

Modele dojrzałości ISAC – Jak budować współpracę w sektorach i podsektorach?

Poradnik dla interesariuszy Krajowego
Systemu Cyberbezpieczeństwa

Słowo wstępu

Szanowni Państwo,

Nie ma jednego standardowego formatu dla ISAC (Centrum Wymiany i Analizy Informacji). Każdy ISAC wybiera najlepszy dla siebie model współpracy, dostosowany do swoich możliwości i zapotrzebowania. Może być to współpraca formalna lub nieformalna, ustrukturyzowana lub elastyczna, oparta na spotkaniach osobistych lub też wymianie wiedzy w ramach zaufanej platformy cyfrowej. Albo kombinacja wszystkich możliwości. Tego typu decyzje należą do członków stworzonej struktury ISAC. Rozstrzygnięcia należy poczynić na samym początku, na etapie powoływania organizacji. Inne – w toku dalszych prac.

Wydany przez nas w 2019 roku poradnik *ISAC (Centra Wymiany i Analizy Informacji) w kontekście sektorowych centrów cyberbezpieczeństwa* zawiera porady dotyczące początkowego etapu budowania ISAC. Natomiast niniejsza publikacja poświęcona jest kolejnym etapom rozwoju ISAC i zawiera propozycję dalszych kroków, które można podjąć na drodze do wzmocnienia i poszerzenia współpracy, a także zwiększania możliwości ISAC. Zaproponowany model dojrzałości, został opracowany na podstawie doświadczeń europejskich centrów ISAC. Jego celem jest wskazanie możliwych kierunków rozwoju, a także konkretnych działań, które prowadzą do kolejnych etapów dojrzałości organizacji.

Krzysztof Silicki

Zastępca Dyrektora NASK,
Dyrektor ds. Cyberbezpieczeństwa i Innowacji

Spis treści

Słowo wstępu	2
Wprowadzenie	4
Co to jest model dojrzałości ISAC i dlaczego warto go stosować?	7
Model dojrzałości ISAC	9
Budowanie zaufania	9
Zarządzanie i organizacja	10
Wymiana informacji	12
Usługi	13
Działania zewnętrzne	14
Macierz modelu dojrzałości ISAC	16
Cztery kroki optymalizacji ISAC – jak wykorzystywać model dojrzałości w praktyce?	18



ISBN 978-83-954637-4-7



9 788395 463747

Wprowadzenie

ISAC (*Information Sharing and Analysis Centre*) to centrum wymiany wiedzy i doświadczeń dotyczących incydentów cyberbezpieczeństwa w danym sektorze gospodarki (np. finansowym, energetycznym czy lotniczym). ISAC jest formą partnerstwa publiczno-prywatnego (PPP), rozumianego jako współpraca sektora prywatnego i publicznego, a także jako budowanie relacji pomiędzy różnymi sektorami gospodarki oraz pomiędzy różnymi instytucjami publicznymi. Pierwsze ISAC powstały w latach 90. w Stanach Zjednoczonych. W Europie tego typu organizacje pojawiły się najpierw w sektorze finansowym i energetycznym¹. Po przyjęciu Dyrektywy NIS², ISAC stają się coraz popularniejszym modelem współpracy, ponieważ pomagają podnosić kompetencje operatorów w sektorach kluczowych i budują zaufanie pomiędzy interesariuszami systemu cyberbezpieczeństwa. Dodatkowo, Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) programowo wspiera państwa członkowskie w budowie ISAC na poziomie europejskim. Obecnie funkcjonują cztery takie organizacje – w sektorze finansowym, energetycznym, lotniczym i kolejowym³.

Przyjęta w Polsce w lipcu 2018 roku Ustawa o krajowym systemie cyberbezpieczeństwa wprowadza pojęcie **sektorowego zespołu cyberbezpieczeństwa**, który zgodnie z art. 44 może być powołany przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora wymienionego w załączniku do ustawy. **Jednak utworzenie ISAC może pełnić ważną funkcję wzmacniającą poziom świadomości i cyberbezpieczeństwa w sektorze**, szczególnie kiedy dany sektor nie jest jeszcze na tyle dojrzały i zintegrowany, aby mógł powstać tam sektorowy zespół CSIRT. Dodatkowo, ISAC może być formą samoorganizacji sektora, co oznacza, że nie jest konieczne powołanie takiej struktury przez organ właściwy. Operatorzy z własnej inicjatywy mogą stworzyć Centrum Analiz i Wymiany Informacji, które np. zostanie objęte patronatem przez ministra właściwego dla danego sektora lub podsektora (organ właściwy ds. cyberbezpieczeństwa). Właśnie w taki sposób, w 2020 roku, powstał ISAC- Kolej.

1 Więcej na temat historii ISACs przeczytasz w poradniku ISAC (*Centra Wymiany i Analizy Informacji*) w kontekście sektorowych centrów cyberbezpieczeństwa: <https://cyberpolicy.nask.pl/poradnik-na-temat-tworzenia-isac-centra-wymiany-i-analizy-informacji/>.

