzia techniczne zapewniane przez rząd, takie jak mechanizmy wykrywania lub weryfikacja konfiguracji dla poszczególnych systemów?	1	-	
	5	-		Czy posiadają Państwo co najmniej jeden krajowy organ sprawujący nadzór nad ochroną krytycznej infrastruktury teleinformatycznej oraz bezpieczeństwem sieci i systemów informatycznych, np. zgodnie z wymogami dyrektywy w sprawie bezpieczeństwa sieci i informacji (2016/1148)?	1	Czy posiadają Państwo krajowy rejestr ryzyka zawierający zidentyfikowane lub znane zagrożenia?	1	Czy co najmniej raz na dwa lata przeprowadzają Państwo przegląd wykazu zidentyfikowanych dostawców usług cyfrowych, a następnie go uaktualniają?	1	-	
	6	-		Czy opracowują Państwo sektorowe plany ochrony, np. z uwzględnieniem podstawowych środków w zakresie cyberbezpieczeństwa (obowiązkowe lub w formie wytycznych)?	0	Czy posiadają Państwo metodykę mapowania zależności w obrębie KITI?	1	Czy korzystają Państwo z systemu certyfikacji bezpieczeństwa (krajowego lub międzynarodowego), który pomagałby OUK i dostawcom usług cyfrowych w identyfikacji bezpiecznych produktów ICT, np. SOG-IS MRA w Europie, inicjatywy krajowe itp.?	1	-	

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
11 – Ochrona krytycznej infrastruktury teleinformatycznej, OUK i DUC	7	-		-		Czy wprowadzają Państwo praktyki zarządzania ryzykiem w celu identyfikacji i kwantyfikacji ryzyka związanego z KITI oraz zarządzania nim na szczeblu krajowym?	1	Czy stosują Państwo system certyfikacji bezpieczeństwa lub procedurę kwalifikacyjną do oceny dostawców usług pracujących z OUK, np. dostawców usług w zakresie wykrywania incydentów, reagowania na incydenty, audytu cyberbezpieczeństwa, usług przetwarzania w chmurze, kart chipowych itp.?	1	-	
	8	-		-		Czy biorą Państwo udział w procesie konsultacji w celu określania zależności transgranicznych?	1	Czy dysponują Państwo mechanizmami służącymi do weryfikacji stopnia przestrzegania wymogów przez OUK i dostawców usług cyfrowych w odniesieniu do podstawowych środków w zakresie cyberbezpieczeństwa?	0	-	
	9					Czy wyznaczyli Państwo jeden punkt kontaktowy odpowiedzialny za koordynację kwestii związanych z bezpieczeństwem sieci i systemów informatycznych oraz współpracę transgraniczną na poziomie Unii?	1	Czy posiadają Państwo jakiekolwiek rozwiązania zapewniające ciągłość usług świadczonych przez krytyczną infrastrukturę teleinformatyczną, np. przewidywanie sytuacji kryzysowych, procedury odbudowy krytycznych systemów informacyjnych, ciągłość działania bez technologii informacyjnych, procedury tworzenia kopii zapasowych z fizyczną izolacją sieci (tzw. air gap) itp.?	0		
	10					Czy określają Państwo podstawowe środki cyberbezpieczeństwa (obowiązkowe lub wytyczne) dla dostawców usług cyfrowych i wszystkich sektorów wskazanych w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji (2016/1148)?	1				
	11	-		-		Czy zapewniają Państwo narzędzia lub metody wykrywania cyberincydentów?	1	-		-	

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
12 – Walka z cyberprzestępczością	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy przeprowadzili Państwo badanie w celu określenia wymogów w zakresie egzekwowania prawa (podstawa prawna, zasoby, umiejętności itp.), aby móc skutecznie zwalczać cyberprzestępczość?	1	Czy Państwa krajowe ramy prawne są w pełni zgodne z odpowiednimi ramami prawnymi UE, w tym z dyrektywą 2013/40/UE dotyczącą ataków na systemy informatyczne, np. w zakresie niezgodnego z prawem dostępu do systemów informatycznych, niezgodnej z prawem ingerencji w systemy, niezgodnej z prawem ingerencji w dane, niezgodnego z prawem przechwytywania, narzędzi do popełniania przestępstw itp.?	1	Czy dysponują Państwo jednostkami specjalizującymi się w walce z cyberprzestępczością w prokuraturach?	1	Czy gromadzą Państwo dane statystyczne zgodnie z przepisami art. 14 ust. 1 dyrektywy 2013/40/UE (dyrektywy dotyczącej ataków na systemy informatyczne)?	1	Czy organizują Państwo międzyinstytucjonalne szkolenia lub warsztaty szkoleniowe dla organów ścigania, sędziów, prokuratorów oraz krajowych/rządowych zespołów CSIRT na poziomie krajowym lub wielostronnym?	1
	2	Czy przeprowadzili Państwo badanie w celu określenia wymogów dla prokuratorów i sędziów (podstawa prawna, zasoby, umiejętności itp.), aby mogli skutecznie zwalczać cyberprzestępczość?	1	Czy obowiązują u Państwa przepisy prawne dotyczące kradzieży tożsamości w internecie i kradzieży danych osobowych?	1	Czy dysponują Państwo specjalnym budżetem przeznaczonym dla jednostek zwalczających cyberprzestępczość?	1	Czy gromadzą Państwo odrębne dane statystyczne dotyczące cyberprzestępczości, np. statystyki operacyjne, statystyki dotyczące trendów w cyberprzestępczości, statystyki dotyczące dochodów z cyberprzestępczości i powodowanych przez nią szkód?	1	Czy uczestniczą Państwo w skoordynowanych działaniach na szczeblu międzynarodowym mających na celu utrudnianie działalności przestępczej, np. w infiltracji forów dla hakerów prowadzących działalność przestępczą, zorganizowanych grup cyberprzestępców i czarnego rynku internetowego, likwidowaniu botnetów itp.?	1

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
12 – Walka z cyberprzestępczością	3	Czy Państwa kraj podpisał Konwencję Rady Europy o cyberprzestępczości?	1	Czy obowiązują u Państwa jakiekolwiek przepisy prawne dotyczące własności intelektualnej w internecie i naruszeń praw autorskich?	1	Czy powołali Państwo centralny organ/centralną jednostkę do koordynacji działań w zakresie walki z cyberprzestępczością?	1	Czy dokonują Państwo oceny adekwatności szkoleń dla organów ścigania, wymiaru sprawiedliwości i personelu krajowego zespołu/krajowych zespołów CSIRT w zakresie zwalczania cyberprzestępczości?	1	Czy istnieje wyraźny podział obowiązków między zespołami CSIRT, organami ścigania a wymiarem sprawiedliwości (prokuratorami i sędziami) w ramach współpracy w zakresie zwalczania cyberprzestępczości?	1
	4			Czy obowiązują u Państwa jakiekolwiek przepisy prawne dotyczące nękania w internecie lub cyberprzemocy?	1	Czy ustanowili Państwo mechanizmy współpracy między odpowiednimi instytucjami krajowymi zaangażowanymi w walkę z cyberprzestępczością, w tym z krajowymi zespołami CSIRT zajmującymi się egzekwowaniem prawa?	1	Czy regularnie przeprowadzają Państwo ocenę mającą na celu zweryfikowanie, czy dysponują Państwo dostatecznymi zasobami (personelem, środkami finansowymi i narzędziami) przeznaczonymi dla jednostek zwalczania cyberprzestępczości w organach ścigania?	1	Czy Państwa ramy regulacyjne ułatwiają współpracę między zespołami CSIRT/organami ścigania a wymiarem sprawiedliwości (prokuratorami i sędziami)?	1
	5			Czy obowiązują u Państwa jakiekolwiek przepisy prawa dotyczące oszustw komputerowych, np. zgodne z postanowieniami Konwencji Rady Europy o cyberprzestępczości?	1	Czy współpracują Państwo z innymi państwami członkowskimi i wymieniają się z nimi informacjami w zakresie walki z cyberprzestępczością?	1	Czy regularnie przeprowadzają Państwo ocenę mającą na celu zweryfikowanie, czy dysponują Państwo dostatecznymi zasobami (personelem, środkami finansowymi i narzędziami) przeznaczonymi dla jednostek zwalczania cyberprzestępczości w prokuraturze?	1	Czy uczestniczą Państwo w opracowywaniu i aktualizowaniu jednolitych narzędzi i metod, formularzy i procedur używanych wspólnie z zainteresowanymi stronami z UE (organami ścigania, zespołami CSIRT, ENISA, centrum EC3 działającym w ramach Europolu)?	1
	6	-		Czy obowiązują u Państwa jakiekolwiek przepisy prawa dotyczące ochrony dzieci w internecie, np. zgodne z postanowieniami dyrektywy 2011/93/UE oraz Konwencji Rady Europy o cyberprzestępczości?	1	Czy współpracują Państwo z agencjami UE (np. Europolem, centrum EC3, Eurojustem, ENISA) i wymieniają się z nimi informacjami w zakresie walki z cyberprzestępczością?	1	Czy działają u Państwa specjalne sądy lub sędziowie specjalizujący się w sprawach cyberprzestępczości?	1	Czy istnieją u Państwa zaawansowane mechanizmy zmniejszające atrakcyjność cyberprzestępczości i zniechęcające do angażowania się w cyberprzestępczość?	0
	7	-		Czy wskazali Państwo krajowy punkt kontaktowy do celów wymiany informacji i udzielania odpowiedzi na pilne wnioski o udzielenie informacji od innych państw członkowskich dotyczące przestępstw określonych w dyrektywie 2013/40/UE (dyrektywie dotyczącej ataków na systemy informatyczne)?	1	Czy dysponują Państwo odpowiednimi narzędziami do zwalczania cyberprzestępczości, np. taksonomią i klasyfikacją cyberprzestępczości, narzędziami do gromadzenia dowodów elektronicznych, narzędziami kryminalistyki informatycznej, zaufanymi platformami wymiany informacji itp.?	1	Czy posiadają Państwo jakiekolwiek rozwiązania służące udzielaniu wsparcia i pomocy ofiarom cyberprzestępczości (ogółowi użytkowników, MŚP, dużym przedsiębiorstwom)?	1	Czy Państwa kraj korzysta z unijnego planu skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (EU Blueprint) lub protokołu działań w zakresie egzekwowania prawa w sytuacjach kryzysowych (Law Enforcement Emergency Response Protocol, EU LE ERP) w celu skutecznego reagowania na incydenty cybernetyczne na dużą skalę?	0

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
12 – Walka z cyberprzestępczością	8			Czy Państwa organ porządku publicznego posiada specjalną jednostkę ds. walki z cyberprzestępczością?	1	Czy posiadają Państwo standardowe procedury operacyjne dotyczące dowodów elektronicznych?	1	Czy stworzyli Państwo ramy międzyinstytucjonalne i mechanizmy współpracy między wszystkimi właściwymi zainteresowanymi stronami (np. organami ścigania, krajowym zespołem CSIRT, środowiskami wymiaru sprawiedliwości), w tym (w stosownych przypadkach) sektorem prywatnym (np. operatorami usług kluczowych, dostawcami usług) w celu reagowania na cyberataki?	1	-	
	9			Czy wyznaczyli Państwo punkt kontaktowy dostępny 24 godziny na dobę przez 7 dni w tygodniu zgodnie z art. 35 Konwencji o cyberprzestępczości?	1	Czy Państwa kraj uczestniczy w szkoleniach oferowanych lub finansowanych przez agencje unijne (np. Europol, Eurojust, OLAF, Cepol, ENISA)?	0	Czy Państwa ramy regulacyjne ułatwiają współpracę między zespołami CSIRT a organami ścigania?	1	-	
	10	-		Czy wyznaczyli Państwo punkt kontaktowy ds. unijnego protokołu działań w zakresie egzekwowania prawa w sytuacjach kryzysowych (EU LE RP) dostępny 24 godziny na dobę przez 7 dni w tygodniu w celu reagowania na poważne cyberataki?	1	Czy Państwa kraj rozważa możliwość przyjęcia drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości?	0	Czy posiadają Państwo mechanizmy (np. narzędzia, procedury) ułatwiające wymianę informacji i współpracę między zespołami CSIRT/organami ścigania oraz ewentualnie wymiarem sprawiedliwości (prokuratorami i sędziami) w zakresie walki z cyberprzestępczością?	1	-	
	11			Czy regularnie organizują Państwo specjalistyczne szkolenia dla zainteresowanych stron zaangażowanych w walkę z cyberprzestępczością (organów ścigania, wymiaru sprawiedliwości, zespołu CSIRT), np. szkolenia dotyczące zgłaszania/ścigania przestępstw wykorzystujących cyberprzestrzeń, szkolenia dotyczące m. in. gromadzenia dowodów elektronicznych i zapewnienia integralności całego cyfrowego łańcucha dowodowego i informatyki kryminalistycznej?	1						

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	12			Czy Państwa kraj ratyfikował/przystąpił do Konwencji Rady Europy o cyberprzestępczości?	1			-	-	-	
	13	-		Czy Państwa kraj podpisał i ratyfikował Protokół dodatkowy (dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych) do Konwencji Rady Europy o cyberprzestępczości?	0	-	-	-		-	
13 – Wprowadzenie mechanizmów zgłaszania incydentów	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy istnieją u Państwa nieformalne mechanizmy wymiany informacji na temat cyberincydentów między organizacjami prywatnymi a organami krajowymi?	1	Czy posiadają Państwo system zgłaszania incydentów dla wszystkich sektorów objętych załącznikiem II do dyrektywy w sprawie bezpieczeństwa sieci i informacji?	1	Czy posiadają Państwo faktycznie działający system obowiązkowego zgłaszania incydentów?	1	Czy posiadają Państwo zharmonizowaną procedurę dotyczącą sektorowych systemów zgłaszania incydentów?	1	Czy sporządzają Państwo roczne raporty o incydentach?	1

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
13 – Wprowadzenie mechanizmów zgłaszania incydentów	2	-		Czy wdrożyli Państwo wymogi dotyczące zgłaszania incydentów przez dostawców usług telekomunikacyjnych zgodnie z art. 40 dyrektywy (UE) 2018/1972? Zgodnie z tą dyrektywą, państwa członkowskie mają obowiązek zapewnić, aby przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej powiadamiały właściwy krajowy organ regulacyjny bez zbędnej zwłoki o incydentach związanych z bezpieczeństwem, które miały znaczący wpływ na sieci lub usługi.	1	Czy istnieje u Państwa mechanizm koordynacji/współpracy w zakresie obowiązków zgłaszania incydentów dotyczących RODO, NISD, art. 40 (dawnego art. 13a) i eIDAS?	1	Czy posiadają Państwo system zgłaszania incydentów dla sektorów innych niż sektory objęte dyrektywą w sprawie bezpieczeństwa sieci i informacji?	1	Czy podmiot przyjmujący zgłoszenia incydentów sporządza jakiekolwiek przeglądy cyberbezpieczeństwa (cybersecurity landscape reports) lub innego rodzaju analizy?	1
	3	-		Czy wdrożyli Państwo wymogi dotyczące zgłaszania incydentów przez dostawców usług zaufania zgodnie z art. 19 rozporządzenia eIDAS (rozporządzenie (UE) nr 910/2014)? Artykuł 19 wymaga między innymi, aby dostawcy usług zaufania zgłaszali organowi nadzorczemu istotne incydenty/naruszenia.	1	Czy dysponują Państwo odpowiednimi narzędziami zapewniającymi poufność i integralność informacji przekazywanych za pomocą różnych kanałów zgłoszeniowych?	1	Czy weryfikują Państwo skuteczność procedur zgłaszania incydentów? Np. wskaźniki dotyczące incydentów zgłoszonych za pośrednictwem odpowiednich kanałów, moment zgłoszenia incydentu itp.	1	-	
	4	-		Czy wdrożyli Państwo wymogi dotyczące zgłaszania incydentów przez dostawców usług cyfrowych zgodnie z art. 16 dyrektywy NIS? Zgodnie z art. 16 państwa członkowskie mają obowiązek zapewnić, aby dostawcy usług cyfrowych bez zbędnej zwłoki zgłaszali właściwemu organowi lub krajowemu CSIRT wszelkie incydenty mające istotny wpływ na świadczenie usługi, o której mowa w załączniku III, oferowanej przez tych dostawców w Unii.	1	Czy posiadają Państwo platformę/narzędzie ułatwiające dokonywanie zgłoszeń?	0	Czy na szczeblu krajowym istnieją wspólna taksonomia klasyfikacji incydentów i kategorie przyczyn incydentów?	0	-	

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
14 – Wzmocnienie prywatności i ochrony danych	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy przeprowadzili Państwo badania lub analizy mające na celu wskazanie obszarów wymagających poprawy dla zapewnienia lepszej ochrony praw obywateli do prywatności?	1	Czy krajowy organ ochrony danych zajmuje się problematyką cyberbezpieczeństwa (np. uczestniczy w opracowywaniu nowych ustaw i rozporządzeń w dziedzinie cyberbezpieczeństwa, określił minimalne środki bezpieczeństwa)?	1	Czy promują Państwo najlepsze praktyki w zakresie środków bezpieczeństwa i uwzględniania ochrony danych w fazie projektowania w sektorze publicznym lub prywatnym?	1	Czy regularnie przeprowadzają Państwo ocenę mającą na celu zweryfikowanie, czy dysponują Państwo dostatecznymi zasobami (personelem, środkami finansowymi i narzędziami) przeznaczonymi dla organu ochrony danych?	1	Czy istnieją u Państwa mechanizmy monitorowania zachodzących zmian technologicznych w celu dostosowywania do nich odpowiednich wytycznych i przepisów prawa/obowiązków prawnych?	1
	2	Czy stworzyli Państwo podstawę prawną na poziomie krajowym umożliwiającą egzekwowanie ogólnego rozporządzenia o ochronie danych (rozporządzenie (UE) nr 2016/679), np. utrzymali Państwo lub wprowadzili bardziej szczegółowe postanowienia bądź ograniczenia w stosunku do przepisów rozporządzenia?	0	-		Czy uruchamiają Państwo programy zwiększania świadomości i programy szkoleniowe dotyczące tego zagadnienia?	1	Czy zachęcają Państwo organizacje i przedsiębiorstwa do uzyskiwania certyfikatów według normy ISO/IEC 27701:2019 dotyczącej systemu zarządzania ochroną danych osobowych (PIMS)?	1	Czy aktywnie uczestniczą Państwo w inicjatywach badawczo-rozwojowych dotyczących technologii ochrony prywatności (PET) lub promują takie inicjatywy?	0
	3	-		-		Czy koordynują Państwo procedury zgłaszania incydentów z organem ochrony danych?	1	-		-	
	4	-		-		Czy promują i wspierają Państwo opracowywanie norm technicznych w zakresie bezpieczeństwa informacji i prywatności? Czy są one specjalnie dostosowywane do małych i średnich przedsiębiorstw (MŚP)?	0	-		-	

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	5	-		-		Czy udostępniają Państwo praktyczne i skalowalne wytyczne pomagające różnego rodzaju administratorom danych w spełnianiu wymogów i obowiązków prawnych dotyczących prywatności i ochrony danych?	0	-		-	

4.1.4 Grupa nr 4: Współpraca

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
15 – Ustanowienie partnerstwa publiczno-prywatnego (PPP)	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy panuje powszechna zgoda co do tego, że partnerstwa publiczno-prywatne w wieloraki sposób przyczyniają się do podnoszenia poziomu cyberbezpieczeństwa w kraju, np. dzięki wspólnemu zainteresowaniu rozwojem sektora cyberbezpieczeństwa, współpracy przy tworzeniu odpowiednich ram regulacyjnych w dziedzinie cyberbezpieczeństwa, wspieraniu badań naukowych i innowacji itp.?	1	Czy posiadają Państwo krajowy plan działania na rzecz ustanowienia partnerstw publiczno-prywatnych?	1	Czy utworzyli Państwo krajowe partnerstwa publiczno-prywatne?	1	Czy utworzyli Państwo międzysektorowe partnerstwa publiczno-prywatne?	1	Czy są Państwo w stanie modyfikować lub tworzyć nowe partnerstwa publiczno-prywatne w odpowiedzi na zachodzące zmiany technologiczne i regulacyjne?	1
	2	-		Czy wprowadzają Państwo podstawę prawną lub umowną (przepisy szczególne, wyznaczone organy krajowe, własność intelektualna) służącą do ustalania zakresu działania partnerstw publiczno-prywatnych?	1	Czy utworzyli Państwo sektorowe partnerstwa publiczno-prywatne?	1	Czy w ramach ustanowionych partnerstw publiczno-prywatnych koncentrują się Państwo również na współpracy publiczno-publicznej i prywatno-prywatnej?	1		
	3	-		-		Czy zapewniają Państwo środki finansowe na ustanawianie partnerstw publiczno-prywatnych?	1	Czy promują Państwo partnerstwa publiczno-prywatne wśród małych i średnich przedsiębiorstw (MŚP)?	1	-	