2 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Directive concerning measures for a high common level of security of network and information systems across the Union)

3 <https://www.enisa.europa.eu/>

Korzyści związane z powołaniem ISAC

Dla sektora publicznego	Dla sektora prywatnego
• Informacje na temat poziomu bezpieczeństwa w kluczowych sektorach gospodarki • Lepsze zrozumienie potrzeb sektora prywatnego • Możliwość ustanowienia jednego punktu koordynacji, w przypadku incydentów poważnych i istotnych⁴	• Uczenie się od siebie nawzajem i wymiana wiedzy oraz dobrych praktyk • Poprawa poziomu cyberbezpieczeństwa w sektorze • Zmniejszenie kosztów dzięki wspólnemu zakupowi usług cyberbezpieczeństwa • Wizerunek sektora, który troszczy się o cyberbezpieczeństwo

Powołanie ISAC jest proste i właściwie bezinwestycyjne, a ostateczny kształt organizacji zależy od potrzeb poszczególnych członków Centrum. Proces budowy ISAC składa się z 3 faz: poszukiwania, budowania i kontynuacji.

Fazy powoływania ISAC



Najważniejsze jest znalezienie osób, które myślą o cyberbezpieczeństwie w podobny sposób i widzą korzyść we współpracy. Początki nie muszą być spektakularne. Czasem najlepiej jest zacząć od kilku entuzjastycznie nastawionych oficerów bezpieczeństwa informacji. Pozwoli to stworzyć nieformalną grupę współpracy i wzajemnie się poznać. Warto też na samym początku zastanowić się nad wspólnymi celami, znaleźć podobieństwa i różnice.

Należy rozpocząć od określania celu i charakteru współpracy. Ważnym elementem jest organizacja oficjalnego uruchomienia ISAC. Wspólny wybór przewodniczącego, wiceprzewodniczącego oraz sekretarza. Da im to jasną legitymizację do dalszych działań. Dodatkowo niezwykle istotne jest uzgodnienie częstotliwości spotkań i sposobu komunikacji, a także wytycznych dotyczących członkostwa i przekazywania informacji. Warto od razu spisać to w formie MoU (*Memorandum of Understanding*), które określi zasady, jasne i dostępne dla wszystkich członków ISAC.

Warto być krytycznym, jeśli chodzi o uczestnictwo w ISAC, stworzyć przestrzeń do oceny i podsumowania swoich działań. ISAC jest pewnego rodzaju „żywym organizmem”, który powinien ewoluować wraz ze zmianą potrzeb jego członków. Ważne tylko, aby te zmiany odbywały się w sposób transparentny, za zgodą wszystkich.

Udana współpraca wymaga tego, aby uczestnicy ISAC mieli równy status w organizacji. Nie powinno się tworzyć hierarchicznych relacji. Jeśli organizacje są podległe jedna drugiej poza ISAC, zapewne nie będą przygotowane na to, aby dzielić się informacjami wewnątrz grupy. Trudno dzielić się wiedzą, która w przyszłości może zostać wykorzystana przeciw Tobie.

⁴ UoKSC, art. 2 pkt 7 i 8: incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej; incydent istotny – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151”;

Szczegółowy proces utworzenia ISAC został opisany w poradniku ISAC (Centra Wymiany i Analizy Informacji) w kontekście sektorowych centrów cyberbezpieczeństwa⁵.

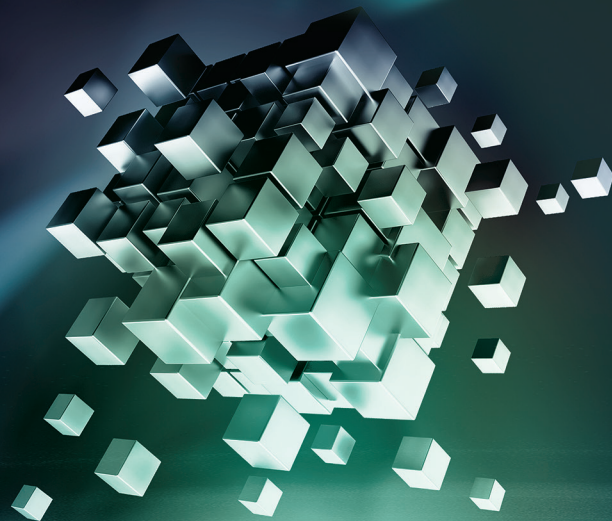
PdC w NASK PIB – wsparcie w zakresie budowy ISAC

Od 2016 roku NASK PIB prowadzi bezpłatny Program Partnerstwo dla Cyberbezpieczeństwa (PdC), którego celem jest budowanie zaufania i tworzenie warunków do wymiany wiedzy, doświadczeń oraz informacji o incydentach i zagrożeniach teleinformatycznych. W jego ramach, wspieramy także sektory w budowie kompetencji i integracji. Jednym z działań realizowanych przez NASK w tym obszarze jest wsparcie i doradztwo w budowie ISAC. Więcej informacji na temat PdC można otrzymać pod adresem pdcc@nask.pl

Szczegółowe nominacje na temat PdC znajdują się na stronie internetowej: <https://www.nask.pl/pl/dzialalnosc/csirt-nask/pdc/3415,Program-Partnerstwo-dla-Cyberbezpieczenstwa.html>



⁵ Poradnik można pobrać ze strony: <https://cyberpolicy.nask.pl/poradnik-na-temat-tworzenia-isac-centra-wymiany-i-analizy-informacji/>



Co to jest model dojrzałości ISAC i dlaczego warto go stosować?

Doświadczenie wdrażania Ustawy o krajowym systemie cyberbezpieczeństwa i współpracy z sektorami rynkowymi oraz organami właściwymi ds. cyberbezpieczeństwa udowodniło, że koncepcja ISAC cieszy się dużym zainteresowaniem i wiele sektorów chce stworzyć takie Centra. Model dojrzałości powstał właśnie po to by im to ułatwić.

Model pokazuje w jaki sposób można rozwijać nowo powstały ISAC tak, aby wraz z upływem czasu zwiększać jego kompetencje, a tym samym korzyści dla członków. W poradniku zawarta została także lista kontrolna dla kolejnych etapów rozwoju Centrum (w podziale na poszczególne obszary), która może być gotowym narzędziem dla osób zaangażowanych w budowę ISAC. Poradnik powstał na podstawie doświadczeń holenderskich⁶, badań przeprowadzonych przez Europejską Agencję ds. Cyberbezpieczeństwa⁷, a także doświadczeń PIB NASK związanych z budową w Polsce ekosystemu cyberbezpieczeństwa.

⁶ Narodowe Centrum Cyberbezpieczeństwa w Holandii, w 2020 roku wydało publikację *Benefit more from your ISAC. A practical guide*.

⁷ *Maturity Framework for ISACs. Information Sharing and Analysis Center Maturity Model*

Jak wygląda model?

Model dojrzałości ISAC uwzględnia 8 kluczowych obszarów:



Budowa zaufania

Sposób budowania zaufania pomiędzy uczestnikami ISAC, etapy budowania współpracy



Zarządzanie i organizacja

Sposób organizacji i zarządzania ISAC (stopień sformalizowania ISAC), sposób finansowania



Wymiana informacji

Sposób przekazywania i analizy informacji przez ISAC oraz rodzaje przekazywanych i analizowanych informacji



Usługi (narzędzia IT, analizy, budowanie zdolności)

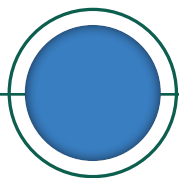
Usługi wspólne, które świadczy ISAC na potrzeby swoich członków, w tym: narzędzia technologiczne, które wspierają proces zarządzania ISAC oraz przekazywania i analizy informacji, analizy których dostarcza ISAC, działania podejmowane przez ISAC w celu budowania kompetencji poszczególnych członków



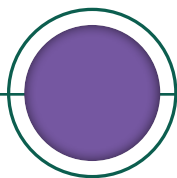
Działania zewnętrzne

Sposób współpracy ISAC z zewnętrznymi interesariuszami (m.in. CSIRT krajowe, sektorowe zespoły cyberbezpieczeństwa, CSIRT sektorowe, inne ISAC i organy właściwe ds. cyberbezpieczeństwa)

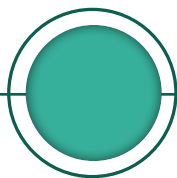
Każda w wymienionych kategoriach jest analizowana na pięciu poziomach dojrzałości:



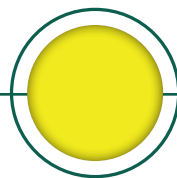
Poziom 1
Niebieski



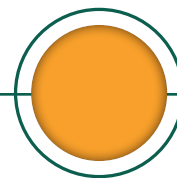
Poziom 2
Fioletowy



Poziom 3
Zielony



Poziom 4
Żółty



Poziom 5
Pomarańczowy

Każdy z poziomów zawiera konkretne i mierzalne kryteria, dzięki którym członkowie mogą samodzielnie ocenić poziom dojrzałości ISAC w danym obszarze.

Model dojrzałości ISAC



Budowanie zaufania

Budowa zaufania jest jednym z najtrudniejszych zadań jakie stoi przed członkami ISAC. Bez niego trudno o rzeczywistą współpracę Centrum oraz wymianę wrażliwych informacji. Dlatego tak ważne jest, aby od pierwszego poziomu dojrzałości organizacji przy stole zasiadali stali przedstawiciele poszczególnych członków, bo znajome twarze sprzyjają zaufaniu. Zaangażowanie uczestników w pierwszych miesiącach funkcjonowania Centrum może być różne, w zależności od potrzeb, co będzie zmieniać się z biegiem czasu. Początkowo spotkania ISAC organizowane są *ad hoc*, wtedy kiedy jest taka potrzeba. Służą one przede wszystkim ustaleniu kwestii organizacyjnych. Na drugim poziomie, członkowie zaczynają spotykać się systematycznie. Jest to silnie powiązane z drugim obszarem (zarządzanie i organizacja), kiedy wybrany jest już Przewodniczący i Wiceprzewodniczący oraz funkcjonuje sekretariat. Na trzecim – poza zebraniami biznesowymi pojawiają się również wydarzenia integracyjne, które mają służyć lepszemu poznaniu się i budowaniu zaufania. Dzięki większej integracji członków ISAC, zaczynają oni kontaktować się ze sobą również poza oficjalnymi spotkaniami w Centrum, wymieniają między sobą kontakty robocze i korzystają z wzajemnej pomocy. Rośnie również ich aktywność w ramach organizacji.