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
15 – Ustanowienie partnerstwa publiczno-prywatnego (PPP)	4	-		-		Czy ogół partnerstw publiczno-prywatnych podlega instytucjom publicznym, tj. partnerstwa publiczno-prywatne są zarządzane i koordynowane przez jeden punkt kontaktowy z sektora publicznego, organy publiczne uzgadniają z wyprzedzeniem, co chcą osiągnąć, jasne wytyczne dotyczące potrzeb i ograniczeń kierowane przez organy administracji publicznej do sektora prywatnego?	1	Czy mierzą Państwo rezultaty działania partnerstw publiczno-prywatnych?	1	-	
	5	-		-		Czy są Państwo członkiem umownego partnerstwa publiczno-prywatnego (cPPP) Europejskiej Organizacji ds. Cyberbezpieczeństwa (ECSO)?	0	-		-	
	6	-		-		Czy posiadają Państwo jedno lub więcej partnerstw publiczno-prywatnych zajmujących się działalnością CSIRT?	0	-		-	
	7					Czy posiadają Państwo jedno lub więcej partnerstw publiczno-prywatnych zajmujących się kwestiami ochrony krytycznej infrastruktury teleinformatycznej?	0				
	8	-		-		Czy posiadają Państwo jedno lub więcej partnerstw publiczno-prywatnych zajmujących się zwiększaniem świadomości zagadnień cyberbezpieczeństwa i rozwojem umiejętności?	0	-		-	
16 – Instytucjonalizacja współpracy między agencjami publicznymi	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1
	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy posiadają Państwo nieformalne kanały współpracy między agencjami publicznymi?	1	Czy posiadają Państwo krajowy program współpracy dotyczący cyberbezpieczeństwa, np. komisje doradcze, grupy sterujące, fora, rady, centra cybernetyczne lub spotkania grup eksperckich?	1	Czy organy publiczne uczestniczą w programie współpracy?	1	Czy zadbali Państwo o to, aby istniały kanały współpracy związanej z cyberbezpieczeństwem przynajmniej między następującymi organami publicznymi: służby wywiadowcze, krajowe organy ścigania, prokuratura, podmioty rządowe, krajowy zespół CSIRT oraz wojsko?	1	Czy agencje publiczne otrzymują jednolite minimum informacji na temat zmian zachodzących w krajobrazie zagrożeń i orientacji sytuacyjnej w dziedzinie cyberbezpieczeństwa?	1
	2	-		-		Czy ustanowili Państwo platformy współpracy w celu wymiany informacji?	1	Czy oceniają Państwo sukcesy i ograniczenia różnych systemów współpracy w zakresie wspierania skutecznej współpracy?	1	-	
16 – Instytucjonalizacja współpracy między agencjami publicznymi	3	-		-		Czy określili Państwo zakres działania platform współpracy (np. zadania i zakres odpowiedzialności, liczba obszarów tematycznych)?	1	-		-	
	4	-		-		Czy organizują Państwo coroczne spotkania?	1	-		-	
	5	-		-		Czy istnieją u Państwa mechanizmy współpracy między właściwymi organami w różnych regionach geograficznych, np. sieć korespondentów ds. bezpieczeństwa w każdym regionie, urzędnicy ds. cyberbezpieczeństwa w regionalnych izbach gospodarczych itp.?	1	-		-	
17 – Podejmowanie współpracy międzynarodowej (nie tylko z państwami członkowskimi UE)	a	Czy ten cel został uwzględniony w Państwa aktualnej krajowej strategii cyberbezpieczeństwa, czy też planują Państwo uwzględnienie go w kolejnej edycji strategii?	1	Czy istnieją nieformalne praktyki lub działania, które w sposób nieskoordynowany przyczyniają się do osiągnięcia tego celu?	1	Czy posiadają Państwo formalnie zdefiniowany i udokumentowany plan działania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić jego skuteczność?	1	Czy posiadają Państwo mechanizmy umożliwiające dynamiczne dostosowywanie planu działania do zmian zachodzących w otoczeniu?	1

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
17 – Podejmowanie współpracy międzynarodowej (nie tylko z państwami członkowskimi UE)	b			Czy określili Państwo planowane rezultaty, zasady przewodnie lub kluczowe działania dla swojego planu działania?	1	Czy posiadają Państwo plan działania przewidujący jasny podział zasobów i sposób zarządzania?	1	Czy weryfikują Państwo plan działania dotyczący tego celu, aby sprawdzić, czy prawidłowo ustalono w nim priorytety i czy został on zoptymalizowany?	1		
	c			W stosownych przypadkach, czy Państwa plan działania został wdrożony i czy jest już realizowany w ograniczonym zakresie?	0						
	1	Czy posiadają Państwo strategię zaangażowania na szczeblu międzynarodowym?	1	Czy zawarli Państwo umowy o współpracy z innymi krajami (dwustronne, wielostronne) lub partnerami w innych krajach, np. w sprawie wymiany informacji, budowania zdolności, pomocy itp.?	1	Czy prowadzą Państwo wymianę informacji na poziomie strategicznym, np. dotyczących polityki na wysokim szczeblu, postrzegania ryzyka itp.?	1	Czy krajowe agencje publiczne ds. cyberbezpieczeństwa w Państwa kraju uczestniczą w programach współpracy międzynarodowej?	1	Czy prowadzą Państwo rozmowy na jeden lub więcej tematów w ramach umów wielostronnych?	1
	2	Czy posiadają Państwo nieformalne kanały współpracy z innymi krajami?	1	Czy posiadają Państwo jeden punkt kontaktowy, który może pełnić funkcję łącznikową dla zapewnienia współpracy transgranicznej z organami państw członkowskich (grupą współpracy, siecią CSIRT itp.)?	1	Czy wymieniają Państwo informacje na poziomie taktycznym, np. katalog agresorów, ISAC, TTP itp.?	1	Czy regularnie oceniają Państwo wyniki przedsięwzięć prowadzonych we współpracy międzynarodowej?	1	Czy prowadzą Państwo rozmowy na jeden lub więcej tematów w ramach traktatów lub konwencji międzynarodowych?	1
	3	Czy władze publiczne wyraziły zamiar zaangażowania się we współpracę międzynarodową w dziedzinie cyberbezpieczeństwa?	1	Czy we współpracę międzynarodową są u Państwa zaangażowane specjalnie wybrane osoby?	1	Czy wymieniają Państwo informacje na poziomie operacyjnym, np. informacje dotyczące koordynacji operacyjnej, bieżących incydentów, IOC itp.?	1	-		Czy prowadzą Państwo rozmowy lub negocjacje dotyczące jednego lub więcej tematów na forum międzynarodowych grup eksperckich, np. Światowej Komisji ds. Stabilności w Cyberprzestrzeni (GCSC), grupy współpracy ENISA ds. bezpieczeństwa sieci i informacji, grupy ekspertów rządowych ONZ ds. bezpieczeństwa informacji (GGE) itp.?	1
	4	-		-		Czy biorą Państwo udział w międzynarodowych ćwiczeniach w dziedzinie bezpieczeństwa cybernetycznego?	1	-		-	
	5	-		-		Czy angażują się Państwo w międzynarodowe inicjatywy na rzecz budowania zdolności, np. szkolenia, rozwój umiejętności, opracowywanie standardowych procedur itp.?	0	-		-	

Cel NCSS	#	Poziom 1	R	Poziom 2	R	Poziom 3	R	Poziom 4	R	Poziom 5	R
	6	-		-		Czy zawarli Państwo umowy o wzajemnej pomocy z innymi krajami, np. w sprawie działania organów ścigania, postępowań sądowych, uwspólniania możliwości reagowania na incydenty, wspólnego korzystania z aktywów służących cyberbezpieczeństwu?	0	-		-	
	7	-		-		Czy podpisali Państwo lub ratyfikowali międzynarodowe traktaty bądź konwencje w dziedzinie cyberbezpieczeństwa, np. Międzynarodowy kodeks postępowania w zakresie bezpieczeństwa informacji (International Code of Conduct for Information Security), Konwencję o cyberprzestępczości?	0	-		-	

4.2 WYTYCZNE DOTYCZĄCE STOSOWANIA RAM

Celem niniejszego punktu jest przedstawienie państwom członkowskim wytycznych i zaleceń dotyczących wdrażania ram i wypełniania ankiety. Poniższe zalecenia wynikają głównie z informacji zwrotnych uzyskanych w rozmowach z przedstawicielami państw członkowskich:

- **Wygospodarowanie czasu na działania koordynacyjne w celu zgromadzenia danych i ich konsolidacji.** Większość państw członkowskich uznaje, że przeprowadzenie takiej samooceny powinno zająć około 15 osobodni. W celu przeprowadzenia samooceny trzeba będzie się zwrócić do wielu różnych zainteresowanych stron. Zaleca się zatem, aby przeznaczyć trochę czasu na etap przygotowawczy, co umożliwi zidentyfikowanie wszystkich właściwych zainteresowanych stron w organach rządowych, agencjach publicznych i w sektorze prywatnym.
- **Wskazanie centralnego organu odpowiedzialnego za przeprowadzenie samooceny na szczeblu krajowym.** Ponieważ gromadzenie materiałów na potrzeby wszystkich wskaźników NCAF może wymagać zaangażowania wielu zainteresowanych stron, zaleca się zlecenie przeprowadzenia samooceny w drodze współpracy i koordynacji ze wszystkimi zainteresowanymi stronami centralnemu organowi lub agencji.
- **Wykorzystanie oceny jako sposobu na wymianę i przekazywanie informacji dotyczących zagadnień cyberbezpieczeństwa.** Z doświadczeń opisywanych przez państwa członkowskie wynika, że rozmowy (w formie indywidualnych wywiadów, jak i grupowych warsztatów) stanowią dobrą okazję do wspierania debaty nad zagadnieniami cyberbezpieczeństwa oraz do informowania o wspólnych poglądach i obszarach wymagających poprawy. Informowanie o rezultatach nie tylko rzuca światło na najważniejsze osiągnięcia, ale może również pomóc w promowaniu zagadnień związanych z cyberbezpieczeństwem.
- **Wykorzystanie krajowej strategii cyberbezpieczeństwa do określenia zakresu celów podlegających ocenie.** 17 celów składających się na ramy NCAF opracowano w oparciu o cele, które zostały powszechnie uwzględnione przez państwa członkowskie w ich krajowych strategiach cyberbezpieczeństwa. Cele uwzględnione w ramach krajowej strategii cyberbezpieczeństwa powinny zostać wykorzystane do określenia zakresu oceny. Krajowa strategia cyberbezpieczeństwa nie powinna jednak ograniczać tej oceny. Ponieważ krajowe strategie cyberbezpieczeństwa z natury skupiają się na priorytetach, niektóre obszary zostały w nich celowo pominięte. Nie oznacza to jednak, że dana zdolność nie istnieje. Na przykład w przypadku, gdy konkretny cel został w krajowej strategii bezpieczeństwa cybernetycznego pominięty, ale państwo posiada zdolności w zakresie cyberbezpieczeństwa związane z tym celem, ocena tego celu jest możliwa.
- **Gdy zakres krajowej strategii cyberbezpieczeństwa ulegnie zmianie, należy zadbać o to, by interpretacja oceny punktowej uwzględniała tę zmianę.** Cykl życia krajowej strategii cyberbezpieczeństwa jest procesem wieloletnim. Krajowe strategie cyberbezpieczeństwa niektórych państw członkowskich są zazwyczaj realizowane z planem działania obejmującym od 3 do 5 lat, a między kolejnymi edycjami strategii zmienia się jej zakres. W związku z tym przedstawiając wyniki samooceny z dwóch kolejnych edycji krajowej strategii cyberbezpieczeństwa należy zachować szczególną ostrożność, ponieważ zmiana zakresu może faktycznie wpływać na ostateczną ocenę punktową dojrzałości. Zaleca się porównywanie ocen punktowych obejmujących pełny zakres celów strategicznych z poszczególnych lat (tj. zbiorcza ogólna ocena punktowa).

Przypomnienie dotyczące mechanizmu oceny punktowej – przykład dotyczący wskaźnika pokrycia

Mechanizm oceny punktowej obejmuje oceny punktowe na dwóch poziomach:

(i) **zbiorczy ogólny wskaźnik pokrycia** oparty na pełnym wykazie celów strategicznych zawartych w ramach samooceny; oraz
(ii) **zbiorczy szczegółowy wskaźnik pokrycia** oparty na celach strategicznych wybranych przez państwo członkowskie (zazwyczaj odpowiadających celom zawartym w krajowej strategii cyberbezpieczeństwa danego państwa).

Z założenia (zob. punkt 3.1 dotyczący mechanizmu oceny punktowej), zbiorczy szczegółowy wskaźnik pokrycia będzie co najmniej równy zbiorczemu ogólnemu wskaźnikowi pokrycia, ponieważ ten drugi wskaźnik może obejmować cele, które nie zostały uwzględnione przez dane państwo członkowskie, przez co obniża się zbiorczy ogólny wskaźnik pokrycia. Gdy państwo członkowskie wprowadzi nowy cel, zbiorczy wskaźnik pokrycia wzrośnie (tj. będzie obejmował więcej wskaźników dojrzałości), natomiast zbiorczy szczególny wskaźnik dojrzałości może się zmniejszyć (jeśli nowo dodany cel znajduje się na początkowym etapie, a tym samym jego poziom dojrzałości jest niski).

- **Wypełniając ankietę samooceny, należy pamiętać, że nadrzędnym celem jest wspieranie państw członkowskich w budowaniu zdolności w zakresie cyberbezpieczeństwa.** W związku z tym przy wypełnianiu ankiety samooceny, jeśli nawet w pewnych sytuacjach udzielenie zdecydowanej odpowiedzi na pytanie będzie trudne, zaleca się wybranie najbardziej pasującej odpowiedzi. Jeżeli na przykład odpowiedź na dane pytanie jest twierdząca w odniesieniu do określonego zakresu, ale przecząca w odniesieniu do innego zakresu, państwa członkowskie powinny pamiętać, że odpowiedź przecząca wymaga podjęcia działania: planu naprawczego lub planu działania w obszarze wymagającym poprawy, które będzie trzeba uwzględnić przy wprowadzaniu dalszych zmian.

5. DALSZE DZIAŁANIA

5.1 ULEPSZENIA W PRZYSZŁOŚCI

Podczas rozmów z przedstawicielami państw członkowskich oraz na etapie badania źródeł wtórnych, jako potencjalne zmiany do wprowadzenia w przyszłości w celu udoskonalenia istniejących ram oceny zdolności krajowych wskazano również następujące zalecenia:

- **Rozbudowanie systemu oceny punktowej w celu zwiększenia jego dokładności.** Na przykład dychotomiczne odpowiedzi „TAK/NIE” można by zastąpić odsetkiem pokrycia, który lepiej uwzględni złożoność zdolności, które zostały scalone na szczeblu krajowym. Na początek wybrano proste podejście przewidujące odpowiedzi „TAK/NIE”.
- **Wprowadzenie ilościowych wskaźników służących do pomiaru skuteczności krajowych strategii cyberbezpieczeństwa państw członkowskich.** Ramy oceny zdolności krajowych faktycznie skupiają się na ocenie poziomu dojrzałości zdolności państw członkowskich w zakresie cyberbezpieczeństwa. Dla uzupełnienia można by wprowadzić wskaźniki służące do pomiaru skuteczności działań i planów działania wdrażanych przez państwa członkowskie w celu budowania tych zdolności. Skonstruowanie takich wskaźników efektywności na obecnym etapie wydawało się nierealne ze względu na niewielką ilość informacji zwrotnych otrzymywanych z terenu, trudności ze znalezieniem miarodajnych wskaźników umożliwiających powiązanie rezultatów z wdrażaniem krajowych strategii cyberbezpieczeństwa, a także trudności ze stworzeniem realistycznych wskaźników, które następnie mogłyby być gromadzone. W przyszłości będą jednak prowadzone prace nad tym zagadnieniem.
- **Zmiana podejścia z samooceny na ocenę.** Ramy mogłyby zostać zmienione w kierunku podejścia opartego na ocenie, co zwiększyłoby spójność oceny dojrzałości zdolności państw członkowskich w zakresie cyberbezpieczeństwa. Przeprowadzenie oceny przez osobę trzecią mogłoby faktycznie ograniczyć ewentualny brak obiektywizmu.

ZAŁĄCZNIK A — PODSUMOWANIE WYNIKÓW BADANIA ŹRÓDEŁ WTÓRNYCH

Załącznik A zawiera podsumowanie wcześniejszych prac ENISA nad krajową strategią cyberbezpieczeństwa oraz zestawienie istotnych, ogólnodostępnych modeli dojrzałości odnoszących się do zdolności w zakresie cyberbezpieczeństwa. Przy dokonywaniu wyboru i przeglądu modeli przyjęto następujące założenia:

- Nie wszystkie modele opierają się na rygorystycznej metodologii badawczej;
- Struktura modeli i uzyskiwane na ich podstawie wyniki nie zawsze są dokładnie objaśnione, wraz ze wskazaniem wyraźnych powiązań między różnymi elementami charakteryzującymi poszczególne modele;
- Niektóre modele nie zawierają szczegółowych informacji na temat procesu ich powstawania, struktury i metod oceny;
- W przypadku pozostałych znalezionych przez nas modeli i narzędzi nie były dostępne żadne szczegółowe informacje o ich strukturze i zawartości, dlatego nie zostały one uwzględnione; oraz
- Wybór modeli do przeglądu jest oparty na ich zasięgu geograficznym. Najwięcej uwagi poświęcone będzie modelom dojrzałości dotyczącym zdolności w zakresie cyberbezpieczeństwa opracowanym do oceny wyników państw europejskich. Warto jednak rozszerzyć zasięg geograficzny w celu przeanalizowania dobrych praktyk w zakresie opracowywania modeli dojrzałości z całego świata.

Systematyczny przegląd istotnych, dostępnych publicznie modeli dojrzałości dotyczących zdolności w zakresie cyberbezpieczeństwa przeprowadzono z wykorzystaniem zmodyfikowanych ram analizy, opartych na metodologii opracowywania modeli dojrzałości zdefiniowanej przez Beckera[22]. Dla każdego istniejącego modelu dojrzałości przeanalizowano następujące elementy:

- **Nazwa modelu dojrzałości:** Nazwa modelu dojrzałości i najważniejsze odniesienia;
- **Źródło instytucjonalne:** Instytucja publiczna lub prywatna odpowiedzialna za opracowanie modelu;
- **Ogólny cel i przeznaczenie:** Ogólny zakres modelu i jego zamierzony cel lub cele;
- **Liczba i definicja poziomów:** Liczba poziomów dojrzałości w modelu oraz ich ogólny opis;
- **Liczba i nazwy atrybutów:** Liczba i nazwa atrybutów zastosowanych w modelu dojrzałości. Analiza atrybutów ma trzy cele:
  - Podział modelu dojrzałości na łatwe do zrozumienia części;
  - Połączenie szeregu atrybutów w grupy atrybutów realizujące ten sam cel; oraz
  - Przedstawienie różnych punktów widzenia na temat poziomu dojrzałości.

[22] J. Becker, R. Knackstedt i J. Pöppelbuß, „Developing Maturity Models for IT Management: A Procedure Model and its Application", Business & Information Systems Engineering, tom 1, nr 3, s. 213–222, czerwiec 2009.

- **Metoda oceny:** Metoda oceny modelu dojrzałości;
- **Przedstawienie wyników**: Określenie metody wizualizacji wyników modelu dojrzałości. Za tym krokiem przemawiają względy logiczne, a mianowicie zanadto złożone modele dojrzałości zazwyczaj nie spełniają pokładanych w nich oczekiwań, dlatego sposób przedstawienia wyników musi odpowiadać praktycznym potrzebom.

Dotychczasowe prace nad krajowymi strategiami cyberbezpieczeństwa

W ramach swoich początkowych działań, w 2012 r. ENISA opublikowała dwa dokumenty na temat krajowych strategii cyberbezpieczeństwa. Najpierw zaproponowała w przewodniku zatytułowanym „Practical guide on the development and execution phase of NCSS”[23] zestaw konkretnych działań umożliwiających sprawne wdrażanie krajowych strategii cyberbezpieczeństwa oraz przedstawiła w nim cykl życia krajowej strategii cyberbezpieczeństwa składający się z czterech faz: opracowanie strategii, realizacja strategii, ocena strategii i aktualizacja strategii. Następnie w dokumencie zatytułowanym „Setting the course for national efforts to strengthen security in cyberspace”[24] przedstawiła stan strategii cyberbezpieczeństwa w UE i poza nią w 2012 r. i zaproponowała, aby państwa członkowskie określiły pokrywające się obszary tematyczne w swoich krajowych strategiach cyberbezpieczeństwa i różnice między nimi.

W 2014 r. opublikowano pierwsze ramy ENISA do oceny krajowej strategii cyberbezpieczeństwa państwa członkowskiego[25]. Ramy te zawierają zalecenia i dobre praktyki, a także zestaw narzędzi do budowania zdolności na potrzeby oceny krajowych strategii cyberbezpieczeństwa (np. określone cele, dane wejściowe, rezultaty, kluczowe wskaźniki efektywności itp.). Narzędzia te są dostosowane do zróżnicowanych potrzeb państw o różnym poziomie dojrzałości planowania strategicznego. W tym samym roku ENISA opublikowała „Online NCSS Interactive Map”[26] – interaktywną internetową mapę NCSS, która umożliwia użytkownikom szybkie zapoznanie się z krajowymi strategiami cyberbezpieczeństwa wszystkich państw członkowskich i państw EFTA, wraz z ich celami strategicznymi i przykładami zakończonych sukcesem wdrożeń. Mapa, która została opracowana po raz pierwszy jako repozytorium krajowych strategii cyberbezpieczeństwa (w 2014 r.), została w 2018 r. zaktualizowana o przykłady wdrożeń, a od 2019 r. stanowi *węzeł informacyjny* umożliwiający centralizację danych dostarczanych przez państwa członkowskie, dotyczących ich działań na rzecz zwiększenia krajowego bezpieczeństwa cybernetycznego.

W przewodniku „NCSS Good Practice Guide”[27] opublikowanym w 2016 r. określono piętnaście celów strategicznych. Przeanalizowano w nim również stan wdrożenia krajowych strategii bezpieczeństwa cybernetycznego poszczególnych państw członkowskich oraz określono różne luki i wyzwania związane z ich wdrażaniem.