Na poziomie czwartym ISAC zaczyna rekrutować do swoich struktur nowych członków, którzy początkowo nie są na równi zintegrowani jak grupa założycielska i dopiero z czasem muszą zdobyć zaufanie pozostałych. Dlatego nadawane są różne statusy członkostwa, uwzględniające staż w organizacji i odzwierciedlające poziom zaufania. Jest to silnie powiązane z rodzajem wymienianych informacji.

Poziom piąty charakteryzuje wysoki poziom zaufania. Członkowie ISAC dobrze się znają, funkcjonują również utarte sposoby komunikacji bezpośredniej. Ponieważ ISAC ma rozbudowaną strukturę, wiele grup roboczych i poziomów członkostwa, dostęp do różnych informacji zależy z jednej strony od statusu członkostwa, a z drugiej od zainteresowania i zapotrzebowania danej organizacji.

Poniższa lista kontrolna przedstawia podział na poszczególne poziomy.

	Poziom 1	Spotkania ad hoc, na których podejmowane są doraźne decyzje	
		Stali przedstawiciele reprezentujący członków na spotkaniach ISAC	
		Członkowie zaangażowani w zależności od potrzeb danej organizacji	
	Poziom 2	Systematyczne spotkania bezpośrednie	
	Poziom 3	Spotkania integracyjne	
		Kontakty robocze (pomiędzy spotkaniami ISAC)	
		Wzrost aktywności członków ISAC	
	Poziom 4	Różne statusy członków (w zależności od stażu w organizacji)	
	Poziom 5	Utarte sposoby komunikacji bezpośredniej (wysoki poziom zaufania)	
		Członkowie wymieniają się informacjami zgodnie ze zdefiniowanym statusem członkostwa i zapotrzebowaniem	

Zarządzanie i organizacja

Sposób zarządzania i organizacji zmienia się wraz z rozwojem ISAC. Na początku działalności potrzebny jest przede wszystkim jasny regulamin, zasady członkostwa i współpracy, które zostały zaakceptowane i podpisane przez wszystkich członków. Najczęściej jedna z organizacji członkowskich oferuje prowadzenie sekretariatu, a przewodniczący zgłasza się dobrowolnie. Na drugim poziomie pojawia się większa formalizacja: oficjalny sekretariat, wybory przewodniczącego i wiceprzewodniczącego, zgodnie z zasadami określonymi w regulaminie. Odpowiadają oni za ustalenie agendy kolejnych spotkań, a także dbają o utrwalenie ich przebiegu w formie notatek, czy minutek. ISAC zaczyna wyznaczać cele swojej działalności, które są zapisywane w planie rocznym. Plan roczny przyjmują wszyscy członkowie ISAC.

Na trzecim poziomie dojrzałości zwiększa się zakres tematyczny działalności organizacji. Powstają grupy robocze, dedykowane konkretnym wyzwaniom stojącym przed sektorem, które także mają swoich przewodniczących. W zależności od zapotrzebowania, Centrum tworzy doraźny budżet na wybrane projekty. Mogą być to również fundusze pozyskane w ramach dofinansowania krajowego, czy projektów europejskich. Na poziomie czwartym ISAC najczęściej ma już stały budżet, tworzony ze składek członkowskich, z którego można zakupić konkretne usługi. Pojawia się długoterminowy plan działania, którego realizacji pilnuje Zarząd. W jego skład najczęściej wchodzi osoby,

które od samego początku brały udział w tworzeniu organizacji (tzw. „stara gwardia”). Grupy robocze są bardziej ustrukturyzowane, regularnie się spotykają, a ich praca ma wymierne efekty dla całego ISAC – dedykowani przedstawiciele i przewodniczący, prezentują wyniki prac na ogólnych spotkaniach. Co roku organizowane jest spotkanie dla wszystkich członków, na którym podsumowuje się działalność całego ISAC, a także weryfikuje stopień realizacji celów i wyznacza cele na kolejny rok.

Na poziomie piątym ISAC jest już dojrzałą organizacją, posiada osobowość prawną, odrębny sekretariat, własnych pracowników i siedzibę (może być w ramach wybranej organizacji członkowskiej). Istnieje ustrukturyzowany budżet centralny, z którego pokrywane są koszty działalności, usługi, szkolenia, analizy itp.

Poniższa lista kontrolna przedstawia podział na poszczególne poziomy.

	Poziom 1	Porozumienie określające zasady współpracy oraz zasady członkostwa i regulamin ISAC	
		Jedna z organizacji sprawuje nieoficjalną funkcję przewodniczącego i sekretariatu	
	Poziom 2	Funkcjonuje oficjalny sekretariat ISAC	
		Przewodniczący i wiceprzewodniczący wybrani zgodnie z regulaminem	
		Ustrukturyzowane spotkania, zgodnie z przygotowaną i zaakceptowaną wcześniej agendą	
		Ustalony i przyjęty roczny plan ISAC	
	Poziom 3	Grupy robocze dedykowane konkretnym tematom	
		Doraźny budżet na wybrane projekty	
	Poziom 4	Długoterminowy plan działalności organizacji, weryfikowany na spotkaniach rocznych	
		Wyodrębniony zarząd, który nadzoruje realizację celów	
		Ustrukturyzowane, tematyczne grupy robocze (z wybranymi przewodniczącymi i stałymi przedstawicielami)	
		Stały budżet, tworzony ze składek członkowskich	
		Roczne spotkanie podsumowujące działalność ISAC	
	Poziom 5	Osobowość prawna	
		Osobna struktura, z własnym sekretariatem	
		Pracownicy zatrudnieni przez ISAC	
		Siedziba, w której odbywają się spotkania zarządu i grup roboczych	
		Ustrukturyzowany budżet centralny	



Wymiana informacji

Wymiana informacji to podstawowa działalność każdego ISAC. Wraz ze wzrostem zaufania pomiędzy poszczególnymi członkami Centrum oraz coraz większą formalizacją struktury, ISAC wymienia coraz więcej informacji. Na początku jest to tylko wymiana dobrych praktyk, silnie połączona z coraz lepszym poznawaniem się przedstawicieli poszczególnych instytucji. Kolejnym etapem jest omawianie na spotkaniach poszczególnych przykładów (np. incydentów) oraz doraźna wymiana informacji o incydentach i wymiana ostrzeżeń. Sprzyja temu fakt, że przedstawiciele poszczególnych instytucji coraz lepiej się znają oraz, że wykorzystywana jest szyfrowana lista mailingowa. Informacje wymieniane są zgodnie z tzw. „protokołem sygnalizacji świetlnej” (*Traffic Light Protocol*). Kolejnym etapem jest wymiana informacji o incydentach *post factum*, połączona z wymianą analiz na temat incydentów i informacji o podatnościach. Sprzyja temu wykorzystywanie takich narzędzi jak platformy do wymiany informacji (np. MISP⁸). Na poziomie czwartym, ISAC dzieli się już informacjami o incydentach w czasie rzeczywistym oraz podejmuje współpracę w zakresie obsługi incydentów. Na ostatnim poziomie struktura jest już na tyle rozwinięta, że możliwa jest wymiana informacji wrażliwych i poufnych, a członkowie ISAC wspólnie koordynują kryzysy wynikające z incydentów w sektorze lub podsektorze (także w zakresie komunikacji zewnętrznej – wspólne opracowywanie komunikatów prasowych).

Traffic Light Protocol jest to zestaw reguł, pogrupowanych w 4 kategorie, używanych w celu lepszego zdefiniowania grupy odbiorców wrażliwych informacji. Dla ułatwienia kategorie opisywane są kolorami (czerwony, pomarańczowy, zielony oraz biały). Zakwalifikowanie do odpowiedniej kategorii leży po stronie organizacji, z której pochodzą informacje. Jeśli odbiorca chciałby podzielić się uzyskanymi informacjami z szerszym gronem, musi uzyskać odpowiednią akceptację od autora wiadomości.

	Znaczenie kolorów TLP dla odbiorców wiadomości	Znaczenie kolorów TLP dla autorów wiadomości
TLP: RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.	Oznaczenie wiadomości, które mogą za sobą nieść poważne zagrożenie ujawnienia wrażliwych danych w wyniku ich nieprawidłowego przetworzenia, jak również, gdy ich wykorzystanie przez innych niż odbiorcy nie ma sensu.
TLP: AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i <i>constituency</i>) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane.	Oznaczenie wiadomości wymagających podjęcia odpowiednich kroków przez dodatkowe osoby. Informacje te niosą ze sobą ryzyko ujawnienia zbyt wielu wrażliwych danych, jeśli zostałyby przekazane podmiotom innym niż bezpośrednio zaangażowanym.
TLP: GREEN	Odbiorcy mogą dzielić się informacjami ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.	Oznaczenie wiadomości niosących ze sobą informacje ogólnie przydatne dla wszystkich organizacji partnerskich oraz w obrębie środowiska.
TLP: WHITE	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).	Oznaczenie wiadomości, których wykorzystanie nie powinno wiązać się z żadnym bądź minimalnym ryzykiem niewłaściwego użycia.

Informację o użytym TLP powinna zostać umieszczona w nagłówku lub stopce przekazywanej wiadomości, przeważnie stosując zapis w formacie: „TLP: [Kolor]”. Należy mieć na uwadze, że *Traffic Light Protocol* nie ma zastosowania do informacji tajnych lub poufnych⁹.

⁸ MISP (kiedyś: *Malware Information Sharing Platform*, a obecnie: *Open Source Threat Intelligence Platform*) to platforma do dzielenia się informacjami na temat zagrożeń z zakresu cyberbezpieczeństwa <https://www.misp-project.org/>

⁹ Źródło: <https://www.cert.pl/tlp/>

Poniższa lista kontrolna przedstawia podział na poszczególne poziomy.