[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, zaktualizowana w 2019 r.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Ten dokument stanowi aktualizację przewodnika z 2012 r.: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
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

Następnie w 2018 r. ENISA opublikowała „National Cybersecurity Strategies Evaluation Tool" (narzędzie do oceny krajowych strategii cyberbezpieczeństwa)[28]: interaktywne narzędzie samooceny, pomagające państwom członkowskim w ocenie strategicznych priorytetów i celów związanych z ich krajowymi strategiami bezpieczeństwa cybernetycznego. Narzędzie to zawiera zbiór prostych pytań, na podstawie których państwa członkowskie otrzymują szczegółowe rekomendacje dotyczące realizacji poszczególnych celów. Natomiast w opublikowanym w 2019 r. dokumencie pt. „Good practices in innovation on Cybersecurity under the NCSS"[29] przedstawiono temat innowacji w dziedzinie cyberbezpieczeństwa w krajowej strategii bezpieczeństwa cybernetycznego. W dokumencie tym omówiono wyzwania i dobre praktyki w różnych wymiarach innowacji z punktu widzenia ekspertów merytorycznych, z myślą o opracowywaniu przyszłych, innowacyjnych celów strategicznych.

A.1 Model zdolności w zakresie cyberbezpieczeństwa dla państw (Cybersecurity Capacity Maturity Model for Nations, CMM)

Model zdolności w zakresie cyberbezpieczeństwa dla państw (CMM) został opracowany przez Global Cyber Security Capacity Centre (Centrum Zdolności) działające w ramach Oxford Martin School na Uniwersytecie Oksfordzkim. Zadaniem Centrum Zdolności jest zwiększanie skali i efektywności budowania zdolności w zakresie cyberbezpieczeństwa, zarówno w Zjednoczonym Królestwie, jak i na szczeblu międzynarodowym, poprzez wdrożenie modelu zdolności w zakresie cyberbezpieczeństwa (CMM). Model CMM jest skierowany bezpośrednio do krajów, które chcą zwiększać swoje krajowe zdolności w zakresie cyberbezpieczeństwa. Model został pierwotnie uruchomiony w 2014 r., a w 2016 r., po zastosowaniu go do przeglądu 11 krajowych zdolności w zakresie cyberbezpieczeństwa, wprowadzono do niego zmiany.

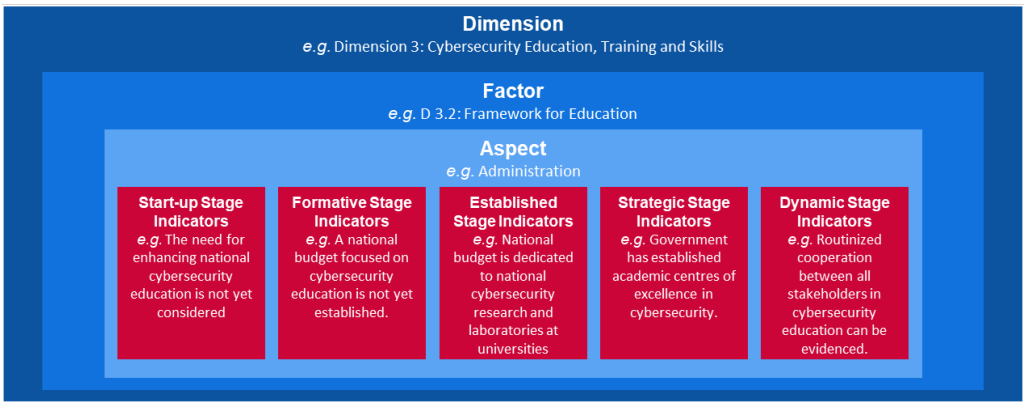
Atrybuty/ wymiary

CMM dzieli zdolności w zakresie cyberbezpieczeństwa na **pięć wymiarów** odpowiadających grupom zdolności w zakresie cyberbezpieczeństwa. Każda grupa reprezentuje inną „optykę" badawczą, przy użyciu której można badać i poznawać zdolności w zakresie cyberbezpieczeństwa. **Czynniki** wyróżnione w tych pięciu wymiarach opisują szczegóły posiadanych zdolności w zakresie cyberbezpieczeństwa. Te szczegóły to elementy, które przyczyniają się do wzrostu dojrzałości zdolności w zakresie cyberbezpieczeństwa w każdym z wymiarów. Dla każdego czynnika wyróżniono kilka **aspektów** reprezentujących różne składowe tego czynnika. Aspekty te stanowią metodę organizacyjną służącą do podziału wskaźników na mniejsze, bardziej zrozumiałe grupy. Każdy aspekt jest następnie oceniany za pomocą **wskaźników** w celu opisania etapów, działań lub elementów składowych typowych dla danego etapu dojrzałości (opisanych w następnym punkcie) w ramach danego aspektu, czynnika i wymiaru.

Powyższe określenia można zobrazować jako warstwy pokazane na poniższym rysunku.

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

Rys. 4: Przykładowe wskaźniki CMM



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Wymiar Np. wymiar 3: Edukacja, szkolenia i umiejętności w dziedzinie cyberbezpieczeństwa
Factor e.g. D 3.2: Framework for Education	Czynnik Np. D 3.2: Ramy edukacji
Aspect e.g. Administration	Aspekt Np. administracja
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Wskaźniki etapu początkowego Np. konieczność wzbogacenia edukacji w zakresie cyberbezpieczeństwa w kraju nie została jeszcze uwzględniona
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Wskaźniki etapu formacji Np. nie ustanowiono jeszcze krajowego budżetu z przeznaczeniem na edukację w zakresie cyberbezpieczeństwa
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Wskaźniki etapu ugruntowania Np. przeznaczono środki z krajowego budżetu na krajowe badania naukowe i laboratoria uczelniane w dziedzinie cyberbezpieczeństwa
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Wskaźniki etapu strategicznego Np. rząd ustanowił akademickie centrum doskonałości zajmujące się edukacją w dziedzinie cyberbezpieczeństwa
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Wskaźniki etapu dynamicznego Np. rutynowa współpraca między wszystkimi zainteresowanymi stronami jest możliwa do wykazania

Poniżej przedstawiono dokładniej pięć wymiarów modelu:

i Opracowanie polityki i strategii w zakresie cyberbezpieczeństwa (6 czynników);
ii Wspieranie odpowiedzialnej kultury cyberbezpieczeństwa w społeczeństwie (5 czynników);
iii Poszerzanie wiedzy o cyberbezpieczeństwie (3 czynniki);
iv Tworzenie skutecznych ram prawnych i regulacyjnych (3 czynniki); oraz
v Kontrolowanie ryzyka za pomocą norm, organizacji i technologii (7 czynników).

Poziomy dojrzałości

W CMM zastosowano **5 poziomów dojrzałości**, służących do określania stopnia, w jakim dany kraj poczynił postępy w odniesieniu do określonego czynnika/aspektu zdolności w zakresie cyberbezpieczeństwa. Poziomy te służą do zobrazowania istniejących zdolności w zakresie cyberbezpieczeństwa:

- **Etap początkowy**: Na tym etapie dojrzałość w zakresie cyberbezpieczeństwa w ogóle nie istnieje lub znajduje się w fazie zalążkowej. Może dochodzić do wstępnych rozmów na temat budowania zdolności w zakresie cyberbezpieczeństwa, ale nie podjęto żadnych konkretnych działań. Na tym etapie brak jest jakichkolwiek możliwych do zaobserwowania dowodów;
- **Etap formacji**: Niektóre cechy poszczególnych aspektów zaczęły się pojawiać i kształtować, ale mogą one mieć charakter doraźny, niezorganizowany, być słabo zdefiniowane lub po prostu „nowe". Można jednak wyraźnie wykazać, że takie działania są prowadzone;
- **Etap ugruntowania**: Elementy danego aspektu zostały wprowadzone i funkcjonują. Nie przemyślano jednak dokładnie kwestii względnej alokacji zasobów. Zapadło niewiele decyzji dotyczących kompromisów co do „względnej" wysokości nakładów przeznaczanych na poszczególne elementy tego aspektu. Aspekt ten jest jednak funkcjonalny i zdefiniowany;
- **Etap strategiczny**: Podjęto decyzje o tym, które części tego aspektu są ważne, a które są mniej istotne dla danej organizacji lub narodu. Etap strategiczny odzwierciedla fakt, że dokonano takich wyborów na podstawie szczególnej sytuacji danego kraju lub organizacji; oraz
- **Etap dynamiczny**: Na tym etapie istnieją jasno określone mechanizmy umożliwiające modyfikację strategii w zależności od panujących okoliczności, takich jak technologia stosowana w środowisku zagrożeń, globalny konflikt lub znacząca zmiana w jednym z obszarów zainteresowania (np. cyberprzestępczość lub prywatność). Dynamiczne organizacje opracowały metody umożliwiające bezproblemową zmianę strategii. Na tym etapie charakterystyczne są szybkie podejmowanie decyzji, realokacja zasobów i nieustanne obserwowanie zmieniającego się otoczenia.

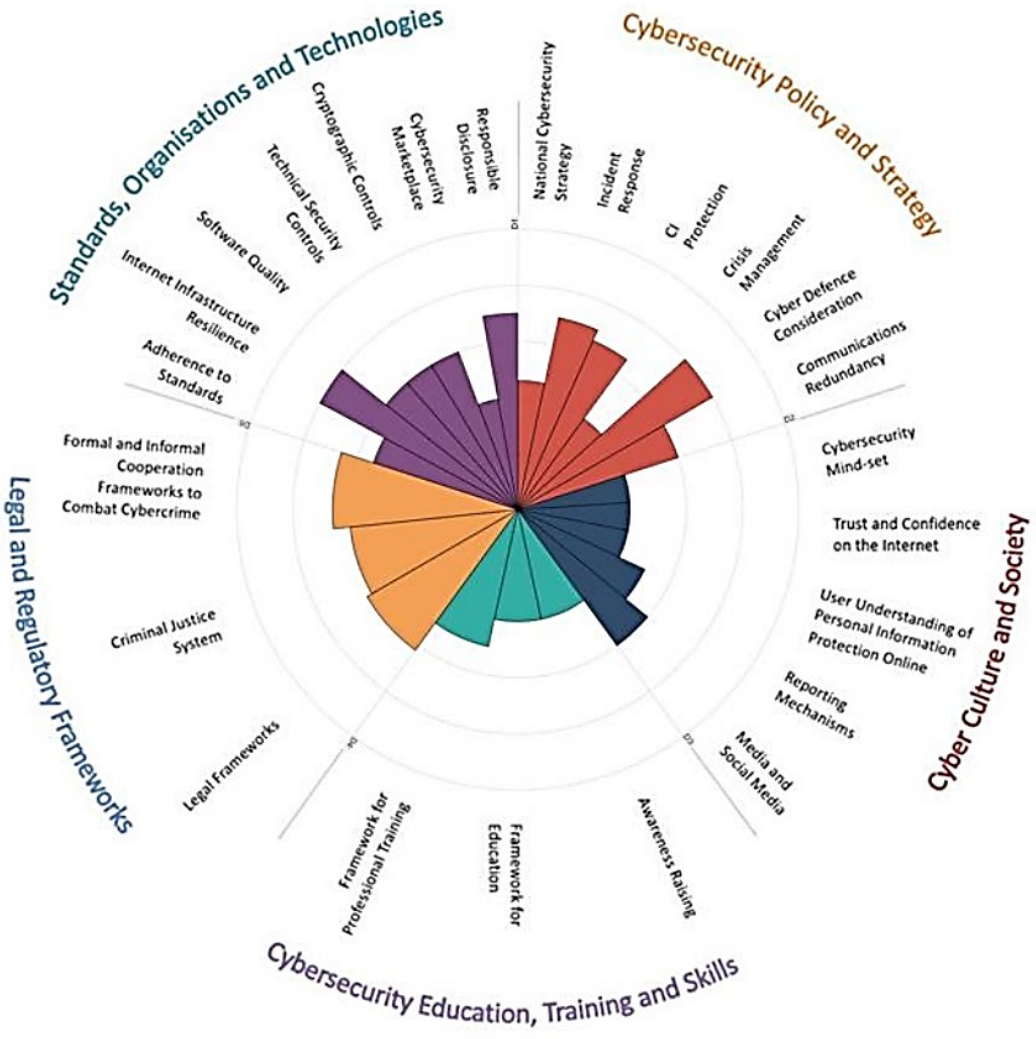
Metoda oceny

Ponieważ Centrum Zdolności nie posiada kompleksowej, obszernej wiedzy o wszystkich krajowych kontekstach, w których stosowany jest ten model, współpracuje z organizacjami międzynarodowymi, właściwymi ministerstwami lub organizacjami w danym państwie w celu oceny dojrzałości zdolności w zakresie cyberbezpieczeństwa. Aby móc ocenić poziom dojrzałości pięciu wymiarów zawartych w modelu CMM, Centrum Zdolności i właściwa organizacja odbywają dwu- lub trzydniowe spotkania z odpowiednimi zainteresowanymi stronami z sektora publicznego i prywatnego w danym kraju, organizując grupy dyskusyjne na temat wymiarów modelu CMM. Każdy wymiar jest omawiany co najmniej dwukrotnie przez różne grupy zainteresowanych stron. W ten sposób uzyskana zostaje wstępna pula danych na potrzeby późniejszej oceny.

Sposób przedstawienia lub zobrazowania wyników

Model CCM przedstawia obraz poziomu dojrzałości poszczególnych krajów w postaci wykresu radarowego składającego się z pięciu części, z których każda odpowiada jednemu wymiarowi. Każdy wymiar zajmuje jedną piątą wykresu, natomiast pięć poziomów dojrzałości dla poszczególnych czynników sięga od środka wykresu do zewnątrz; jak widać poniżej, „etap początkowy" znajduje się najbliżej środka wykresu, a „etap dynamiczny" znajduje się na obrzeżach wykresu.

Rys. 5 CMM: Zestawienie wyników



Standards, Organisations and Technologies	Normy, organizacje i technologie
Legal Regulatory Frameworks	Prawne ramy regulacyjne
Cybersecurity Education, Training and Skills	Edukacja, szkolenia i umiejętności w dziedzinie cyberbezpieczeństwa
Cybersecurity Policy and Strategy	Polityka i strategia cyberbezpieczeństwa
Cyber Culture and Society	Cyberkultura i cyberspołeczeństwo
Responsible Disclosure	Odpowiedzialne ujawnianie informacji
Cybersecurity market place	Rynek cyberbezpieczeństwa
Cryptographic Controls	Kryptograficzne mechanizmy kontroli
Technical Security Controls	Kontrole bezpieczeństwa technicznego
Software Quality	Jakość oprogramowania
Internet Infrastructure Resilience	Odporność infrastruktury internetowej
Adherence to Standards	Przestrzeganie norm
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formalne i nieformalne ramy współpracy na rzecz zwalczania cyberprzestępczości
Criminal Justice System	System sądownictwa karnego
Legal Frameworks	Ramy prawne
Framework for Professional Training	Ramy szkolenia zawodowego
Framework for Education	Ramy edukacji
Awareness Raising	Zwiększanie świadomości
Media and Social Medai	Media i media społecznościowe
Reporting Mechanisms	Mechanizmy sprawozdawcze
User Understanding of Personal Information Protection Online	Wiedza użytkowników o ochronie informacji osobowych w internecie
Trust and Confidence on the Internet	Zaufanie i pewność w internecie
Cybersecurity Mind-set	Nastawienie na cyberbezpieczeństwo
Communications Redundancy	Redundancja w komunikacji
Cyber Defence Consideration	Uwzględnianie zagadnień cyberobrony
Crisis Management	Zarządzanie kryzysowe
CI Protection	Ochrona infrastruktury krytycznej
Incident Response	Reagowanie na incydenty

National Cybersecurity Strategy	Krajowa strategia cyberbezpieczeństwa

Global Cyber Security Capacity Centre, Oxford Martin School, Uniwersytet Oksfordzki, 2017

A.2 Model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Cybersecurity Capability Maturity Model, C2M2)

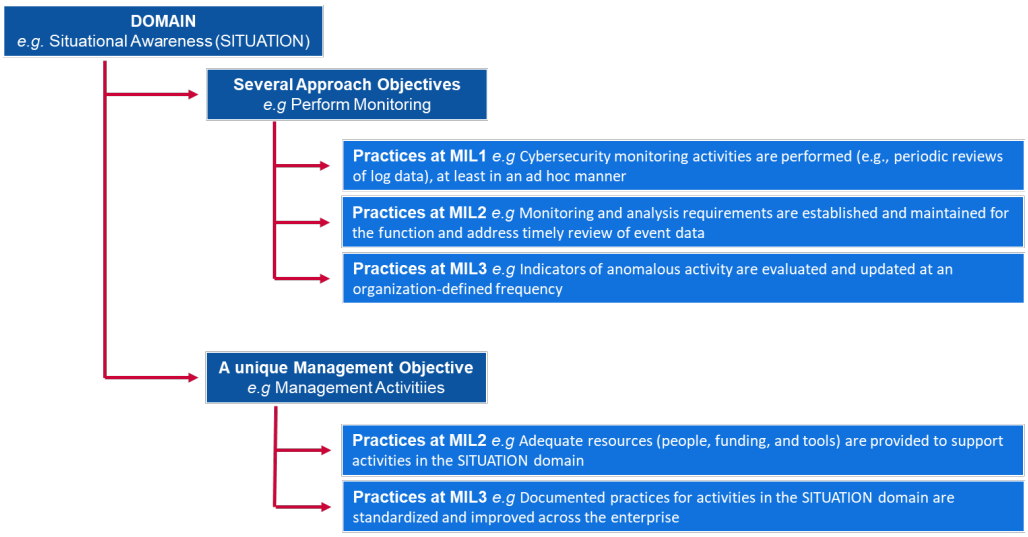
Model dojrzałości zdolności w zakresie cyberbezpieczeństwa (C2M2) został opracowany przez Departament Energii Stanów Zjednoczonych we współpracy z ekspertami z sektora prywatnego i publicznego. Zadaniem Centrum Zdolności jest pomaganie organizacjom ze wszystkich sektorów, niezależnie od ich rodzaju i wielkości, w ocenie i udoskonalaniu ich programów cyberbezpieczeństwa oraz zwiększaniu ich odporności operacyjnej. Model C2M2 koncentruje się na wdrażaniu praktyk w zakresie cyberbezpieczeństwa związanych z zasobami informacyjnymi, technologią informacyjną (IT) i technologią operacyjną (OT) oraz środowiskami działania tych technologii, a także na zarządzaniu tymi praktykami. W C2M2 modele dojrzałości definiuje się jako: „zbiór cech, atrybutów, wskaźników lub wzorców, które obrazują zdolność i postępy w danej dyscyplinie". Model C2M2 został pierwotnie uruchomiony w 2014 r., a w 2019 r. wprowadzono do niego zmiany.

Atrybuty/ wymiary

Model C2M2 obejmuje **dziesięć dziedzin** odpowiadających logicznemu podziałowi praktyk w zakresie cyberbezpieczeństwa. Każdy zbiór praktyk przedstawia działania, które organizacja może realizować w celu wprowadzenia i zwiększania dojrzałości zdolności w danej dziedzinie. Każda dziedzina zostaje następnie powiązana z **unikatowym celem zarządzania** i **kilkoma celami podejścia**. W ramach celów podejścia i celów zarządzania wyszczególniono **szereg praktyk** w celu opisania zinstytucjonalizowanych działań.

Związek między tymi pojęciami został podsumowany poniżej:

Rys. 6: Przykładowy wskaźnik C2M2



Domain eg Situational Awareness (SITUATION)
Several Approaches Objectives e.g. Perform Monitoring
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner

Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data

Dziedzina, np. orientacja sytuacyjna (SYTUACJA)
Kilka celów podejścia, np. wykonywanie monitoringu
Praktyki na poziomie MIL1, np. prowadzenie działań w zakresie monitorowania cyberbezpieczeństwa (takich jak okresowe przeglądanie danych z dziennika), przynajmniej w trybie doraźnym
Praktyki na poziomie MIL2, np. wprowadzenie i utrzymywanie wymogów monitorowania i analizy dla danej funkcji, zapewniających terminowe zapoznawanie się z danymi dotyczącymi zdarzeń

Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency A unique Management Objectve e.g. Management Activities **Practices at MIL2** e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain **Practices at MIL3** e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Praktyki na poziomie MIL3**, np. ocena i aktualizacja wskaźników aktywności odbiegającej od normy z częstotliwością wskazaną przez organizację. Unikatowy cel zarządzania, np. działania zarządcze **Praktyki na poziomie MIL2**, np. zapewnienie odpowiednich zasobów (personelu, środków finansowych i narzędzi) do wspierania działań w dziedzinie SYTUACJA. **Praktyki na poziomie MIL3**, np. udokumentowane praktyki dotyczące działań w dziedzinie SYTUACJA są ujednolicone i udoskonalane w całym przedsiębiorstwie

Poniżej przedstawiono szczegółowo dziesięć dziedzin modelu:

i Zarządzanie ryzykiem (RISK);
ii Zarządzanie aktywami, zmianami i konfiguracją (AKTYWA);
iii Zarządzanie tożsamością i dostępem (DOSTĘP);
iv Zarządzanie zagrożeniami i podatnościami (ZAGROŻENIE);
v Orientacja sytuacyjna (SYTUACJA);
vi Reagowanie na zdarzenia i incydenty (REAGOWANIE);
vii Zarządzanie łańcuchem dostaw i zależnościami zewnętrznymi (ZALEŻNOŚCI);
viii Zarządzanie siłą roboczą (SIŁA ROBOCZA);
ix Architektura cyberbezpieczeństwa (ARCHITEKTURA);
x Zarządzanie programem cyberbezpieczeństwa (PROGRAM).