 Poziom 1	Wymiana dobrych praktyk	
	Stopniowe poznawanie organizacji, które biorą udział w ISAC	
 Poziom 2	Na spotkaniach omawiane są ciekawe przykłady zagrożeń i incydentów	
	Doraźna wymiana ostrzeżeń i informacji o incydentach (poprzez szyfrowaną listę mailingową)	
	Informacje wymieniane są zgodnie z zasadami TLP	
 Poziom 3	Wymiana informacji o incydentach <i>post factum</i>	
	Wymiana analiz na temat incydentów	
	Wymiana informacji o podatnościach	
 Poziom 4	Współpraca w czasie obsługi incydentów	
	Wymiana informacji o incydentach w czasie rzeczywistym	
 Poziom 5	Wymiana informacji wrażliwych i poufnych	
	Wspólna koordynacja kryzysu i dużych incydentów (także wspólne komunikaty prasowe)	



Usługi

Usługi świadczone w ramach ISAC to przede wszystkim narzędzia IT, które wspierają wymianę informacji między członkami oraz budowę wzajemnego zaufania. Poza tym są to także wszystkie działania, które podejmuje ISAC na rzecz swoich członków – przygotowywanie analiz, ćwiczeń, szkoleń, warsztatów itp. Na pierwszym poziomie, a więc na samym początku funkcjonowania ISAC, jest to po prostu lista mailingowa. Na poziomie drugim, lista ta jest już szyfrowana tak, aby w sposób doraźny można było wymieniać informacje o incydentach i zagrożeniach. Kolejnym etapem (poziom 3) jest uruchomienie platformy do wymiany informacji. W tym celu można wykorzystywać gotowe narzędzia takie jak MISP, lub platformę dostępną w ramach Partnerstwa dla Cyberbezpieczeństwa, prowadzonego przez NASK. Także na poziomie trzecim, ISAC organizuje wspólne ćwiczenia w formule *table top* – ćwiczenia procedur. Poza tym ISAC organizuje także szkolenia i warsztaty dla swoich członków. Może być to realizowane metodą wymiany wiedzy – organizacje bardziej rozwinięte w zakresie cyberbezpieczeństwa pomagają tym słabiej rozwiniętym nabyć konkretne kompetencje, tak aby podnieść ogólny poziom bezpieczeństwa w sektorze lub podsektorze. Na poziomie czwartym funkcjonuje chat, pozwalający członkom na wymianę informacji w czasie rzeczywistym. Ponieważ ISAC się rozrasta – grupy robocze, wyodrębniony zarząd – mogą funkcjonować dedykowane chaty dla różnych grup. Poza tym ISAC organizuje wspólne ćwiczenia techniczne (formuła *red – blue team*), a także przygotowywane są raporty i analizy dla członków. ISAC organizuje także szkolenia i warsztaty dla całego sektora lub podsektora, a nie tylko tych organizacji które są członkami. Jest to bezpośrednio związane z coraz większą aktywnością zewnętrzną ISAC i poszukiwaniem nowych członków. Na poziomie piątym, istnieje zaufana platforma do wymiany informacji z systemem monitorowania zagrożeń, a raporty i analizy ISAC są udostępniane wszystkim uczestnikom krajowego systemu cyberbezpieczeństwa. Podobnie jest z organizacją ćwiczeń, szkoleń i warsztatów.

Poniższa lista kontrolna przedstawia podział na poszczególne poziomy.

	Poziom 1	Lista mailingowa	
	Poziom 2	Szyfrowana lista mailingowa	
	Poziom 3	Platforma do wymiany informacji	
		Wspólne ćwiczenia <i>table top</i> dla członków ISAC	
		Organizowanie szkoleń i warsztatów dla członków ISAC	
	Poziom 4	Zaufany i bezpieczny chat do rozmów bezpośrednich w czasie rzeczywistym	
		Wspólne ćwiczenia techniczne dla członków ISAC	
		Przygotowywanie raportów i analiz dla członków ISAC	
		Organizowanie szkoleń i warsztatów dla całego sektora (także dla podmiotów nie będących członkami ISAC)	
	Poziom 5	Zaufana platforma z systemem monitorowania zagrożeń	
		Przygotowywanie raportów i analiz dla uczestników krajowego systemu cyberbezpieczeństwa	
		Organizacja ćwiczeń, szkoleń i warsztatów dla podmiotów krajowego systemu cyberbezpieczeństwa	



Działania zewnętrzne

Działania zewnętrzne są związane z aktywnością ISAC w obrębie sektora lub podsektora i współpracy z innymi interesariuszami krajowego systemu cyberbezpieczeństwa. Na pierwszym poziomie ISAC uzyskuje patronat ministra właściwego dla danego sektora lub podsektora, nawiązuje współpracę z CSIRT poziomu krajowego oraz rozpoczyna rozmowy o współpracy z przedstawicielami administracji publicznej (np. organów właściwych ds. cyberbezpieczeństwa), przedstawicielami CSIRT sektorowych, innych ISAC oraz firmami świadczącymi usługi z zakresu cyberbezpieczeństwa. Na poziomie drugim, przedstawiciele powyższych instytucji są doraźnie zapraszani na spotkania. Na poziomie trzecim są już jasno określone zasady współpracy z partnerami zewnętrznymi.

Na poziomie czwartym, ISAC jest już bardziej sformalizowaną strukturą, posiada spójną i zaplanowaną komunikację zewnętrzną (logo, kolorystyka, plan komunikacji). Centrum zaczyna reprezentować interesy sektora przed organami właściwymi ds. cyberbezpieczeństwa oraz sektorowymi CSIRT i krajowymi CSIRT. Oznacza to, że wypowiada się w imieniu członków w zakresie nowych regulacji prawnych i dokumentów strategicznych (np. Strategia Cyberbezpieczeństwa RP). Prowadzi także regularną i ustrukturyzowaną współpracę z członkami krajowego systemu cyberbezpieczeństwa, a zarząd reprezentuje organizację w wydarzeniach zewnętrznych (m.in. konferencje, warsztaty). Centrum działa również aktywnie na rzecz pozyskiwania nowych członków (ma jasną politykę rozwoju w tym zakresie).

Na poziomie piątym, ISAC uczestniczy w budowaniu wyższego poziomu cyberbezpieczeństwa w całym krajowym systemie cyberbezpieczeństwa, a nie tylko w sektorze. Dzieje się to poprzez organizację własnych konferencji, warsztatów i spotkań w których mogą brać udział podmioty zewnętrzne, udostępnianie analiz i raportów podmiotom zewnętrznym oraz oferowanie szkoleń i warsztatów.

Poniższa lista kontrolna przedstawia podział na poszczególne poziomy.

	Poziom 1	Pozyskanie patronatu ministra właściwego dla danego sektora lub podsektora	
		Współpraca z CSIRT poziomu krajowego	
		Wstępne rozmowy o współpracy z przedstawicielami administracji publicznej	
		Wstępne rozmowy współpracy z przedstawicielami CSIRT sektorowych, innych ISAC oraz firmami świadczącymi usługi z zakresu cyberbezpieczeństwa	
	Poziom 2	Doraźne uczestnictwo przedstawicieli administracji publicznej w spotkaniach ISAC	
		Doraźne uczestnictwo przedstawicieli CSIRT sektorowych, innych ISAC oraz firm świadczących usługi z zakresu cyberbezpieczeństwa w spotkaniach ISAC	
	Poziom 3	Jasno określone zasady współpracy z administracją	
		Jasno określone zasady współpracy z CSIRT sektorowymi, innymi ISAC oraz firmami świadczącymi usługi z zakresu cyberbezpieczeństwa	
		Jasno określone zasady współpracy z przedstawicielami sektora/ podsektora którzy nie są członkami ISAC	
	Poziom 4	ISAC ma zaplanowaną działalność zewnętrzną (komunikacja i współpraca z organizacjami trzecimi)	
		ISAC reprezentuje interesy sektora przed organami właściwymi ds. cyberbezpieczeństwa oraz sektowymi CSIRT i krajowymi CSIRT	
		Istnieje polityka rozwoju ISAC i pozyskiwania nowych członków	
		Członkowie zarządu reprezentują ISAC w wydarzeniach zewnętrznych (konferencje, warsztaty)	
		Regularna i ustrukturyzowana współpraca z członkami krajowego systemu cyberbezpieczeństwa	
	Poziom 5	ISAC uczestniczy w budowaniu wyższego poziomu cyberbezpieczeństwa w całym krajowym systemie cyberbezpieczeństwa, a nie tylko w sektorze Na przykład: • Organizuje własne konferencje, warsztaty i spotkania w których mogą brać udział podmioty zewnętrzne • Udostępnia swoje analizy i raporty podmiotom zewnętrznym • Organizuje szkolenia i warsztaty dla podmiotów zewnętrznych	