Poziomy dojrzałości

Model C2M2 zawiera **4 poziomy dojrzałości** (nazywane poziomami wskaźnika dojrzałości – MIL) służące do określania dwutorowego wzrostu dojrzałości: wzrostu dojrzałości podejścia i wzrostu dojrzałości zarządzania. Poziomy dojrzałości są uszeregowane od MIL0 do MIL3 i stosuje się je niezależnie dla każdej dziedziny.

- **MIL0**: Nie stosuje się żadnych praktyk.
- **MIL1**: Pierwsze praktyki są stosowane, choć mogą mieć charakter doraźny.
- **MIL2**: Charakterystyka zarządzania:
  - Praktyki są udokumentowane;
  - Zapewniono odpowiednie zasoby do wsparcia tego procesu;
  - Personel realizujący praktyki posiada odpowiednie kwalifikacje i wiedzę; oraz
  - Dokonano podziału odpowiedzialności i uprawnień w związku z wykonywaniem tych praktyk.

  Charakterystyka podejścia:
  - Praktyki są bardziej kompletne lub zaawansowane niż w przypadku MIL1.
- **MIL3**: Charakterystyka zarządzania:
  - Działania są prowadzone zgodnie z polityką (lub innymi wytycznymi organizacyjnymi);
  - Wprowadzono cele dotyczące wyników dla działań w danej dziedzinie i są one monitorowane w celu śledzenia ich realizacji; oraz
  - Udokumentowane praktyki dotyczące działań w danej dziedzinie zostały ujednolicone i udoskonalone w całym przedsiębiorstwie.

  Charakterystyka podejścia:
  - Praktyki są bardziej kompletne lub zaawansowane niż w przypadku MIL2.

Metoda oceny

Model C2M2 jest przeznaczony do stosowania z **metodologią samooceny** i zestawem narzędzi (dostępnym na żądanie) i służy organizacji do pomiaru i doskonalenia programu cyberbezpieczeństwa. Samoocenę z zastosowaniem zestawu narzędzi można przeprowadzić w ciągu jednego dnia, ale zestaw narzędzi można zmodyfikować w celu przeprowadzenia bardziej rygorystycznej oceny. Model C2M2 może również pomóc przy opracowaniu nowego programu cyberbezpieczeństwa.

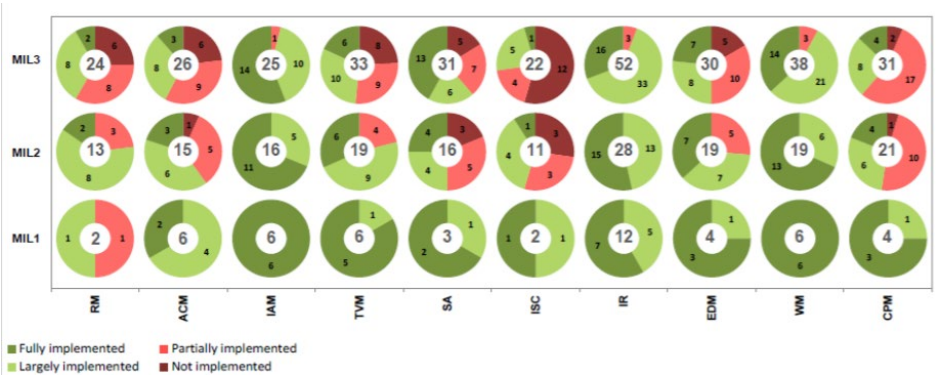
Zawartość modelu jest prezentowana na dużym poziomie abstrakcji, co umożliwia jej interpretowanie przez organizacje różnego rodzaju, o różnej strukturze i wielkości, należące do różnych branż. Powszechne stosowanie modelu w danym sektorze może pomagać w analizach porównawczych zdolności sektora w zakresie cyberbezpieczeństwa.

Sposób przedstawienia lub zobrazowania wyników

W modelu C2M2 na podstawie wyników badania generowany jest raport z oceny (Evaluation Scoring Report). Wyniki w raporcie są podzielone na dwa widoki: widok celów, pokazujący odpowiedzi na praktyczne pytania w podziale na dziedziny i ich cele, oraz widok dziedzin, pokazujący odpowiedzi dla wszystkich dziedzin i MIL. W obu ujęciach zastosowano system wizualizacji wykorzystujący wykresy kołowe (lub „pierścieniowe"), po jednym dla każdej odpowiedzi, a także mechanizm oceny punktowej w postaci „sygnalizacji świetlnej". Jak widać na Rys. 7, czerwone sektory na wykresie pierścieniowym pokazują liczbę pytań, na które w ankiecie udzielono odpowiedzi „Nie wdrożono" (ciemnoczerwone) lub „Wdrożono częściowo" (jasnoczerwone). Zielone sektory wskazują, na ile pytań udzielono odpowiedzi „Wdrożono w dużym stopniu" (jasnozielone) lub „Wdrożono w pełni" (ciemnozielone).

Rys. 7 przedstawia przykład karty oceny punktowej na koniec oceny dojrzałości. Na osi X oznaczono 10 dziedzin modelu C2M2, a na osi Y poziomy dojrzałości (MIL). Patrząc na wykres i rozpatrując dziedzinę zarządzania ryzykiem (RM), można zobaczyć trzy wykresy kołowe, odpowiadające poziomom dojrzałości MIL1, MIL2 i MIL3. W przypadku dziedziny RM, z wykresu wyraźnie wynika, że istnieją dwa elementy, które należy ocenić pod kątem osiągnięcia pierwszego poziomu dojrzałości (MIL1). W tym przypadku jeden uzyskał ocenę „Wdrożono w dużym stopniu", a drugi „Wdrożono częściowo". W przypadku drugiego poziomu dojrzałości (MIL2), model przewiduje ocenę 13 elementów. Dwa z tych 13 elementów należą do poziomu pierwszego, tj. ML1, a 11 do poziomu drugiego, tj. MIL2. To samo dotyczy trzeciego poziomu (MIL3).

Rys. 7: Model C2M2 – Przykładowy widok dziedzin



Fully implemented	Wdrożono w pełni
Largely implemented	Wdrożono w dużym stopniu
Partially implemented	Wdrożono częściowo
Not implemented	Nie wdrożono
MIL1	MIL1
MIL2	MIL2
MIL3	MIL3
RM	RM
ACM	ACM
IAM	IAM
TVM	TVM
SA	SA
ISC	ISC
IR	IR
EDM	EDM
WM	WM
CPM	CPM

Źródło: Departament Energii Stanów Zjednoczonych, Office of Electricity Delivery and Energy Reliability, 2015.

A.3 Ramy na rzecz poprawy cyberbezpieczeństwa infrastruktury krytycznej (Framework for Improving Critical Infrastructure Cybersecurity)

Ramy na rzecz poprawy cyberbezpieczeństwa infrastruktury krytycznej zostały opracowane w Narodowym Instytucie Standaryzacji i Technologii (NIST). Koncentrują się one na wyznaczaniu kierunków działań w zakresie cyberbezpieczeństwa i zarządzaniu ryzykiem w organizacji. Są przeznaczone dla wszystkich rodzajów organizacji, bez względu na ich wielkość, stopień ryzyka dla cyberbezpieczeństwa czy stopień złożoności cyberbezpieczeństwa. Ponieważ są to ramy, a nie model, zostały one skonstruowane inaczej niż już przeanalizowane modele.

Ramy składają się z trzech elementów: trzonu ram, poziomów realizacji oraz profili ram:

- **Trzonem ram** jest zbiór działań w dziedzinie cyberbezpieczeństwa, oczekiwanych rezultatów oraz odpowiednich źródeł, wspólnych dla wszystkich sektorów infrastruktury krytycznej. Są one zbliżone do atrybutów lub wymiarów występujących w modelach dojrzałości zdolności w zakresie cyberbezpieczeństwa.
- **Poziomy realizacji ram** („poziomy") informują, jak organizacja postrzega ryzyko dla cyberbezpieczeństwa oraz wdrożone procesy służące do zarządzania tym ryzykiem. Poziomy są uszeregowane od podstaw (poziom 1) do zdolności adaptacji (poziom 4) w zależności od rygorystyczności oraz zaawansowania praktyk zarządzania ryzykiem dla cyberbezpieczeństwa. Poziomy nie odzwierciedlają poziomów dojrzałości, ich zadaniem jest raczej wspieranie procesu decyzyjnego w organizacji w zakresie sposobu zarządzania ryzykiem dla cyberbezpieczeństwa, a także wybierania priorytetowych aspektów organizacji, do których można by było przydzielić dodatkowe zasoby.
- **Profil ram** („profil") przedstawia wyniki w oparciu o potrzeby biznesowe wskazane przez organizację spośród kategorii i podkategorii ram. Profil można scharakteryzować w odniesieniu do dostosowania norm, wytycznych i praktyk do rdzenia ram w danym scenariuszu wdrożeniowym. Profile mogą służyć do określania możliwości poprawy stanu cyberbezpieczeństwa poprzez porównaniu profilu „aktualnego" (stanu obecnego) z profilem „docelowym" (stanem planowanym).

Rdzeń ram

Rdzeń ram składa się z pięciu **funkcji**. Wszystkie funkcje razem wzięte przedstawiają ogólny, strategiczny obraz cyklu życia zarządzania ryzykiem dla cyberbezpieczeństwa przez organizację. Następnie w rdzeniu ram określone zostają podstawowe, kluczowe **kategorie** i **podkategorie** dla poszczególnych funkcji, które zostają dopasowane do przykładowych źródeł informacyjnych, takich jak istniejące normy, wytyczne i praktyki dla poszczególnych podkategorii.

Funkcje i kategorie zostały przedstawione szczegółowo poniżej:

i **Określanie**: Zrozumienie przez organizację, w jaki sposób zarządzać zagrożeniami dla cyberbezpieczeństwa systemów, ludzi, aktywów, danych i zdolności.
   - Podkategorie: Zarządzanie aktywami; otoczenie biznesowe; ogół zarządzania; ocena ryzyka; strategia zarządzania ryzykiem

ii **Ochrona**: Opracowanie i wdrożenie odpowiednich zabezpieczeń w celu zapewnienia świadczenia usług o krytycznym znaczeniu.
   - Podkategorie: Zarządzanie tożsamością i kontrola dostępu; wiedza i szkolenia; bezpieczeństwo danych; procesy i procedury ochrony informacji; utrzymanie; technologia zabezpieczeń

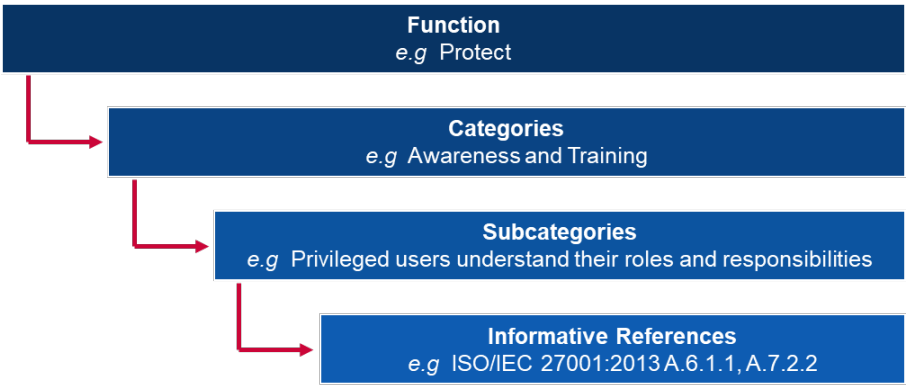
iii **Wykrywanie**: Opracowanie i wdrożenie odpowiednich działań umożliwiających stwierdzenie zdarzenia związanego z cyberbezpieczeństwem.
   - Podkategorie: Anomalie i zdarzenia; ciągłe monitorowanie bezpieczeństwa; procesy detekcji.

iv **Reagowanie**: Opracowanie i wdrożenie odpowiednich działań w celu podjęcia działań związanych ze stwierdzeniem cyberincydentu.

- Podkategorie: Planowanie reakcji; komunikacja, analiza, ograniczanie; doskonalenie.

v **Przywracanie**: Opracowanie i wdrożenie odpowiednich działań mających na celu posiadanie planów zapewniających odporność na cyberincydenty oraz przywracanie zdolności lub usług, które zostały zakłócone wskutek wystąpienia cyberincydentu.
- Podkategorie: planowanie przywracania; doskonalenie procesów przywracania; komunikacja w ramach przywracania

Rys. 8: Przykładowe ramy na rzecz poprawy cyberbezpieczeństwa infrastruktury krytycznej



Function e.g Project
Categories e.g Awarness and Training
Subcategories e.g Privileged useres understand their roles and responsibilities
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Funkcja np. projekt
Kategorie np. wiedza i szkolenia
Podkategorie np. uprzywilejowani użytkownicy znają swoje role i obowiązki

Źródła informacyjne, np. ISO/IEC 27001:2013 A.6.1.1, A.7.2.2

Poziomy

Ramy na rzecz poprawy cyberbezpieczeństwa infrastruktury krytycznej opierają się na **4 poziomach**, z których każdy jest zdefiniowany wzdłuż trzech osi: Proces zarządzania ryzykiem, zintegrowany program zarządzania ryzykiem i partycypacja zewnętrzna. Poziomów nie należy traktować jako poziomów dojrzałości, lecz jako ramy zapewniające organizacjom kontekstualizację ich poglądów na temat ryzyka dla cyberbezpieczeństwa oraz wdrożonych procesów zarządzania tym ryzykiem.

- **Poziom 1: Podstawy**
  - **Proces zarządzania ryzykiem**: organizacyjne praktyki zarządzania ryzykiem dla cyberbezpieczeństwa nie są sformalizowane, a ryzykiem zarządza się w sposób doraźny, a czasem reaktywny;
  - **Zintegrowany program zarządzania ryzykiem**: znajomość ryzyka dla cyberbezpieczeństwa na poziomie organizacyjnym jest ograniczona. Organizacja wdraża zarządzanie ryzykiem dla cyberbezpieczeństwa w sposób nieregularny i jednostkowy, może przy tym nie posiadać procesów umożliwiających wymianę informacji na temat cyberbezpieczeństwa w ramach organizacji;
  - **Partycypacja zewnętrzna**: organizacja nie rozumie swojej roli w szerzej pojętym ekosystemie w odniesieniu do jego elementów, od których jest zależna, lub które są zależne od niej. Organizacja zasadniczo nie jest świadoma zagrożeń związanych z cybernetycznym łańcuchem dostaw produktów i usług, które dostarcza i wykorzystuje;
- **Poziom 2: Znajomość ryzyka**
  - **Proces zarządzania ryzykiem**: praktyki zarządzania ryzykiem zostały zatwierdzone przez kierownictwo, ale mogły nie zostać ugruntowane jako polityka obowiązująca w całej organizacji;
  - **Zintegrowany program zarządzania ryzykiem**: istnieje znajomość ryzyka dla cyberbezpieczeństwa na poziomie organizacyjnym, ale nie wprowadzono podejścia do zarządzania ryzykiem dla cyberbezpieczeństwa obowiązującego w

całej organizacji. Ocena cyberryzyka dla zasobów organizacyjnych i zewnętrznych jest przeprowadzana, ale z reguły nie jest powtarzalna ani regularna;
- **Partycypacja zewnętrzna**: zasadniczo organizacja rozumie swoją rolę w szerzej pojętym ekosystemie albo w odniesieniu do jego elementów, od których jest zależna, albo w odniesieniu do jego elementów, które są zależne od niej. Ponadto organizacja jest świadoma zagrożeń związanych z cybernetycznym łańcuchem dostaw produktów i usług, które dostarcza i wykorzystuje, ale nie podejmuje konsekwentnych lub formalnych działań w odpowiedzi;

- **Poziom 3: Powtarzalność**
  - **Proces zarządzania ryzykiem**: praktyki organizacji w zakresie zarządzania ryzykiem są formalnie zatwierdzone i ujęte w formie polityki. Organizacyjne praktyki w zakresie cyberbezpieczeństwa są regularnie modyfikowane na podstawie stosowanych procesów zarządzania ryzykiem do zmian wymogów biznesowych/wymogów misji oraz zmieniającego się krajobrazu zagrożeń i technologii;
  - **Zintegrowany program zarządzania ryzykiem**: istnieje podejście do zarządzania ryzykiem dla cyberbezpieczeństwa obowiązujące w całej organizacji. Polityki, procesy i procedury oparte na analizie ryzyka są określone, wdrażane zgodnie z planem i poddawane przeglądom. Kadra kierownicza wyższego szczebla dba o to, żeby cyberbezpieczeństwo było uwzględniane we wszystkich kierunkach działania organizacji;
  - **Partycypacja zewnętrzna**: organizacja rozumie swoją rolę, elementy, od których jest zależna oraz elementy, które są od niej zależne w szerzej pojętym ekosystemie i może przyczyniać się do lepszego poznania zagrożeń przez społeczność. Organizacja jest świadoma zagrożeń związanych z cybernetycznym łańcuchem dostaw produktów i usług, które dostarcza i wykorzystuje;
- **Poziom 4: Zdolność adaptacji**
  - **Proces zarządzania ryzykiem**: organizacja modyfikuje swoje praktyki w zakresie cyberbezpieczeństwa na podstawie wcześniejszych i bieżących działań w zakresie cyberbezpieczeństwa, w tym zdobytych doświadczeń i wskaźników predyktywnych;
  - **Zintegrowany program zarządzania ryzykiem**: istnieje podejście do zarządzania ryzykiem dla cyberbezpieczeństwa obowiązujące w całej organizacji, w którym polityki, procesy i procedury oparte na analizie ryzyka są wykorzystywane do reagowania na potencjalne zdarzenia związane z cyberbezpieczeństwem; oraz
  - **Partycypacja zewnętrzna**: organizacja rozumie swoją rolę, elementy, od których jest zależna oraz elementy, które są od niej zależne w szerzej pojętym ekosystemie i przyczynia się do lepszego poznania zagrożeń przez społeczność.

Metoda oceny

Ramy na rzecz poprawy cyberbezpieczeństwa infrastruktury krytycznej mają służyć organizacjom do przeprowadzania samooceny ryzyka, tak aby uczynić ich podejście do cyberbezpieczeństwa i inwestycje w cyberbezpieczeństwo bardziej racjonalnymi, efektywnymi i wartościowymi. Aby móc ocenić efektywność inwestycji, organizacja musi najpierw zadbać o to, aby jej cele organizacyjne i zależności między tymi celami a pozytywnymi rezultatami w zakresie cyberbezpieczeństwa były dokładnie zrozumiane. Rezultaty stosowania rdzenia ram w zakresie cyberbezpieczeństwa ułatwiają przeprowadzanie samooceny efektywności inwestycji i działań w zakresie cyberbezpieczeństwa.

A.4 Katarski model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Qatar Cybersecurity Capability Maturity Model, Q-C2M2)

Katarski model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Q-C2M2) został opracowany przez Kolegium Prawa Uniwersytetu w Katarze w 2018 r. Model Q-C2M2 opiera się na różnych istniejących modelach służących tworzeniu kompleksowej metodologii oceny w celu wzmocnienia ram cyberbezpieczeństwa Kataru.

Atrybuty/ wymiary

W modelu Q-C2M2 przyjęto podejście przewidziane w ramach opracowanych przez Narodowy Instytut Standaryzacji i Technologii (NIST), polegające na stosowaniu pięciu podstawowych funkcji jako głównych dziedzin modelu. Pięć podstawowych funkcji ma zastosowanie w kontekście Kataru, ponieważ są to funkcje wspólne dla wszystkich sektorów infrastruktury krytycznej, które stanowią ważny element ram cyberbezpieczeństwa Kataru. Model Q-C2M2 opiera się na **pięciu dziedzinach**, z których każda została dodatkowo podzielona na kilka **poddziedzin**, aby objąć pełny zakres dojrzałości zdolności w zakresie cyberbezpieczeństwa.

Poniżej przedstawiono szczegółowo pięć poddziedzin modelu:

i **Dziedzina „Zrozumienie”** obejmuje cztery poddomeny: cyberzarządzanie, aktywa, ryzyko i szkolenia;
ii Do **dziedziny „Zabezpieczanie”** należą poddziedziny bezpieczeństwa danych, bezpieczeństwa technologii, bezpieczeństwa kontroli dostępu, bezpieczeństwa komunikacji i bezpieczeństwa personelu;
iii Do **dziedziny „Wykrywanie”** należą poddziedziny monitorowania, zarządzania incydentami, wykrywania incydentów, ich analizy i narażenia na incydenty;
iv **Dziedzina „Reagowanie”** obejmuje planowanie reakcji, łagodzenie skutków i komunikację w związku z reagowaniem na incydenty;
v **Dziedzina „Utrzymanie”** obejmuje planowanie przywracania, zarządzanie ciągłością działania, doskonalenie i zależności zewnętrzne.

Poziomy dojrzałości

W Q-C2M2 wyróżnia się **5 poziomów dojrzałości**, które mierzą dojrzałość zdolności podmiotu państwowego lub organizacji niepaństwowej na poziomie podstawowych funkcji. Poziomy te mają na celu ocenę dojrzałości w pięciu dziedzinach wymienionych w poprzednim punkcie.

- **Inicjowanie**: Stosowanie doraźnych praktyk i procesów w zakresie cyberbezpieczeństwa w niektórych dziedzinach;
- **Wdrożenie**: Przyjęto polityki mające na celu wdrożenie wszystkich działań w zakresie cyberbezpieczeństwa w ramach dziedzin w celu zakończenia ich wdrażania w określonym czasie;
- **Rozwijanie**: Wdrożono polityki i praktyki mające na celu opracowywanie i udoskonalanie działań w zakresie cyberbezpieczeństwa w ramach dziedzin z myślą o proponowaniu nowych działań do wdrożenia;
- **Zdolność adaptacji**: Rewidowanie i weryfikowanie działań w zakresie cyberbezpieczeństwa oraz przyjmowanie praktyk opartych na wskaźnikach predyktywnych wynikających z wcześniejszych doświadczeń i zastosowanych środków; oraz
- **Sprawność**: Dalsze praktykowanie etapu zdolności adaptacji, ale ze szczególnym naciskiem na sprawność i szybkość wdrażania działań w dziedzinach.

Metoda oceny

Model Q-C2M2 znajduje się na wczesnym etapie badań i nie został jeszcze dopracowany w stopniu umożliwiającym jego wdrożenie. Są to ramy, które można wykorzystać do wdrożenia szczegółowego modelu oceny dla katarskich organizacji w przyszłości.

A.5 Certyfikacja modelu dojrzałości cyberbezpieczeństwa (Cybersecurity Maturity Model Certification, CMMC)

Certyfikacja modelu dojrzałości cyberbezpieczeństwa (CMMC) została opracowana przez Departament Obrony Stanów Zjednoczonych (DoD) we współpracy z Uniwersytetem Carnegie Mellon i Laboratorium Fizyki Stosowanej Uniwersytetu Johnsa Hopkinsa. Głównym zadaniem DoD przy projektowaniu tego modelu jest ochrona informacji pochodzących z sektora bazy przemysłu obronnego (DIB). Informacje stanowiące przedmiot zainteresowania CMMC są klasyfikowane jako „informacje o zamówieniach federalnych” (Federal Contract Information),

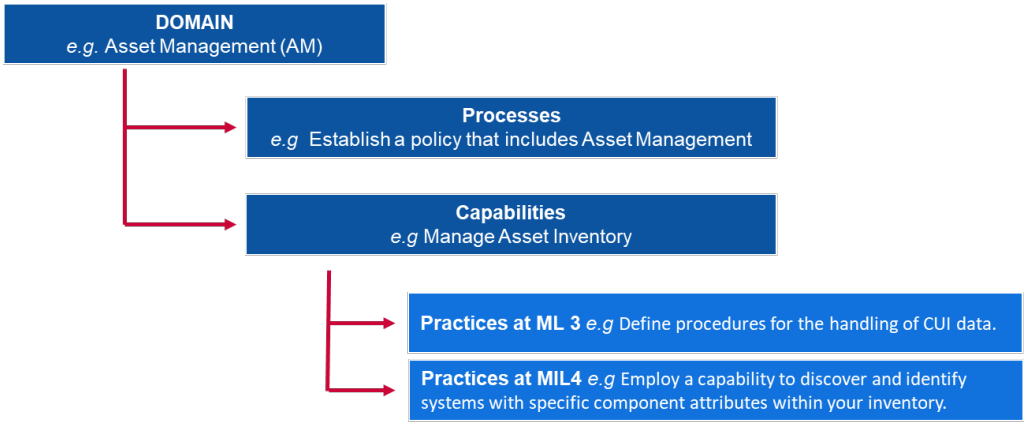
czyli informacje dostarczane przez rząd lub generowane na jego potrzeby w ramach zamówień, które nie są ujawniane publicznie, bądź jako „kontrolowane informacje jawne", które wymagają zabezpieczenia lub kontroli rozpowszechniania zgodnie z przepisami ustawowymi i wykonawczymi oraz polityką ogólnorządową. Model CMMC umożliwia pomiar dojrzałości w zakresie cyberbezpieczeństwa i zapewnia najlepsze praktyki wraz z elementem certyfikacyjnym w celu wdrożenia praktyk związanych z poszczególnymi poziomami dojrzałości. Najnowsza wersja modelu CMMC została opublikowana w 2020 r.

Atrybuty/ wymiary

W modelu CMMC uwzględniono **siedemnaście dziedzin** odpowiadających grupom procesów i zdolności w zakresie cyberbezpieczeństwa. Każda dziedzina została następnie podzielona na wiele **procesów**, które dla wszystkich dziedzin są podobne; a także na jedną lub więcej **zdolności** znajdujących się na pięciu poziomach dojrzałości. Zdolności (lub zdolność) zostały następnie uszczegółowione w postaci **praktyk** odpowiadających poszczególnym poziomom dojrzałości.

Między tymi pojęciami istnieje następujący związek:

Rys. 9: Przykładowe wskaźniki CMMC



DOMAIN e.g. Asset Management (AM)
Processes
e.g Establish a policy that includes Asset Management
Capabilities
e.g Manage Asset Inventory
Practices at ML 3 e.g Define procedures for the handling of CUI data
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory

DZIEDZINA np. zarządzanie aktywami (AM)
Procesy
np. ustanowienie polityki obejmującej zarządzanie aktywami
Zdolności
np. zarządzanie wykazem aktywów
Praktyki dla MIL 3 np. określenie procedur postępowania z danymi CUI
Praktyki dla MIL4 np. wprowadzenie zdolności umożliwiającej odkrywanie i identyfikację systemów o określonych atrybutach składowych w wykazie

Poniżej przedstawiono szczegółowo siedemnaście dziedzin modelu:

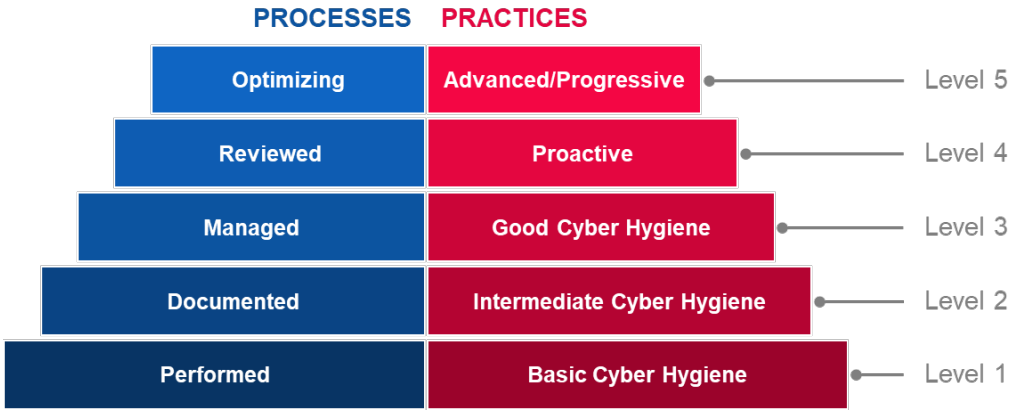
i Kontrola dostępu (AC);
ii Zarządzanie aktywami (AM);
iii Audyt i rozliczalność (AU);
iv Wiedza i szkolenia (AT);
v Zarządzanie konfiguracją (CM);
vi Identyfikacja i uwierzytelnianie (IA);
vii Reagowanie na incydenty (IR);
viii Utrzymanie (MA);
ix Ochrona nośników (MP);
x Bezpieczeństwo osobowe (PS);
xi Ochrona fizyczna (PE);
xii Przywracanie (RE);
xiii Zarządzanie ryzykiem (RM);
xiv Ocena bezpieczeństwa (CA);

xv Orientacja sytuacyjna (SA);
xvi Ochrona systemów i łączności (SC); oraz
xvii Integralność systemów i informacji (SI).

Poziomy dojrzałości

W CMMC wyróżniono **5 poziomów dojrzałości** określanych w oparciu o procesy i praktyki. Aby osiągnąć określony poziom dojrzałości w modelu CMMC, organizacja musi spełnić warunki konieczne dotyczące procesów i praktyk dla tego szczebla. Oznacza to także spełnienie warunków koniecznych dla wszystkich szczebli poniżej.

Rys. 10: Poziomy dojrzałości w modelu CMMC



PROCESSES	PROCESY
Optimizing	Optymalizacja
Reviewed	Weryfikowane
Managed	Zarządzane
Documented	Udokumentowane
Performed	Wykonywane
PRACTICES	PRAKTYKI
Advanced/Progressive	Zaawansowane/postępowe
Proactive	Proaktywne
Good Cyber Hygiene	Dobra cyberhigiena
Intermediate Cyber Hygiene	Umiarkowana cyberhigiena
Basic Cyber Hygiene	Podstawowa cyberhigiena
Level 5	Poziom 5
Level 4	Poziom 4
Level 3	Poziom 3
Level 2	Poziom 2
Level 1	Poziom 1

- **Poziom 1**
  - **Procesy – wykonywane**: ze względu na to, że organizacja może być w stanie stosować te praktyki jedynie doraźnie i może, ale nie musi opierać się na dokumentacji. Dla poziomu 1 nie ocenia się dojrzałości procesów;
  - **Praktyki – podstawowa cyberhigiena**: poziom 1 koncentruje się na ochronie informacji FCI (informacji o zamówieniach federalnych) i obejmuje wyłącznie praktyki, które odpowiadają podstawowym wymogom ochrony;
- **Poziom 2**
  - **Procesy – udokumentowane**: poziom 2 wymaga, aby organizacja ustanowiła i udokumentowała praktyki i polityki wskazujące kierunki realizacji działań związanych z modelem CMMC. Udokumentowanie praktyk umożliwia wykonywanie ich w powtarzalny sposób. Dojrzałe zdolności powstają w organizacjach dzięki dokumentowaniu procesów, a następnie realizowaniu ich zgodnie z dokumentacją;
  - **Praktyki – umiarkowana cyberhigiena**: poziom 2 to etap przejściowy między poziomem 1 a poziomem 3, składający się z podzbioru wymogów bezpieczeństwa

określonych w NIST SP 800-171 oraz praktyk zaczerpniętych z innych norm i źródeł;

- **Poziom 3**
  - **Procesy – zarządzane**: poziom 3 wymaga, aby organizacja ustanowiła i utrzymywała plan mówiący o sposobie zarządzania działaniami służącymi wdrażaniu praktyk oraz zapewniała zasoby jego realizacji. Plan może zawierać informacje na temat misji, celów, planów dotyczących projektów, zapewnienia zasobów, wymaganych szkoleń i zaangażowania odpowiednich zainteresowanych stron;
  - **Praktyki – dobra cyberhigiena**: poziom 3 dotyczy ochrony informacji CUI i obejmuje wszystkie wymogi bezpieczeństwa określone w NIST SP 800-171 oraz dodatkowe praktyki zaczerpnięte z innych norm i źródeł, mające na celu ograniczanie zagrożeń;
- **Poziom 4**
  - **Procesy – weryfikowane**: poziom 4 wymaga, aby organizacja dokonywała przeglądów i pomiarów praktyk pod kątem ich efektywności. Poza pomiarem praktyk pod kątem ich efektywności, organizacje, które osiągnęły ten poziom, są w stanie w razie potrzeby podejmować działania naprawcze i regularnie informować kierownictwo wyższego szczebla o sytuacji lub problemach;
  - **Praktyki – proaktywne:**: poziom 4 skupia się na ochronie informacji CUI (kontrolowanych informacji jawnych) i obejmuje podzbiór zaostrzonych wymogów w zakresie bezpieczeństwa. Praktyki te zwiększają zdolności organizacji w zakresie wykrywania i reagowania w celu odpowiadania na zmieniające się taktyki, techniki i procedury oraz dostosowywania się do nich;
- **Poziom 5**
  - **Procesy – optymalizacja**: poziom 5 wymaga od organizacji ujednolicenia i optymalizacji wdrożenia procesów w całej organizacji; oraz
  - **Praktyki – zaawansowane/proaktywne**: poziom 5 skupia się na ochronie informacji CUI. Dodatkowe praktyki pogłębiają zdolności w zakresie cyberbezpieczeństwa i zwiększają ich stopień zaawansowania.

Metoda oceny

CMMC jest stosunkowo nowym modelem, ukończonym w pierwszym kwartale 2020 r. Jak dotąd nie został wdrożony w żadnej organizacji. Niemniej jednak wykonawcy pracujący dla DoD przewidują, że będą zlecali przeprowadzanie audytów certyfikowanym kontrolerom zewnętrznym. DoD oczekuje od swoich wykonawców wdrożenia najlepszych praktyk w celu wspierania cyberbezpieczeństwa i ochrony informacji szczególnie chronionych.

A.6 Społecznościowy model dojrzałości cyberbezpieczeństwa (CCSMM)

Społecznościowy model dojrzałości cyberbezpieczeństwa (CCSMM) został stworzony przez Centre for Infrastructure Assurance and Security na Uniwersytecie Teksańskim. Celem modelu CCSMM jest dookreślenie metod służących ustalaniu aktualnego statusu społeczności w zakresie gotowości cybernetycznej oraz zapewnienie planu działania dla społeczności, którym będą się one mogły kierować podczas prac przygotowawczych. Społeczności, do których skierowany jest model CCSMM, to głównie samorządy lokalne i władze państwowe. Model CCSMM powstał w 2007 r.

Atrybuty/ wymiary

Poziomy dojrzałości są określane według **sześciu głównych wymiarów**, które obejmują różne aspekty cyberbezpieczeństwa w społecznościach i organizacjach. Wymiary te zostały jasno określone dla każdego poziomu dojrzałości (szczegółowe przedstawienie na Rys. 11: Podsumowanie wymiarów CCSMM). Tych sześć wymiarów to:

i Uwzględnione zagrożenia;
ii Mierniki;
iii Wymiana informacji;

iv Technologia;
v Szkolenia; oraz
vi Test.

Poziomy dojrzałości

CCSMM opiera się na **pięciu poziomach dojrzałości** uzależnionych od głównych rodzajów zagrożeń oraz działań podejmowanych na danym poziomie:

- **Poziom 1: Świadomość w zakresie bezpieczeństwa**
  Głównym tematem działań na tym poziomie jest uświadamianie osobom fizycznym i organizacjom zagrożeń, problemów i tematów związanych z cyberbezpieczeństwem;
- **Poziom 2: Rozwój procesów**
  Poziom mający pomagać społecznościom w ustanawianiu i udoskonalaniu procesów bezpieczeństwa niezbędnych do skutecznego rozwiązywania problemów związanych z cyberbezpieczeństwem;
- **Poziom 3: Zasobność w informacje**
  Poziom mający na celu usprawnienie mechanizmów wymiany informacji w obrębie społeczności, aby umożliwić jej efektywne korelowanie pozornie niezwiązanych ze sobą informacji.
- **Poziom 4: Opracowanie taktyki**
  Elementy tego poziomu mają na celu opracowanie lepszych i bardziej proaktywnych metod wykrywania ataków i reagowania na nie. Na tym poziomie powinna już zostać wprowadzona większość metod zapobiegawczych.
- **Poziom 5: Pełna zdolność operacyjna w zakresie bezpieczeństwa**
  Ten poziom przedstawia elementy, które powinny występować w organizacji, żeby mogła uznawać się za w pełni przygotowaną operacyjnie do reagowania na wszelkiego rodzaju cyberzagrożenia.

Rys. 11: Podsumowanie wymiarów CCSMM na poszczególnych poziomach

	Level 1 Security Aware	Level 2 Process Development	Level 3 Information Enabled	Level 4 Tactics Development	Level 5 Full Security Operational Capability
Threats Addressed	Unstructured	Unstructured	Structured	Structured	Highly Structured
Metrics	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens
Information Sharing	Information Sharing Committee	Community Security Web Site	Information Correlation Center	State/Fed Correlation	Complete Info Vision
Technology	Rosters, GETS, Access Controls, Encryption	Secure Web Site Firewalls, Backups	Event Correlation SW IDS/IPS	24/7 manned operations	Automated Operations
Training	1-day Community Seminar	Conducting a CCSE	Vulnerability Assessments	Operational Security	Multi-Discipline Red Teaming
Test	Dark Screen - EOC	Community Dark Screen	Operational Dark Screen	Limited Black Demon	Black Demon

Level 1
Security Aware
Level 2
Process Development
Level 3
Information Enabled

Poziom 1
Świadomość w zakresie bezpieczeństwa
Poziom 2
Rozwój procesów
Poziom 3
Zasobność w informacje

Level 4	Poziom 4
Tactics Development	Opracowanie taktyki
Level 5	Poziom 5
Full Security Operational Capability	Pełna zdolność operacyjna w zakresie bezpieczeństwa
Threats Addressed	Uwzględnione zagrożenia
Metrics	Mierniki
Information sharing	Wymiana informacji
Technology	Technologia
Training	Szkolenia
Test	Test
Unstructured	Nieusystematyzowane
Governement	Władze
Industry	Przemysł
Citizens	Obywatele
Information Sharing Committee	Komitet ds. wymiany informacji
Rosters, GETS, Assess Controls, Encryption	Wykazy, GETS, kontrola dostępu, szyfrowanie
1-dat Community Seminar	Jednodniowe seminarium dla społeczności
Dark Screen – EOC	Dark Screen – EOC
Unstructured	Nieusystematyzowane
Governement	Władze
Industry	Przemysł
Citizens	Obywatele
Community Security Web site	Strona internetowa społeczności poświęcona bezpieczeństwu
Secure Web Site Firewalls, Backups	Bezpieczne zapory sieciowe dla stron internetowych, kopie zapasowe
Conudcting a CCSE	Przeprowadzanie CCSE
Community Dark Screen	Community Dark Screen
Structured	Usystematyzowane
Governement	Władze
Industry	Przemysł
Citizens	Obywatele
Information Correlation Center	Centrum korelacji informacji
Event Correlation SW IDS/IPS	Korelacja zdarzeń SW IDS/IPS
Vulnerability Assessment	Ocena podatności
Operational Dark Screen	Operational Dark Screen
Structured	Usystematyzowane
Governement	Władze
Industry	Przemysł
Citizens	Obywatele
State/Fed Correlation	Korelacja stanowa/federalna
24/7 manned operations	Personel pracujący przez całą dobę, 7 dni w tygodniu
Operational Security	Bezpieczeństwo operacyjne
Limited Black Demon	Limited Black Demon
Highly Structured	Wysoceusystematyzowany
Complete Info	Pełna wizja
Vision	informacji
Automated	Operacje
Operations	zautomatyzowane
Multi-Discipline	Wielodyscyplinarny
Red	red
Teaming	teaming
Black Demon	Black Demon

Metoda oceny

CCSMM jako metodologia oceny ma zostać wdrożona przez społeczności z udziałem państwowych i federalnych organów ścigania. Jej celem jest pomóc społeczności w określeniu najważniejszych zagadnień, najbardziej prawdopodobnych celów ataków, a także elementów, które należy objąć ochroną (oraz zakresu tej ochrony). Mając na uwadze te cele, można opracować plany służące doprowadzeniu poszczególnych aspektów społeczności do wymaganego poziomu dojrzałości w zakresie cyberbezpieczeństwa. Szczególne dane generowane przez CCSMM pomagają określić cele różnych testów i ćwiczeń, które można wykorzystać do pomiaru skuteczności wprowadzonych programów.

A.7 Model dojrzałości bezpieczeństwa informacji na potrzeby ram cyberbezpieczeństwa NIST (Information Security Maturity Model for NIST Cyber Security Framework, ISMM)

Model dojrzałości bezpieczeństwa informacji (ISMM) został opracowany w Kolegium Nauk Komputerowych i Inżynierii Uniwersytetu Ropy i Minerałów im. Króla Fahda w Arabii Saudyjskiej. Zaproponowano w nim nowy model dojrzałości zdolności służący do oceny

wdrażania środków w zakresie cyberbezpieczeństwa. Model ISMM ma na celu umożliwienie organizacjom oceny postępów wdrożeń w czasie za pomocą tego samego narzędzia pomiarowego w celu zapewnienia utrzymania pożądanego stanu cyberbezpieczeństwa. ISMM opracowano w 2017 r.

Atrybuty/ wymiary

ISMM opiera się na poddanych dotychczas ocenie obszarach ram NIST, przy czym dodano do niego wymiar oceny zgodności. Dzięki temu model został poszerzony do **23 obszarów podlegających ocenie** pod kątem stanu cyberbezpieczeństwa w organizacji. Do 23 obszarów podlegających ocenie należą:

i Zarządzanie aktywami;
ii Otoczenie biznesu;
iii Zarządzanie;
iv Ocena ryzyka;
v Strategia zarządzania ryzykiem;
vi Ocena zgodności;
vii Kontrola dostępu;
viii Świadomość i szkolenia;
ix Bezpieczeństwo danych;
x Procesy i procedury ochrony informacji;
xi Utrzymanie;
xii Technologia ochronna;
xiii Anomalie i zdarzenia;
xiv Stałe monitorowanie bezpieczeństwa;
xv Procesy detekcji;
xvi Planowanie reakcji;
xvii Komunikacja w związku z reagowaniem na incydenty;
xviii Analiza reagowania;
xix Łagodzenie reagowania;
xx Doskonalenie reagowania;
xxi Planowanie przywracania;
xxii Doskonalenie procesów przywracania; oraz
xxiii Komunikacja w ramach przywracania.

Poziomy dojrzałości

ISMM opiera się na **pięciu poziomach dojrzałości**, które niestety nie zostały szczegółowo omówione w dostępnej dokumentacji.

- **Poziom 1:** Proces realizowany;
- **Poziom 2:** Proces zarządzany;
- **Poziom 3:** Proces ugruntowany;
- **Poziom 4:** Proces przewidywalny; oraz
- **Poziom 5:** Optymalizacja procesu.

Metoda oceny

ISMM nie proponuje żadnej konkretnej metodologii przeprowadzania oceny w odniesieniu do organizacji.

A.8 Model audytu wewnętrznego (IA-CM) dla sektora publicznego (Internal Audit Capability Model (IA-CM) for the Public Sector)

Model audytu wewnętrznego (IA-CM) został opracowany przez Institute of Internal Auditors Research Foundation z myślą o budowaniu zdolności i rzecznictwa w drodze samooceny przeprowadzanej w sektorze publicznym. Model IA-CM jest skierowany do zawodowych audytorów i zawiera omówienie samego modelu oraz wytyczne do jego stosowania, które pomagają w posługiwaniu się nim jako narzędziem samooceny.

Mimo że model IA-CM koncentruje się na zdolnościach w zakresie audytu wewnętrznego, a nie na budowaniu zdolności w zakresie cyberbezpieczeństwa, został on opracowany jako narzędzie samooceny dojrzałości dla podmiotów sektora publicznego, które można stosować na całym świecie do udoskonalania procesów i zwiększania efektywności. Ponieważ zakres tego modelu nie koncentruje się na cyberbezpieczeństwie, jego atrybuty nie zostaną przeanalizowane. Model IA-CM został ukończony w 2009 r.

Poziomy dojrzałości

Model audytu wewnętrznego (IA-CM) obejmuje **pięć poziomów dojrzałości**, z których każdy opisuje cechy i zdolności funkcji audytu wewnętrznego na danym poziomie. Poziomy zdolności w modelu stanowią plan działania na rzecz ciągłego doskonalenia.

- **Poziom 1: Początkowy**
  Brak trwałych i powtarzalnych zdolności – zależny od działań podejmowanych indywidualnie
  - Doraźny lub nieusystematyzowany.
  - Sporadyczne pojedyncze audyty lub przeglądy dokumentów i transakcji pod kątem poprawności i zgodności.
  - Wyniki uzależnione od umiejętności konkretnej osoby zajmującej dane stanowisko.
  - Nie wprowadzono żadnych zasad praktyki zawodowej poza zasadami udostępnianymi przez stowarzyszenia zawodowe.
  - Zatwierdzanie finansowania przez kierownictwo, stosownie do potrzeb.
  - Brak infrastruktury.
  - Audytorzy najczęściej wchodzą w skład większej jednostki organizacyjnej.
  - Nie powstały żadne zdolności instytucjonalne.
- **Poziom 2: Infrastruktura**
  Trwałe i powtarzalne praktyki i procedury
  - Kluczową kwestią lub wyzwaniem dla poziomu 2 jest sposób zapewnienia i utrzymania powtarzalności procesów, a tym samym powtarzalnej zdolności.
  - Pojawiają się zależności w zakresie sprawozdawczości z audytu wewnętrznego, infrastruktura zarządcza i administracyjna oraz zasady i procesy praktyki zawodowej (wytyczne w zakresie audytu wewnętrznego, procesy i procedury).
  - Planowanie audytów oparte jest głównie na priorytetach kierownictwa.
  - Ciągłe opieranie się zasadniczo na umiejętnościach i kompetencjach konkretnych osób.
  - Częściowa zgodność z normami.
- **Poziom 3: Integracja**
  Jednolite stosowanie praktyki zarządzania i zasad praktyki zawodowej
  - Polityki, procesy i procedury audytu wewnętrznego są zdefiniowane, udokumentowane i zintegrowane ze sobą oraz z infrastrukturą organizacji.
  - Praktyka zarządzania i zasady praktyki zawodowej w zakresie audytu wewnętrznego są dobrze ugruntowane i jednolicie stosowane w ramach całej funkcji audytu wewnętrznego.
  - Audyt wewnętrzny zaczyna być dostosowywany do działalności organizacji i do związanego z nią ryzyka.
  - W audycie zewnętrznym zachodzą zmiany, w wyniku których odchodzi się od przeprowadzania wyłącznie tradycyjnego audytu wewnętrznego, zamiast tego audyt wewnętrzny integruje się z resztą zespołu i udziela porad dotyczących efektywności i zarządzania ryzykiem.
  - Nacisk kładzie się na integrację zespołu i zdolność funkcji audytu wewnętrznego, a także jej niezależność i obiektywizm.
  - Zasadniczo zapewniona jest zgodność z normami.
- **Poziom 4: Zarządzanie**
  Scalanie informacji pochodzących z całej organizacji w celu udoskonalania zarządzania organizacją i ryzykiem
  - Oczekiwania audytu wewnętrznego i głównych zainteresowanych stron są zbieżne.
  - Istnieją wskaźniki efektywności umożliwiające pomiar oraz monitorowanie procesów i wyników audytu wewnętrznego.
  - Uznaje się, że audyt wewnętrzny wnosi znaczący wkład w organizację.

- Audyt wewnętrzny funkcjonuje jako integralna część zarządzania organizacją i ryzykiem w organizacji.
- Audyt wewnętrzny to dobrze zarządzana komórka organizacyjna.
- Pomiar ryzyka i zarządzanie ryzykiem prowadzone są w ujęciu ilościowym.
- Zapewnione zostały wymagane umiejętności i kompetencje, a także możliwość ich odnawiania i dzielenia się wiedzą (w ramach audytu wewnętrznego i w całej organizacji).

▶ **Poziom 5: Optymalizacja**

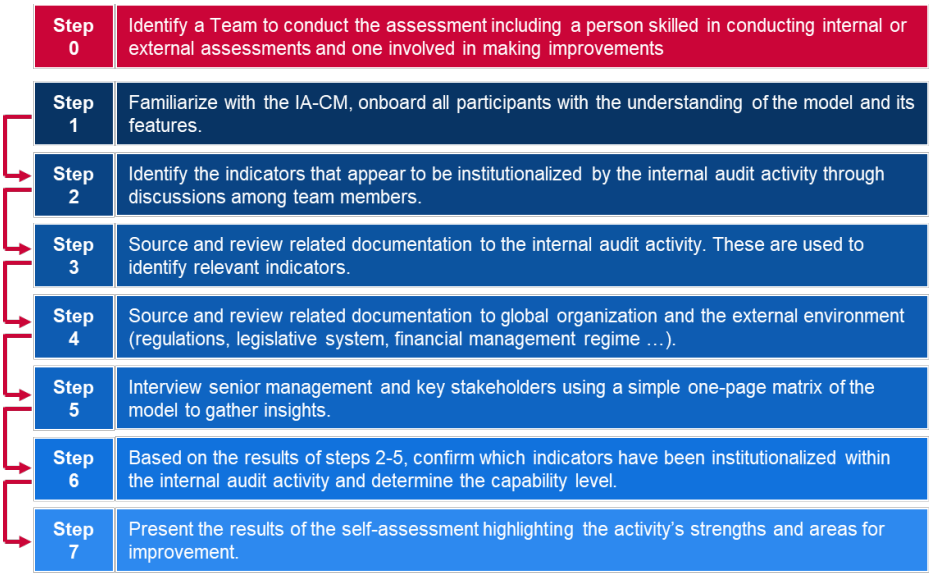
Uczenie się wewnątrz i na zewnątrz organizacji w celu ciągłego doskonalenia

- Audyt wewnętrzny jest organizacją uczącą się, w której procesy podlegają ciągłemu doskonaleniu oraz pojawiają się innowacje.
- W ramach audytu wewnętrznego wykorzystuje się informacje pochodzące z organizacji i spoza niej, aby przyczynić się do realizacji strategicznych celów.
- Wyniki odpowiadające poziomowi światowemu/zaleceniom/najlepszym praktykom.
- Audyt wewnętrzny stanowi krytyczny element struktury zarządzania organizacji.
- Kwalifikacje zawodowe i specjalistyczne na najwyższym poziomie.
- Indywidualne, działowe i organizacyjne mierniki efektywności są w pełni zintegrowane w celu
- zwiększania efektywności.

Metoda oceny

Model audytu wewnętrznego został wyraźnie opracowany na potrzeby samooceny. Zawiera on szczegółowy opis kroków, jakie należy podjąć w celu jego zastosowania, a także przykładową prezentację, którą można dostosować do swoich potrzeb. Przed rozpoczęciem samooceny należy powołać specjalny zespół, w tym co najmniej jedną osobę posiadającą kwalifikacje w zakresie przeprowadzania wewnętrznych lub zewnętrznych ocen audytów wewnętrznych oraz jedną osobę, która uczestniczy we wprowadzaniu usprawnień w tym obszarze.

Rys. 12: Etapy samooceny IC-AM



Step 0	Etap 0
Step 1	Etap 1
Step 2	Etap 2
Step 3	Etap 3
Step 4	Etap 4
Step 5	Etap 5
Step 6	Etap 6
Step 7	Etap 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Należy powołać zespół, który będzie przeprowadzał ocenę, w tym osobę posiadającą kwalifikacje w zakresie przeprowadzania ocen wewnętrznych lub zewnętrznych oraz osobę uczestniczącą we wprowadzaniu usprawnień.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Zaznajomienie się z IA-CM, wdrożenie wszystkich uczestników, którzy muszą posiadać wiedzę o modelu i jego cechach.

Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members. Source and review related documentation to the internal audit activity. These are used to identify relevant indicators. Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …). Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights. Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level. Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Określenie wskaźników, które wydają się zinstytucjonalizowane przez funkcję audytu wewnętrznego poprzez dyskusję między członkami zespołu. Pozyskanie i przeprowadzenie przeglądu dokumentacji dotyczącej funkcji audytu wewnętrznego. Jest ona wykorzystywana do określania istotnych wskaźników. Pozyskanie i przeprowadzenie przeglądu dokumentacji dotyczącej całej organizacji i jej otoczenia zewnętrznego (regulacje, system legislacyjny, system zarządzania finansami itp.). Przeprowadzenie rozmów z kadrą kierowniczą wyższego szczebla i kluczowymi zainteresowanymi stronami przy użyciu prostej jednostronicowej matrycy modelu w celu zapoznania się z ich spostrzeżeniami. Potwierdzenie na podstawie wyników etapów 2–5, które wskaźniki zostały zinstytucjonalizowane w ramach funkcji audytu wewnętrznego, a także określenie poziomu zdolności. Przedstawienie wyników samooceny ze szczególnym uwzględnieniem mocnych stron funkcji i obszarów wymagających poprawy.

A.9 Globalny indeks cyberbezpieczeństwa (Global Cybersecurity Index, GCI)

Globalny indeks cyberbezpieczeństwa (GCI) to inicjatywa Międzynarodowego Związku Telekomunikacyjnego (ITU), której celem jest dokonanie przeglądu zaangażowania i sytuacji w zakresie cyberbezpieczeństwa we wszystkich regionach działania ITU: w Afryce, Ameryce Północnej i Południowej, państwach arabskich, regionie Azji i Pacyfiku, WNP i Europie, a także wyróżnienie państw o dużym zaangażowaniu, stosujących godne polecenia praktyki. Celem GCI jest pomoc państwom we wskazaniu obszarów wymagających poprawy w dziedzinie cyberbezpieczeństwa, a także zachęcenie ich do podejmowania działań mających na celu poprawę ich pozycji w rankingu, co przyczyni się do podniesienia ogólnego poziomu cyberbezpieczeństwa na całym świecie.

Ponieważ GCI jest indeksem, a nie modelem dojrzałości, nie wykorzystuje się w nim poziomów dojrzałości, tylko punktację, która umożliwia uszeregowanie i porównanie globalnego zaangażowania państw i regionów w dziedzinie cyberbezpieczeństwa.

Atrybuty/ wymiary

Globalny indeks cyberbezpieczeństwa (GCI) opiera się na pięciu filarach globalnego programu na rzecz cyberbezpieczeństwa (Global Security Agenda, GCA). Filary te stanowią pięć indeksów cząstkowych GCI i każdy z nich zawiera zbiór wskaźników. W skład GCI wchodzi następujących pięć filarów i wskaźników:

i **Prawne**: środki opierające się na istnieniu instytucji i ram prawnych związanych z cyberbezpieczeństwem i cyberprzestępczością.
   - Przepisy dotyczące cyberprzestępczości;
   - Regulacje dotyczące cyberbezpieczeństwa; oraz
   - Przepisy dotyczące ograniczenia rozprzestrzeniania spamu.

ii **Techniczne**: Środki opierające się na istnieniu instytucji i ram technicznych związanych z cyberbezpieczeństwem.
   - CERT/CIRT/CSRIT;
   - Ramy wdrażania norm;
   - Organ normalizacyjny;
   - Mechanizmy i zdolności techniczne wprowadzone w celu rozwiązania problemu spamu;
   - Wykorzystanie technologii chmury obliczeniowej do celów cyberbezpieczeństwa; oraz
   - Mechanizmy ochrony dzieci w internecie.

iii **Organizacyjne**: Środki opierające się na istnieniu instytucji i strategii koordynacji polityki na rzecz rozwoju cyberbezpieczeństwa na szczeblu krajowym.
   - Krajowa strategia cyberbezpieczeństwa;
   - Odpowiedzialna agencja; oraz
   - Cyberbezpieczeństwo.

iv **Budowanie zdolności**: Środki opierające się na istnieniu programów badawczo-rozwojowych, edukacyjnych i szkoleniowych, certyfikowanych specjalistów i agencji sektora publicznego wspierających budowanie zdolności.

- Publiczne kampanie informacyjne;
- Ramy certyfikacji i akredytacji specjalistów w dziedzinie cyberbezpieczeństwa;
- Szkolenia zawodowe w dziedzinie cyberbezpieczeństwa;
- Programy edukacyjne lub programy studiów w dziedzinie cyberbezpieczeństwa;
- Programy badawczo-rozwojowe w dziedzinie cyberbezpieczeństwa; oraz
- Mechanizmy zachęt.

v **Współpraca**: Środki opierające się na istnieniu partnerstw, ram współpracy i sieci wymiany informacji.

- Porozumienia dwustronne;
- Umowy wielostronne;
- Udział w forach/stowarzyszeniach międzynarodowych;
- Partnerstwa publiczno-prywatne;
- Partnerstwa międzyagencyjne/wewnątrzagencyjne; oraz
- Najlepsze praktyki.

Metoda oceny

GCI to narzędzie do samooceny opierające się na ankiecie[30] zawierającej pytania dychotomiczne, pytania z odpowiedziami do wyboru oraz pytania otwarte. Wykorzystanie odpowiedzi dychotomicznych pozwala wyeliminować ocenę bazującą na opinii oraz ewentualne preferencje dla określonych rodzajów odpowiedzi. Odpowiedzi do wyboru pozwalają zaoszczędzić czas i umożliwiają dokładniejszą analizę danych. Ponadto uproszczona, dychotomiczna skala umożliwia szybszą i bardziej kompleksową ocenę, ponieważ nie wymaga udzielania długich odpowiedzi, co przyspiesza i usprawnia proces udzielania odpowiedzi i późniejszej oceny. Respondent powinien jedynie potwierdzić obecność lub brak pewnych wskazanych z góry rozwiązań w zakresie cyberbezpieczeństwa. Mechanizm ankiety internetowej wykorzystywany do gromadzenia odpowiedzi i zamieszczania odpowiednich materiałów umożliwia wytypowanie dobrych praktyk i zbioru tematycznych ocen jakościowych przez zespół ekspertów.

Ogólna procedura GCI przebiega w następujący sposób:

- Do wszystkich uczestników wystosowane zostaje zaproszenie, zawierające informacje o inicjatywie i prośbę o wyznaczenie punktu kontaktowego odpowiedzialnego za zgromadzenie wszystkich istotnych danych i wypełnienie internetowej ankiety GCI. Podczas przeprowadzania ankiety internetowej zatwierdzony punkt kontaktowy zostaje oficjalnie poproszony przez ITU o udzielenie odpowiedzi na pytania zawarte w ankiecie;
- Zgromadzenie danych pierwotnych (w przypadku państw, które nie wypełniają ankiety):
  - ITU opracowuje wstępny projekt odpowiedzi na ankietę, wykorzystując publicznie dostępne dane i badania przeprowadzone w internecie;
  - Projekt ankiety zostaje przesłany do punktów kontaktowych w celu dokonania weryfikacji;
  - Punkty kontaktowe poprawiają odpowiedzi, a następnie odsyłają projekt ankiety;
  - Poprawione projekty ankiety zostają przesłane do poszczególnych punktów kontaktowych w celu ostatecznego zatwierdzenia; oraz
  - Zatwierdzona ankieta jest wykorzystywana do analizy, oceny punktowej i klasyfikacji.
- Zgromadzenie danych wtórnych (w przypadku państw, które wypełniają ankietę):
  - ITU wskazuje wszelkie brakujące odpowiedzi, dokumenty pomocnicze, łącza itp.;

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

- Punkt kontaktowy w razie potrzeby poprawia odpowiedzi;
- Poprawione projekty ankiety zostają przesłane do poszczególnych punktów kontaktowych w celu ostatecznego zatwierdzenia; oraz
- Zatwierdzona ankieta jest wykorzystywana do analizy, oceny punktowej i klasyfikacji.

A.10 Indeks potęgi cybernetycznej (Cyber Power Index, CPI)

Indeks potęgi cybernetycznej (CPI) został opracowany w ramach programu badawczego zrealizowanego przez Economist Intelligence Unit, sfinansowanego przez firmę Booz Allen Hamilton w 2011 r. CPI to „dynamiczny model ilościowy i jakościowy, [...] który mierzy określone cechy środowiska cybernetycznego względem czterech czynników potęgi cybernetycznej: ram prawnych i regulacyjnych; kontekstu gospodarczego i społecznego; infrastruktury technologicznej; oraz zastosowania w przemyśle, które obrazuje postęp cyfryzacji najważniejszych gałęzi przemysłu”[31]. Celem indeksu potęgi cybernetycznej jest porównanie zdolności państw grupy G-20 do opierania się cyberatakom oraz wdrażania infrastruktury cyfrowej, która jest niezbędna dla silnej i bezpiecznej gospodarki. Poziom odniesienia określony przez CPI obejmuje 19 państw z grupy G-20 (z wyłączeniem UE). Indeks umożliwia też sporządzenie rankingu państw dla poszczególnych wskaźników.

Atrybuty/ wymiary

Indeks potęgi cybernetycznej (CPI) opiera się na czterech czynnikach potęgi cybernetycznej. Następnie każda kategoria zostaje zmierzona przy użyciu szeregu wskaźników i każdy kraj otrzymuje określoną ocenę punktową. Kategorie i filary indeksu przedstawiają się następująco:

i **Ramy prawne i regulacyjne**
- Zaangażowanie rządu w rozwój cyberprzestrzeni
- Polityka w zakresie ochrony cyberprzestrzeni
- Cenzura w cyberprzestrzeni (lub jej brak)
- Skuteczność polityczna
- Ochrona własności intelektualnej

ii **Kontekst gospodarczy i społeczny**
- Poziomy kształcenia
- Umiejętności techniczne
- Otwartość wymiany handlowej
- Stopień innowacyjności w otoczeniu biznesowym

iii **Infrastruktura technologiczna**
- Dostęp do technologii informacyjno-komunikacyjnych
- Jakość technologii informacyjno-komunikacyjnych
- Przystępność cenowa technologii informacyjno-komunikacyjnych
- Wydatki na technologie informacyjne
- Liczba bezpiecznych serwerów

iv **Zastosowanie w przemyśle**
- Inteligentne sieci
- E-zdrowie
- Handel elektroniczny
- Inteligentny transport
- E-administracja

Metoda oceny

CPI to model ilościowej i jakościowej oceny punktowej. Ocena została przeprowadzona przez The Economist Intelligence Unit z wykorzystaniem wskaźników ilościowych uzyskanych z dostępnych źródeł statystycznych i oszacowań dokonywanych w przypadku braku danych. Dane zaczerpnięto głównie z następujących źródeł: The Economist Intelligence Unit;

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

Organizacja Narodów Zjednoczonych do spraw Oświaty, Nauki i Kultury (UNESCO); Międzynarodowy Związek Telekomunikacyjny (ITU) oraz Bank Światowy.

A.11 Indeks potęgi cybernetycznej (Cyber Power Index, CPI)

Ten punkt zawiera podsumowanie najważniejszych ustaleń analizy istniejących modeli dojrzałości. Tabela 5: Zestawienie modeli dojrzałości objętych **analizą** zawiera przegląd głównych cech charakterystycznych poszczególnych modeli według zmodyfikowanego modelu Beckera. Tabela 6 Porównanie poziomów dojrzałości ogólne definicje poziomów dojrzałości w analizowanych modelach. Tabela 7 zawiera zestawienie wymiarów lub atrybutów zastosowanych w poszczególnych modelach.

Tabela 5: Zestawienie modeli dojrzałości objętych analizą

Nazwa modelu	Instytucja Źródło	Cel	Odbiorcy	Liczba poziomów	Liczba atrybutów	Metoda oceny	Przedstawienie wyników
Model zdolności w zakresie cyberbezpieczeństwa dla państw (Cybersecurity Capacity Maturity Model for Nations, CMM)	Global Cyber Security Capacity Centre Uniwersytet Oksfordzki	Zwiększenie skali i skuteczności budowania zdolności w zakresie cyberbezpieczeństwa na szczeblu międzynarodowym	Kraje	5	5 głównych wymiarów	Współpraca z lokalną organizacją w celu dopracowania modelu przed zastosowaniem go w kontekście krajowym	Pięcioelementowy wykres radarowy
Model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Cybersecurity Capability Maturity Model, C2M2)	Departament Energii Stanów Zjednoczonych (DOE)	Pomaganie organizacjom w ocenie i udoskonalaniu ich programów cyberbezpieczeństwa oraz zwiększaniu ich odporności operacyjnej	Organizacje ze wszystkich sektorów, niezależnie od ich rodzaju i wielkości	4	10 głównych dziedzin	Metodologia i zestaw narzędzi do samooceny	Karta oceny z wykresami kołowymi
Ramy na rzecz poprawy cyberbezpieczeństwa infrastruktury krytycznej (Framework for Improving Critical Infrastructure Cybersecurity)	Narodowy Instytut Standaryzacji i Technologii (NIST)	Ramy mające na celu wyznaczanie kierunków działań w zakresie cyberbezpieczeństwa i zarządzanie ryzykiem w organizacjach	Organizacje	nd. (4 poziomy)	5 podstawowych funkcji	Samoocena	-
Katarski model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Qatar Cybersecurity Capability Maturity Model, Q-C2M2)	Kolegium Prawa Uniwersytetu Katarskiego	Dostarczenie działającego modelu, który można wykorzystać do analizy porównawczej, pomiaru i rozwoju ram cyberbezpieczeństwa Kataru	Organizacje katarskie	5	5 głównych dziedzin	-	-
Certyfikacja modelu dojrzałości cyberbezpieczeństwa (Cybersecurity Maturity Model Certification, CMMC)	Departament Obrony Stanów Zjednoczonych (DOD)	Promowanie najlepszych praktyk w dziedzinie cyberbezpieczeństwa w celu ochrony informacji	Organizacje z sektora bazy przemysłu obronnego (DIB)	5	17 głównych dziedzin	Ocena dokonywana przez audytorów zewnętrznych	-
Społecznościowy model dojrzałości cyberbezpieczeństwa (CCSMM)	Centre for Infrastructure Assurance and Security przy Uniwersytecie Teksańskim	Ustalenie aktualnego statusu społeczności w zakresie gotowości cybernetycznej oraz dostarczenie planu działania dla społeczności, którym będą się one mogły kierować podczas prac przygotowawczych.	Społeczności (samorządy lokalne lub władze państwowe)	5	6 głównych wymiarów	Ocena przeprowadzana wewnątrz społeczności z udziałem państwowych i federalnych organów ścigania	-
Model dojrzałości bezpieczeństwa	Kolegium Nauk Komputerowych i Inżynierii	Umożliwienie organizacjom oceny postępów wdrożeń w czasie w celu	Organizacje	5	23 oceniane obszary	-	-

informacji na potrzeby ram cyberbezpieczeństwa NIST (Information Security Maturity Model for NIST Cybersecurity Framework, ISMM)	Uniwersytet Ropy i Minerałów im. Króla Fahda w Arabii Saudyjskiej	zapewnienia utrzymania przez nie pożądanego stanu cyberbezpieczeństwa					
Model audytu wewnętrznego (IA-CM) dla sektora publicznego (Internal Audit Capability Model (IA-CM) for the Public Sector)	The Institute of Internal Auditors Research Foundation	Budowanie zdolności i rzecznictwa w drodze samooceny przeprowadzanej w sektorze publicznym	Organizacje sektora publicznego	5	6 elementów	Samoocena	-
Globalny indeks cyberbezpieczeństwa (Global Cybersecurity Index, GCI)	Międzynarodowy Związek Telekomunikacyjny (ITU)	Ocena zaangażowania i sytuacji w dziedzinie cyberbezpieczeństwa oraz pomoc państwom w określeniu obszarów wymagających poprawy w dziedzinie cyberbezpieczeństwa	Kraje	nd.	5 filarów	Samoocena	Tabela rankingowa
Indeks potęgi cybernetycznej (Cyber Power Index, CPI)	The Economist Intelligence Unit & Booz Allen Hamilton	Porównanie zdolności państw grupy G-20 do opierania się cyberatakom oraz wdrażania infrastruktury cyfrowej, która jest niezbędna dla silnej i bezpiecznej gospodarki.	Państwa grupy G-20	nd.	4 kategorie	Analiza porównawcza przeprowadzona przez Economist Intelligence Unit	Tabela rankingowa

Tabela 6 Porównanie poziomów dojrzałości

Model	Poziom 1	Poziom 2	Poziom 3	Poziom 4	Poziom 5
Model zdolności w zakresie cyberbezpieczeństwa dla państw (Cybersecurity Capacity Maturity Model for Nations, CMM)	**Etap początkowy** Dojrzałość w zakresie cyberbezpieczeństwa w ogóle nie istnieje lub znajduje się w fazie zalążkowej. Mogą być prowadzone wstępne dyskusje na temat budowania zdolności w zakresie cyberbezpieczeństwa, ale nie podjęto żadnych konkretnych działań. Na tym etapie brak jest jakichkolwiek możliwych do zaobserwowania dowodów.	**Etap formacji** Niektóre cechy poszczególnych aspektów zaczęły się pojawiać i kształtować, ale mogą one mieć charakter doraźny, niezorganizowany, być słabo zdefiniowane lub po prostu „nowe”. Można jednak wyraźnie wykazać, że takie działania są prowadzone.	**Etap ugruntowania** Elementy danego aspektu zostały wprowadzone i funkcjonują. Nie przemyślano jednak dokładnie kwestii względnej alokacji zasobów. Zapadło niewiele decyzji dotyczących kompromisów co do „względnej” wysokości nakładów przeznaczanych na poszczególne elementy tego aspektu. Aspekt ten jest jednak funkcjonalny i zdefiniowany.	**Etap strategiczny** Podjęto decyzje o tym, które części tego aspektu są ważne, a które są mniej istotne dla danej organizacji lub narodu. Etap strategiczny odzwierciedla fakt, że dokonano takich wyborów na podstawie sytuacji danego narodu lub organizacji.	**Etap dynamiczny** Istnieją jasno określone mechanizmy umożliwiające modyfikację strategii w zależności od panujących okoliczności, takich jak technologia stosowana w środowisku zagrożeń, globalny konflikt lub znacząca zmiana w jednym z obszarów zainteresowania (np. cyberprzestępczość lub prywatność). Dynamiczne organizacje opracowały metody umożliwiające bezproblemową zmianę strategii. Na tym etapie charakterystyczne są szybkie podejmowanie decyzji, realokacja zasobów i nieustanne

					obserwowanie zmieniającego się otoczenia.
Model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Cybersecurity Capability Maturity Model, C2M2)	**MIL0** Nie stosuje się żadnych praktyk.	**MIL1** Pierwsze praktyki są stosowane, choć mogą mieć charakter doraźny.	**MIL2** Charakterystyka zarządzania: Praktyki są udokumentowane; Zapewniono odpowiednie zasoby do wsparcia tego procesu; Personel realizujący praktyki posiada odpowiednie kwalifikacje i wiedzę; oraz Dokonano podziału odpowiedzialności i uprawnień w związku z wykonywaniem tych praktyk. Charakterystyka podejścia: Praktyki są bardziej kompletne lub zaawansowane niż w przypadku MIL1.	**MIL3** Charakterystyka zarządzania: Działania są prowadzone zgodnie z polityką (lub innymi wytycznymi organizacyjnymi); Wprowadzono cele dotyczące wyników dla działań w danej dziedzinie i są one monitorowane w celu śledzenia ich realizacji; oraz Udokumentowane praktyki dotyczące działań w danej dziedzinie zostały ujednolicone i udoskonalone w całym przedsiębiorstwie. Charakterystyka podejścia: Praktyki są bardziej kompletne lub zaawansowane niż w przypadku MIL2.	-
Model dojrzałości bezpieczeństwa informacji na potrzeby ram cyberbezpieczeństwa NIST (Information Security Maturity Model for NIST Cyber Security Framework, ISMM)	**Proces realizowany**	**Proces zarządzany**	**Proces ugruntowany**	**Proces przewidywalny**	**Optymalizacja procesu**
Katarski model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Qatar Cybersecurity Capability Maturity Model, Q-C2M2)	**Inicjowanie** Stosowanie doraźnych praktyk i procesów w zakresie cyberbezpieczeństwa w niektórych dziedzinach.	**Rozwijanie** Wdrożono polityki i praktyki mające na celu opracowywanie i udoskonalanie działań w zakresie cyberbezpieczeństwa w ramach dziedzin z myślą o proponowaniu nowych działań do wdrożenia.	**Wdrożenie** Przyjęto polityki mające na celu wdrożenie wszystkich działań w zakresie cyberbezpieczeństwa w ramach dziedzin w celu zakończenia ich wdrażania w określonym czasie.	**Zdolność adaptacji** Rewidowanie i weryfikowanie działań w zakresie cyberbezpieczeństwa oraz przyjmowanie praktyk opartych na wskaźnikach predyktywnych wynikających z wcześniejszych doświadczeń i podjętych środków.	**Sprawność** Dalsze praktykowanie etapu zdolności adaptacji, ale ze szczególnym naciskiem na sprawność i szybkość wdrażania działań w dziedzinach.
Certyfikacja modelu dojrzałości cyberbezpieczeńst	**Procesy: Wykonywane** Ze względu na to, że organizacja może być w stanie stosować te	**Procesy: Udokumentowane** Poziom 2 wymaga, aby organizacja ustanowiła i	**Procesy: Zarządzane** Poziom 3 wymaga, aby organizacja ustanowiła i	**Procesy: Weryfikowane.** Poziom 4 wymaga, aby organizacja dokonywała	**Procesy: Optymalizacja** Poziom 5 wymaga od organizacji ujednolicenia i optymalizacji

wa (Cybersecurity Maturity Model Certification, CMMC)	praktyki jedynie doraźnie i może, ale nie musi opierać się na dokumentacji, na poziomie 1 nie ocenia się dojrzałości procesów. **Praktyki: Podstawowa cyberhigiena** Poziom 1 koncentruje się na ochronie informacji FCI (informacji o zamówieniach federalnych) i obejmuje wyłącznie praktyki, które odpowiadają podstawowym wymogom ochrony.	udokumentowała praktyki i polityki wskazujące kierunki realizacji działań związanych z modelem CMMC. Udokumentowanie praktyk umożliwia ludziom wykonywanie ich w powtarzalny sposób. Dojrzałe zdolności powstają w organizacjach dzięki dokumentowaniu procesów, a następnie realizowaniu ich zgodnie z dokumentacją. **Praktyki: Umiarkowana cyberhigiena** Poziom 2 to etap przejściowy między poziomem 1 a poziomem 3, składający się z podzbioru wymogów bezpieczeństwa określonych w NIST SP 800-171 oraz praktyk zaczerpniętych z innych norm i źródeł.	utrzymywała plan mówiący o sposobie zarządzania działaniami służącymi wdrażaniu praktyk oraz zapewniała zasoby do jego realizacji. Plan może zawierać informacje na temat misji, celów, planów dotyczących projektów, zapewnienia zasobów, wymaganych szkoleń i zaangażowania odpowiednich zainteresowanych stron. **Praktyki: Dobra cyberhigiena**. Poziom 3 dotyczy ochrony informacji CUI (kontrolowanych informacji jawnych) i obejmuje wszystkie wymogi bezpieczeństwa określone w NIST SP 800-171 oraz dodatkowe praktyki zaczerpnięte z innych norm i źródeł, mające na celu ograniczanie zagrożeń.	przeglądów i pomiarów praktyk pod kątem ich skuteczności. Poza pomiarem praktyk pod kątem ich skuteczności, organizacje, które osiągnęły ten poziom, są w stanie w razie potrzeby podejmować działania naprawcze i regularnie informować kierownictwo wyższego szczebla o sytuacji lub problemach. **Praktyki: Proaktywne** Poziom 4 skupia się na ochronie informacji CUI (kontrolowanych informacji jawnych) i obejmuje podzbiór zaostrzonych wymogów w zakresie bezpieczeństwa. Praktyki te zwiększają zdolności organizacji w zakresie wykrywania i reagowania w celu odpowiadania na zmieniające się taktyki, techniki i procedury oraz dostosowywania się do nich.	wdrożenia procesów w całej organizacji. **Praktyki: Zaawansowane/proaktywne** Poziom 5 skupia się na ochronie informacji CUI (kontrolowanych informacji jawnych). Dodatkowe praktyki pogłębiają zdolności w zakresie cyberbezpieczeństwa i zwiększają ich stopień zaawansowania.
Społecznościowy model dojrzałości cyberbezpieczeństwa (CCSMM)	**Świadomość w zakresie bezpieczeństwa** Głównym tematem działań na tym poziomie jest uświadamianie osobom fizycznym i organizacjom zagrożeń, problemów i tematów związanych z cyberbezpieczeństwem.	**Rozwój procesów** Poziom mający pomagać społecznościom w ustanawianiu i udoskonalaniu procesów bezpieczeństwa niezbędnych do skutecznego rozwiązywania problemów związanych z cyberbezpieczeństwem.	**Zasobność w informacje** Poziom mający na celu usprawnienie mechanizmów wymiany informacji w obrębie społeczności, aby umożliwić jej efektywne korelowanie pozornie niezwiązanych ze sobą informacji.	**Opracowanie taktyki** Elementy tego poziomu mają na celu opracowanie lepszych i bardziej proaktywnych metod wykrywania ataków i reagowania na nie. Na tym poziomie powinna już zostać wprowadzona większość metod zapobiegawczych.	**Pełna zdolność operacyjna w zakresie bezpieczeństwa** Ten poziom przedstawia elementy, które powinny występować w organizacji, żeby mogła uznawać się za w pełni przygotowaną operacyjnie do reagowania na wszelkiego rodzaju cyberzagrożenia.
Model audytu wewnętrznego (IA-CM) dla sektora publicznego (Internal Audit Capability Model (IA-CM) for the Public Sector)	**Początkowy** Brak trwałych i powtarzalnych zdolności – zależny od działań podejmowanych indywidualnie	**Infrastruktura** Trwałe i powtarzalne praktyki i procedury	**Integracja** Jednolite stosowanie praktyki zarządzania i zasad praktyki zawodowej	**Zarządzane** Scalanie informacji pochodzących z całej organizacji w celu udoskonalania zarządzania organizacją i ryzykiem	**Optymalizacja** Uczenie się wewnątrz i na zewnątrz organizacji w celu ciągłego doskonalenia

Tabela 7: Porównanie atrybutów/ wymiarów

	Model zdolności w zakresie cyberbezpieczeństwa dla państw (Cybersecurity Capacity Maturity Model for Nations, CMM)	Model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Cybersecurity Capability Maturity Model, C2M2)	Katarski model dojrzałości zdolności w zakresie cyberbezpieczeństwa (Qatar Cybersecurity Capability Maturity Model, Q-C2M2)	Certyfikacja modelu dojrzałości cyberbezpieczeństwa (Cybersecurity Maturity Model Certification, CMMC)	Certyfikacja modelu dojrzałości cyberbezpieczeństwa (Cybersecurity Maturity Model Certification, CMMC)	Model dojrzałości bezpieczeństwa informacji na potrzeby ram cyberbezpieczeństwa NIST (Information Security Maturity Model for NIST Cyber Security Framework, ISMM)	Ramy na rzecz poprawy cyberbezpieczeństwa infrastruktury krytycznej (Framework for Improving Critical Infrastructure Cybersecurity)	Globalny indeks cyberbezpieczeństwa (Global Cybersecurity Index, GCI)	Indeks potęgi cybernetycznej (Cyber Power Index, CPI)
Poziomy	Pięć wymiarów podzielonych na szereg czynników, które z kolei obejmują szereg aspektów i wskaźników (Rys. 4)	Dziesięć dziedzin, w tym unikatowy cel zarządzania i szereg celów podejścia (Rys. 6)	Pięć dziedzin podzielonych na poddziedziny	Siedemnaście dziedzin podzielonych na procesy i jedną lub więcej zdolności, w ramach których wyróżniono praktyki (Rys. 9).	Sześć głównych wymiarów	Dwadzieścia trzy oceniane obszary	Pięć funkcji oraz należące do nich kluczowe kategorie i podkategorie (Rys. 8).	Pięć filarów obejmujących szereg wskaźników	Cztery kategorie z szeregiem wskaźników
Atrybuty/ wymiary	i Opracowanie polityki i strategii w zakresie cyberbezpieczeństwa; ii Wspieranie odpowiedzialnej kultury cyberbezpieczeństwa w społeczeństwie; iii Poszerzanie wiedzy o cyberbezpieczeństwie; iv Tworzenie skutecznych ram prawnych i regulacyjnych; oraz v Kontrolowanie ryzyka za pomocą norm, organizacji i technologii.	i Zarządzanie ryzykiem; ii Zarządzanie aktywami, zmianami i konfiguracją; iii Zarządzanie tożsamością i dostępem; iv Zarządzanie zagrożeniami i podatnościami; v Orientacja sytuacyjna; vi Reagowanie na zdarzenia i incydenty; vii Zarządzanie łańcuchem dostaw i zależnościami zewnętrznymi; viii Zarządzanie siłą roboczą; ix Architektura cyberbezpieczeństwa; x Zarządzanie programem cyberbezpieczeństwa.	i Zrozumienie (cyberzarządzanie, zasoby, ryzyko i szkolenia); ii Zabezpieczanie (bezpieczeństwo danych, bezpieczeństwo technologii, bezpieczeństwo kontroli dostępu, bezpieczeństwo komunikacji i bezpieczeństwo personelu); iii Wykrywanie (monitorowanie, zarządzanie incydentami, wykrywanie incydentów, ich analiza i narażenie na incydenty); iv Reagowanie (planowanie reakcji, łagodzenie skutków i komunikacja w związku z reagowaniem na incydenty); v Utrzymanie (planowanie przywracania, zarządzanie ciągłością działania,	i Kontrola dostępu; ii Zarządzanie aktywami; iii Audyt i rozliczalność; iv Wiedza i szkolenia; v Zarządzanie konfiguracją; vi Identyfikacja i uwierzytelnianie; vii Reagowanie na incydenty; viii Utrzymanie; ix Ochrona nośników; x Bezpieczeństwo personelu; xi Ochrona fizyczna; xii Przywracanie; xiii Zarządzanie ryzykiem; xiv Ocena bezpieczeństwa; xv Orientacja sytuacyjna; xvi Ochrona systemów i łączności; xvii Integralność systemów i informacji.	i Uwzględnione zagrożenia; ii Mierniki; iii Wymiana informacji; iv Technologia; v Szkolenia; vi Test.	i Zarządzanie aktywami; ii Otoczenie biznesu; iii Zarządzanie; iv Ocena ryzyka; v Strategia zarządzania ryzykiem; vi Ocena zgodności; vii Kontrola dostępu; viii Wiedza i szkolenia; ix Bezpieczeństwo danych; x Procesy i procedury ochrony informacji; xi Utrzymanie; xii Technologia ochronna; xiii Anomalie i zdarzenia; xiv Stałe monitorowanie bezpieczeństwa; xv Procesy detekcji; xvi Planowanie reakcji; xvii Komunikacja w związku z reagowaniem na incydenty; xviii Analiza reagowania; xix Łagodzenie reagowania;	i Określanie; ii Ochrona; iii Wykrywanie; iv Reagowanie; v Przywracanie.	i Prawne; ii Techniczne; iii Organizacyjne; iv Budowanie zdolności; v Współpraca.	i Ramy prawne i regulacyjne; ii Kontekst gospodarczy i społeczny; iii Infrastruktura technologiczna; iv Zastosowanie w przemyśle.

			doskonalenie i zależności zewnętrzne).			xx Doskonalenie reagowania; xxi Planowanie przywracania; xxii Doskonalenie procesów przywracania; xxiii Komunikacja w ramach przywracania.			

ZAŁĄCZNIK B – BIBLIOGRAFIA DO BADANIA ŹRÓDEŁ WTÓRNYCH

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

Almuhammadi, S. i Alsaleh, M. (2017) „Information Security Maturity Model for Nist Cyber Security Framework", w: Computer Science & Information Technology (CS & IT). Dokument dostępny pod adresem: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. i in. (2016) Stocktaking, analysis and recommendations on the protection of CIIs. Dokument dostępny pod adresem: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. i in. (2009) Developing Maturity Models for IT Management – A Procedure Model and its Application. Dokument dostępny pod adresem: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Rząd belgijski (2012), Strategia cyberbezpieczeństwa. Dokument dostępny pod adresem: 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. i in. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide. RAND Corporation. Dokument dostępny pod adresem: 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, Stany Zjednoczone (2019), Cybersecurity Capability Maturity Model (C2M2) Version 2.0. Dokument dostępny pod adresem https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019) National Cybersecurity Strategies in Comparison – Challenges for Switzerland. Dokument dostępny pod adresem: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Rada Ministrów (2019), portugalski Dziennik Urzędowy, seria 1 – nr 108 – rezolucja Rady Ministrów nr 92/2019. Dokument dostępny pod adresem: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016) Cybersecurity Capacity Maturity Model for Nations (CMM). Uniwersytet Oksfordzki.

CSIRT Maturity – Self-assessment Tool (brak daty). Dokument dostępny pod adresem: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Projekt Rady Europy i Unii Europejskiej CyberCrime@IPA, globalny projekt Rady Europy i Unii Europejskiej w zakresie cyberprzestępczości oraz Grupa Zadaniowa Unii Europejskiej ds. Zwalczania Cyberprzestępczości (2011): Specialised cybercrime units – Good practice study. Dokument dostępny pod adresem: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (brak daty). Dokument dostępny pod adresem: 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. (brak daty) „Welcome to the NCSS Training Tool".

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting. Dokument dostępny pod adresem: 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. Dokument dostępny pod adresem: 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. Dokument dostępny pod adresem: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Strategia cyberbezpieczeństwa „Cyfrowa Słowenia" (2016). Dokument dostępny pod adresem: 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. *i in.* (2014) *Privacy and data protection by design - from policy to engineering.* Dokument dostępny pod adresem: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Komisja Europejska (2012) – Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. Dokument dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52012PC0238&from=PL

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (2012) NCSS: Practical Guide on Development and Execution. Heraklion: ENISA.

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (2012) NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion: ENISA.

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (2016) Guidelines for SMEs on the security of personal data processing.

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (2016) NCSS good practice guide: designing and implementing national cyber security strategies. Heraklion: ENISA.

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (2017) Handbook on security of personal data processing. Dokument dostępny pod adresem: http://dx.publications.europa.eu/10.2824/569768

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (2014) *ENISA CERT inventory of CERT teams and activities in Europe*. Dokument dostępny pod adresem: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Urząd Wykonawczy Prezydenta Stanów Zjednoczonych (2015) Memorandum for Heads of Executive Departments and Agencies. Dokument dostępny pod adresem: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Urząd Kanclerza Federalnego Republiki Austrii (2013), Austriacka strategia cyberbezpieczeństwa. Dokument dostępny pod adresem: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Federalne Ministerstwo Spraw Wewnętrznych (2011), Strategia cyberbezpieczeństwa Niemiec. Dokument dostępny pod adresem: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

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. Dokument dostępny pod adresem: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., European Union and European Network and Information Security Agency (2015) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. Dokument dostępny pod adresem: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Kancelaria Premiera Francji (2014), francuska narodowa strategia bezpieczeństwa cyfrowego. Dokument dostępny pod adresem: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

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

Uniwersytet Gandawski i in. (2017) „Evaluating Business Process Maturity Models", Journal of the Association for Information Systems. Dokument dostępny pod adresem: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Rząd Bułgarii (2015), Krajowa strategia cyberbezpieczeństwa – Bułgaria odporna na cyberzagrożenia 2020.

Rząd Chorwacji (2015), Krajowa strategia cyberbezpieczeństwa Republiki Chorwacji. Dokument dostępny pod adresem: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Rząd Grecji (2017), Krajowa strategia cyberbezpieczeństwa. Dokument dostępny pod adresem: 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

Rząd Węgier (2018) Strategia na rzecz bezpieczeństwa sieci i systemów informatycznych. Dokument dostępny pod adresem: 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

Rząd Irlandii (2019), Krajowa strategia cyberbezpieczeństwa. Dokument dostępny pod adresem: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Rząd Hiszpanii (2019), Krajowa strategia cyberbezpieczeństwa. Dokument dostępny pod adresem: 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 (red.) (2009) Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

Międzynarodowy Związek Telekomunikacyjny (ITU) (2018) The Global Cybersecurity Index. Dokument dostępny pod adresem: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Międzynarodowy Związek Telekomunikacyjny (ITU) (2018) Guide to developing a national cybersecurity strategy. Dokument dostępny pod adresem: 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.

Rząd łotewski (2014), Strategia cyberbezpieczeństwa Łotwy. Dokument dostępny pod adresem: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. i in. (2014) An evaluation framework for national cyber security strategies. Heraklion: ENISA. Dokument dostępny pod adresem: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

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

Ministerstwo Konkurencyjności i Gospodarki Cyfrowej, Morskiej i Usługowej (2016), Maltańska strategia cyberbezpieczeństwa. Dokument dostępny pod adresem: 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

Ministerstwo Spraw Gospodarczych i Komunikacji (2019), Strategia cyberbezpieczeństwa – Republika Estońska. Dokument dostępny pod adresem: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministerstwo Obrony Narodowej, Republika Litewska (2018), Krajowa strategia cyberbezpieczeństwa

Narodowe Centrum Cyberbezpieczeństwa (2015), Krajowa strategia cyberbezpieczeństwa Republiki Czeskiej. Dokument dostępny pod adresem: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

National Cyber Security Strategies - Interactive Map (brak daty). Dokument dostępny pod adresem: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

National Cybersecurity Strategies Evaluation Tool (2018). Dokument dostępny pod adresem: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Narodowy Instytut Standaryzacji i Technologii (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: Narodowy Instytut Standaryzacji i Technologii. Dokument dostępny pod adresem: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group (2008) Business Process Maturity Model. Dokument dostępny pod adresem: https://www.omg.org/spec/BPMM/1.0/PDF

OECD, Unia Europejska i Wspólne Centrum Badawcze – Komisja Europejska (2008) Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. Dokument dostępny pod adresem: https://www.oecd.org/sdd/42495745.pdf.

Biuro Komisarza ds. Łączności Elektronicznej i Przepisów Pocztowych (2012), Strategia cyberbezpieczeństwa Republiki Cypryjskiej.

Dziennik Urzędowy Unii Europejskiej (2008) DYREKTYWA RADY 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony. Dokument dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32008L0114&from=PL

Organizacja Współpracy Gospodarczej i Rozwoju (OECD) (2012) Cybersecurity policy making at a turning point. Dokument dostępny pod adresem: 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

Urząd Rady Ministrów (2017), Włoski plan działania w dziedzinie cyberbezpieczeństwa. Dokument dostępny pod adresem: 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

Rada Ministrów (2019) Dziennik Urzędowy Rzeczypospolitej Polskiej. Dokument dostępny pod adresem: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Rząd rumuński (2013), Strategia cyberbezpieczeństwa Rumunii. Dokument dostępny pod adresem: 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. and European Union Agency for Cybersecurity (2019) Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Dokument dostępny pod adresem: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Sekretariat Komitetu ds. Bezpieczeństwa (2019), Strategia cyberbezpieczeństwa Finlandii 2019. Dokument dostępny pod adresem: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Rząd słowacki (2015) Koncepcja cyberbezpieczeństwa Republiki Słowackiej. Dokument dostępny pod adresem: 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. (2015) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r.

Smith, R. (2016) „Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r.", w: Smith, R., Core EU Legislation. Londyn: Macmillan Education. Dokument dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=PL.

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

Rząd szwedzki (2017) Nationell strategi för samhällets informations- och cybersäkerhet. Dokument dostępny pod adresem: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Rząd duński – Ministerstwo Finansów (2018), Duńska strategia cyberbezpieczeństwa i bezpieczeństwa informacji. Dokument dostępny pod adresem: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Rada Federalna (2018), Krajowa strategia ochrony Szwajcarii przed cyberryzykiem.

Luksemburska Rada Ministrów (2018), Krajowa strategia cyberbezpieczeństwa. Dokument dostępny pod adresem: 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

Rząd Niderlandów (2018) Krajowy program działań na rzecz cyberbezpieczeństwa. Dokument dostępny pod adresem: 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

Biały Dom (2018), Krajowa cyberstrategia Stanów Zjednoczonych Ameryki. Dokument dostępny pod adresem: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P., i in. (2011) Cyber Europe Report. Dokument dostępny pod adresem: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. i Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (2013) *National-level risk assessments: an analysis report.* Dokument dostępny pod adresem: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., i in. (2015) Report on cyber-crisis cooperation and management. Dokument dostępny pod adresem: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

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

Krajowa strategia bezpieczeństwa Zjednoczonego Królestwa 2016–2021 (2016). Dokument dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Uniwersytet w Innsbrucku i in. (2009) Understanding Maturity Models.

Wamala, D. F. (2011) „ITU National Cybersecurity Strategy Guide". Dokument dostępny pod adresem: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

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

ZAŁĄCZNIK C – POZOSTAŁE CELE OBJĘTE BADANIEM

Wskazane poniżej cele zostały przeanalizowane na etapie badania źródeł wtórnych oraz w ramach rozmów przeprowadzonych przez ENISA. Poniższe cele nie weszły w skład ram oceny zdolności krajowych, ale wskazują na kwestie, które warto omówić. Każdy z poniższych podpunktów będzie zawierał wyjaśnienie przyczyn, dla których dany cel został odrzucony.

- Opracowanie sektorowych strategii cyberbezpieczeństwa;
- Walka z kampaniami dezinformacyjnymi;
- Bezpieczeństwo najnowocześniejszych technologii (5G, sztuczna inteligencja, informatyka kwantowa itp.);
- Zapewnianie suwerenności danych; oraz
- Zachęcanie do rozwoju sektora ubezpieczeń cybernetycznych.

Opracowanie sektorowych strategii cyberbezpieczeństwa

Przyjęcie strategii sektorowych ukierunkowanych na interwencje i zachęty sektorowe zdecydowanie zapewnia lepsze zdolności zdecentralizowane. Jest to szczególnie dobre rozwiązanie w przypadku państw członkowskich, w których OUK mają do czynienia z wieloma różnymi ramami i regulacjami, oraz w których występuje wiele zależności ze względu na przekrojowy charakter cyberbezpieczeństwa. W niektórych państwach członkowskich faktycznie istnieją dziesiątki organów krajowych i organów regulacyjnych posiadających wiedzę na temat specyfiki poszczególnych sektorów, które są uprawnione do egzekwowania szczególnych uregulowań dla każdego sektora.

Na przykład Dania uruchomiła sześć ukierunkowanych strategii obejmujących działania na rzecz cyberbezpieczeństwa i bezpieczeństwa informacji podejmowane w najbardziej krytycznych sektorach z myślą o wzmocnieniu zdecentralizowanych zdolności w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji. Każda „jednostka sektorowa" będzie uczestniczyć między innymi w ocenach zagrożeń na poziomie sektorowym, monitorowaniu, ćwiczeniach w zakresie gotowości, wprowadzaniu systemów bezpieczeństwa, wymianie wiedzy i instruktażach. Strategie sektorowe obejmują następujące sektory:

- Energetyka;
- Ochrona zdrowia;
- Transport;
- Telekomunikacja;
- Finanse; oraz
- Gospodarka morska.

Pozostałe państwa członkowskie wyraziły zainteresowanie możliwością ustanowienia sektorowych strategii cyberbezpieczeństwa w celu uwzględnienia wszystkich wymogów regulacyjnych. Należy jednak zauważyć, że taki cel może nie odpowiadać wszystkim państwom członkowskim, w zależności od ich wielkości, polityki krajowej i dojrzałości. ENISA nie włączyła tego celu do opracowanych ram ze względu na to, że niezwykle trudno jest zapewnić uwzględnienie w nich wszystkich specyficznych uwarunkowań.

Walka z kampaniami dezinformacyjnymi

Państwa członkowskie uwzględniają w swoich krajowych strategiach cyberbezpieczeństwa ochronę podstawowych zasad, takich jak prawa człowieka, przejrzystość i zaufanie publiczne. Jest to bardzo ważne zwłaszcza w przypadku dezinformacji rozpowszechnianej za pośrednictwem tradycyjnych mediów informacyjnych lub serwisów społecznościowych. Cyberbezpieczeństwo jest ponadto obecnie jednym z największych wyzwań w procesie wyborczym. W różnych krajach faktycznie obserwowano w okresach poprzedzających ważne wybory takie działania jak rozpowszechnianie nieprawdziwych informacji czy negatywna propaganda. To zagrożenie może zakłócić proces demokratyczny w Unii Europejskiej. Na szczeblu europejskim, Komisja przedstawiła plan działania[32] na rzecz nasilenia walki z dezinformacją w Europie. Plan ten koncentruje się na czterech kluczowych obszarach (wykrywanie, współpraca, współdziałanie z platformami internetowymi i zwiększanie świadomości) i służy budowaniu zdolności w UE oraz zacieśnianiu współpracy między państwami członkowskimi.

Cztery z 19 państw, z którymi przeprowadzono rozmowy, wyraziło zamiar podjęcia kwestii dezinformacji i propagandy w swoich krajowych strategiach cyberbezpieczeństwa.

Na przykład we francuskiej krajowej strategii cyberbezpieczeństwa[33] stwierdzono, że: „informowanie obywateli o ryzyku związanym z technikami manipulacji i propagandy wykorzystywanymi przez działających w złych zamiarach użytkowników internetu jest obowiązkiem państwa. Na przykład po atakach terrorystycznych na Francję w styczniu 2015 r. rząd stworzył platformę informacyjną poświęconą zagrożeniom związanym z radykalizacją islamu za pośrednictwem sieci komunikacji elektronicznej: « Stop-djihadisme.gouv.fr »". Podejście to mogłoby zostać rozszerzone, aby uwzględnić również inne przejawy propagandy lub destabilizacji.

W kolejnym przykładzie, w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024[34] stwierdzono, że: „(...) do działań o charakterze manipulacyjnym w postaci m.in. kampanii dezinformacyjnych potrzebne jest podjęcie systemowych działań pozwalających na rozwijanie świadomości obywateli w kontekście weryfikacji autentyczności informacji oraz reagowania na próby jej zakłócenia".

W trakcie rozmów przeprowadzonych przez ENISA kilka państw członkowskich poinformowało jednak, że nie uwzględniają tego zagadnienia jako cyberzagrożenia w swoich krajowych strategiach cyberbezpieczeństwa, natomiast podejmują tę problematykę w szerszym wymiarze społecznym, na przykład poprzez inicjatywy polityczne.

Bezpieczeństwo najnowocześniejszych technologii (5G, sztuczna inteligencja, informatyka kwantowa itp.)

Ponieważ aktualny krajobraz cyberzagrożeń nieustannie się poszerza, rozwój nowych technologii najprawdopodobniej doprowadzi do zwiększenia intensywności i liczby cyberataków oraz dywersyfikacji metod, środków i celów wybieranych przez agresorów. Tymczasem takie nowe rozwiązania technologiczne, w postaci najnowocześniejszych technologii, mają potencjał, by stać się fundamentami europejskiego rynku cyfrowego. Aby ustrzec państwa członkowskie przed coraz większym uzależnieniem od technologii cyfrowych oraz chronić je przed pojawiającymi się nowymi technologiami, należy wprowadzać zachęty i kompleksowe strategie polityczne, dzięki którym technologie te będą rozwijane i wprowadzane w UE w bezpieczny i budzący zaufanie sposób.

Na etapie badania źródeł wtórnych przeprowadzonego na podstawie krajowych strategii cyberbezpieczeństwa państw członkowskich, jako przedmiot zainteresowania państw

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

członkowskich wskazano następujące najnowocześniejsze technologie: 5G, sztuczna inteligencja, informatyka kwantowa, kryptografia, przetwarzanie danych na obrzeżach sieci, pojazdy podłączone do sieci i pojazdy autonomiczne, duże zbiory danych, inteligentne dane, blockchain, robotyka i internet rzeczy.

W szczególności na początku 2020 r. Komisja Europejska opublikowała komunikat, w którym zaapelowała do państw członkowskich o podjęcie działań mających na celu wdrożenie środków zalecanych w konkluzjach dotyczących zestawu narzędzi dla technologii 5G[35]. Zestaw narzędzi dla technologii 5G powstał w następstwie zalecenia Komisji (UE) 2019/534 w sprawie cyberbezpieczeństwa sieci 5G przyjętego przez Komisję w 2019 r., w którym wezwano do przyjęcia jednolitego europejskiego podejścia do bezpieczeństwa sieci 5G[36].

Podczas rozmów przeprowadzonych przez ENISA podkreślano, że temat ten jest raczej zagadnieniem przekrojowym, uwzględnianym w całej krajowej strategii cyberbezpieczeństwa, a nie traktowanym jako odrębny cel szczegółowy.

Zapewnienie suwerenności danych

Cyberprzestrzeń może być z jednej strony postrzegana jako potężna, globalna wspólna przestrzeń, która jest łatwo dostępna, sprzyja dobrej komunikacji i oferuje wspaniałe możliwości rozwoju społeczno-gospodarczego. Z drugiej strony cyberprzestrzeń charakteryzuje się również małymi możliwościami egzekwowania prawa, trudnościami z wykrywaniem sprawców, brakiem granic i wzajemnie połączonymi systemami, które mogą być nieszczelne, co grozi kradzieżą danych, a nawet możliwością przechwytywania ich przez władze obcych państw. Poza tym ekosystem cyfrowy charakteryzuje się koncentracją platform usług internetowych i infrastruktury w rękach garstki podmiotów. Wszystkie wyżej wymienione aspekty skłaniają państwa członkowskie do wspierania suwerenności cyfrowej. Osiągnięcie suwerenności cyfrowej oznacza, że obywatele i przedsiębiorstwa są w stanie doskonale prosperować dzięki korzystaniu z godnych zaufania usług cyfrowych i produktów ICT bez obaw o swoje dane osobowe, zasoby cyfrowe, autonomię gospodarczą czy obce wpływy polityczne.

Suwerenność danych, czy też suwerenność cyfrowa, jest wspierana przez państwa członkowskie na szczeblu krajowym i europejskim. Chociaż państwa członkowskie najwyraźniej nie uwzględniły tego zagadnienia bezpośrednio jako celu szczegółowego w swoich krajowych strategiach cyberbezpieczeństwa, traktują je jako ogólnie obowiązującą zasadę lub komunikują zamiar zapewnienia suwerenności cyfrowej na szczeblu krajowym w poszczególnych publikacjach , skupiając się na kluczowych technologiach. Na przykład we francuskim strategicznym przeglądzie cyberobrony z 2018 r. wskazano, że „kontrolowanie następujących technologii ma zasadnicze znaczenie dla suwerenności cyfrowej: szyfrowanie komunikacji, wykrywanie cyberataków, radiotelefony PMR, chmura obliczeniowa i sztuczna inteligencja”[37].

Na szczeblu europejskim państwa członkowskie aktywnie uczestniczą w określaniu europejskiej strategii w zakresie danych (COM/2020/66 final) oraz w tworzeniu unijnych ram certyfikacji produktów, usług i procesów ICT ustanowionych w unijnym akcie o cyberbezpieczeństwie (2019/881) w trosce o strategiczną autonomię cyfrową na szczeblu europejskim.

Etap rozmów z państwami członkowskimi pokazał, że kwestia suwerenności cyfrowej jest często uważana za zagadnienie wykraczające poza ramy cyberbezpieczeństwa. W związku z tym państwa członkowskie nie uwzględniają tego tematu w swoich krajowych strategiach

[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/PL/TXT/?uri=CELEX%3A32019H0534
[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

cyberbezpieczeństwa, a w nielicznych przypadkach, gdzie został on uwzględniony, nie jest ujęty jako odrębny cel szczegółowy.

Zachęcanie do rozwoju sektora ubezpieczeń cybernetycznych

Obecna sytuacja w sektorze ubezpieczeń cybernetycznych wskazuje na to, że światowy rynek zdecydowanie urósł. Jest to jednak dopiero początek jego rozwoju, ponieważ konieczne jest gromadzenie danych oraz ustanowienie wielu precedensów (*np.* niepewność dotycząca zakresu ochrony, systemowe cyberzagrożenia itp.). Ponadto szacunkowe łączne straty ponoszone w wyniku cyberataków na całym świecie o kilka rzędów wielkości przewyższają aktualne możliwości sektora ubezpieczeń cybernetycznych (dokument roboczy MFW – Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143). Rozwój sektora ubezpieczeń cybernetycznych z pewnością może jednak przynieść korzyści i stworzyć grunt pod cenne mechanizmy. Mechanizmy cyberubezpieczeniowe mogą w istocie pomóc w:

- Zwiększaniu świadomości na temat ryzyka dla cyberbezpieczeństwa w przedsiębiorstwach;
- Ocenie ilościowej narażenia na cyberryzyko;
- Poprawie zarządzania ryzykiem dla cyberbezpieczeństwa;
- Zapewnianiu wsparcia dla organizacji padających ofiarą cyberataków;
- Pokrywaniu szkód (materialnych i innych) spowodowanych przez cyberataki.

Niektóre państwa członkowskie rozpoczęły prace nad tym zagadnieniem. Na przykład:

- Estonia przyjęła w swojej krajowej strategii cyberbezpieczeństwa podejście „poczekamy, zobaczymy": „Aby w ogóle ograniczyć cyberryzyko w sektorze prywatnym, przeanalizowane zostaną popyt na usługi w zakresie ubezpieczeń cybernetycznych oraz podaż tych usług w Estonii i na tej podstawie uzgodnione zostaną zasady współpracy dla odpowiednich podmiotów, w tym zasady dotyczące wymiany informacji, opracowywania oceny ryzyka itp. Obecnie na rynku estońskim jest niewielu dostawców usług w zakresie cyberubezpieczeń, najpierw należy więc ustalić, kim oni są i co oferują. Stopień złożoności ochrony ubezpieczeniowej jest często postrzegany jako przeszkoda dla rozwoju rynku ubezpieczeń cybernetycznych".
- Luksemburg wyraźnie popiera rozwój sektora ubezpieczeń cybernetycznych w swojej krajowej strategii cyberbezpieczeństwa: „Cel 1: Tworzenie nowych produktów i usług. W celu grupowania ryzyk i zachęcania ofiar cyberincydentów do zwracania się o profesjonalną pomoc przy opanowaniu incydentu i przywróceniu zaatakowanego systemu, towarzystwa ubezpieczeniowe będą zachęcane do tworzenia specjalnych produktów na potrzeby obszaru ubezpieczeń cybernetycznych".

Opinie rozmówców w tej kwestii były dość rozbieżne – niektóre państwa członkowskie twierdziły, że tematyka ubezpieczeń cybernetycznych jest ostatnio często podejmowana, inne natomiast poinformowały, że choć zagadnienie jest przyszłościowe, to branża nie jest jeszcze wystarczająco dojrzała. Natomiast bardzo wielu z nich zadeklarowało, że temat ten nie został uwzględniony w ramach krajowych strategii cyberbezpieczeństwa, ponieważ uznano, iż jest zbyt szczegółowy lub nie mieści się w nich zakresie.

TP-02-21-253-PL-N

O Agencji Unii Europejskiej ds. Cyberbezpieczeństwa

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. ENISA – utworzona w 2004 r. i wzmocniona unijnym aktem o cyberbezpieczeństwie – wnosi wkład w politykę cybernetyczną UE, zwiększa wiarygodność produktów, usług i procesów informacyjno-komunikacyjnych dzięki systemom certyfikacji cyberbezpieczeństwa, współpracuje z państwami członkowskimi i organami UE oraz pomaga przygotować Europę na przyszłe wyzwania cybernetyczne. Poprzez wymianę informacji, budowanie zdolności i zwiększanie świadomości, Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do gospodarki opartej na łączności i odporność unijnej infrastruktury oraz, w efekcie, zapewnić cyfrowe bezpieczeństwo społeczeństwa i mieszkańców Europy. Aby uzyskać więcej informacji, zob.: 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: 978-92-9204-488-6
DOI: 10.2824/601560