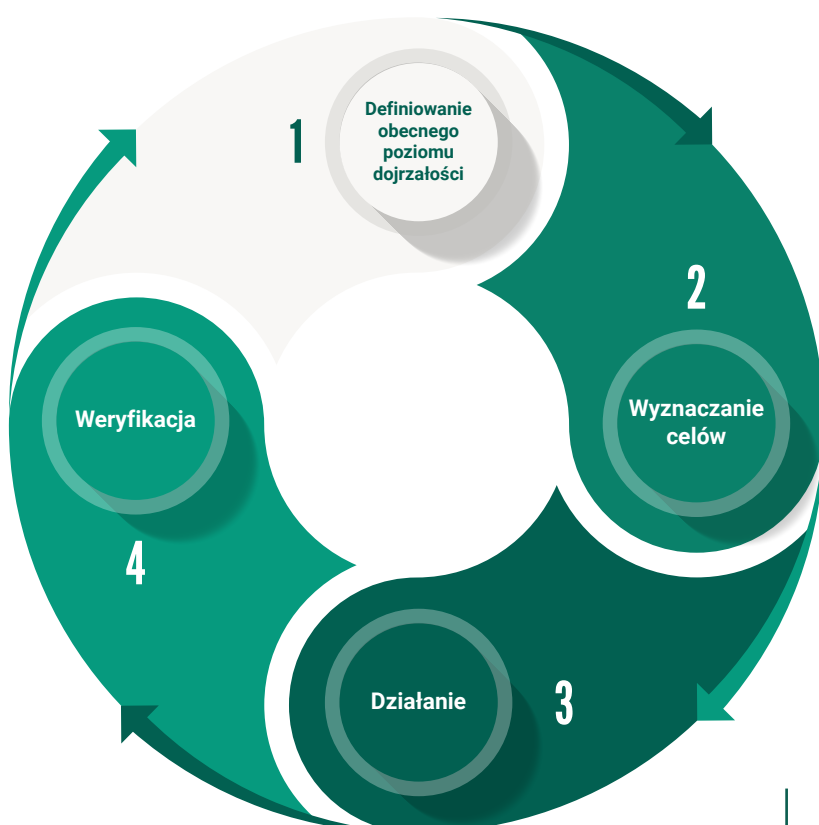
Macierz modelu dojrzałości

Poniższa tabela zawiera macierz modelu dojrzałości ISAC w podziale na obszary i poziomy dojrzałości organizacji, a także wskazówki z propozycją działań, które można podjąć na drodze rozwoju z jednego poziomu do drugiego. Są to proste kroki, wyznaczające kierunek, w którym podąża organizacja. Mogą być zastąpione innymi działaniami, w zależności od potrzeb i decyzji członków ISAC.

Poziomy dojrzałości									
Obszary działalności	Poziom 1		Poziom 2		Poziom 3		Poziom 4		Poziom 5
 Budowa zaufania	- spotkania <i>ad hoc</i>, na których podejmowane są doraźne decyzje - stali przedstawiciele reprezentujący członków na spotkaniach ISAC - członkowie zaangażowani w zależności od potrzeb danej organizacji	Ustalenie kalendarza spotkań (np. 2/ 3 razy w roku – wyznaczenie konkretnych miesięcy, w których spotkania będą się odbywać)	systematyczne spotkania bezpośrednie	Organizacja spotkania integracyjnego (min. raz w roku)	- spotkania integracyjne - kontakty robocze (pomiędzy spotkaniami ISAC) - wzrost aktywności członków ISAC	Podział członków ISAC ze względu na staż i poziom zaangażowania i nadanie im odpowiednich statusów	różne statusy członków (w zależności od stażu w organizacji)	Ustalenie rodzajów informacji, jakie chcą otrzymywać poszczególni członkowie i przyznanie im dostępu do poszczególnych grup	- utarte sposoby komunikacji bezpośredniej (wysoki poziom zaufania) - członkowie wymieniają się informacjami zgodnie ze zdefiniowanym statusem członkostwa i zapotrzebowaniem
 Zarządzanie i organizacja	- porozumienie określające zasady współpracy oraz zasady członkostwa i regulamin ISAC - jedna z organizacji sprawuje nieoficjalną funkcję przewodniczącego i sekretariatu	Wybór przewodniczącego i wiceprzewodniczącego; ustanowienie sekretariatu, ustalenie i przejęcie rocznego planu ISAC (wraz z terminami kolejnych spotkań)	- funkcjonuje oficjalny sekretariat ISAC - przewodniczący i wiceprzewodniczący wybrani zgodnie z regulaminem - ustrukturyzowane spotkania, zgodnie z przygotowaną i zaakceptowaną wcześniej agendą - ustalony i przyjęty roczny plan ISAC	Powołanie tematycznych grup roboczych, zgodnie z potrzebami ISAC	- grupy robocze dedykowane konkretnym tematom - doraźny budżet na wybrane projekty	Powołanie zarządu (w jego składzie powinna być tzw. „stara gwardia” ¹⁰) - przyjęcie długoterminowego planu działalności - wprowadzenie składek członkowskich	- wyodrębniony zarząd, który nadzoruje realizację celów - długoterminowy plan działalności organizacji, weryfikowany na spotkaniach rocznych - ustrukturyzowane, tematyczne grupy robocze - stały budżet, tworzony ze składek członkowskich - roczne spotkanie podsumowujące działalność ISAC	Przekształcenie formuły prawnej ISAC (np. Stowarzyszenie)	- osobowość prawna - osobna struktura, z własnym sekretariatem - pracownicy zatrudnieni przez ISAC - siedziba, w której odbywają się spotkania zarządu i grup roboczych - ustrukturyzowany budżet centralny
 Wymiana informacji	- wymiana dobrych praktyk - stopniowe poznawanie organizacji, które biorą udział w ISAC	- Ustanowienie doraźnej wymiany informacji o incydentach i zagrożeniach - przyjęcie protokołu TLP	- na spotkaniach omawiane są ciekawe przykłady zagrożeń i incydentów - doraźna wymiana ostrzeżeń i informacji o incydentach - informacje wymieniane są zgodnie z zasadami TLP	Zapoczątkowanie wymiany analiz incydentów (<i>post factum</i>) i informacji o podatnościach	- wymiana informacji o incydentach <i>post factum</i> - wymiana analiz na temat incydentów - wymiana informacji o podatnościach	Nawiązanie współpracy w czasie obsługi incydentów, połączone z wymianą informacji o incydentach w czasie rzeczywistym	- współpraca w czasie obsługi incydentów - wymiana informacji o incydentach w czasie rzeczywistym	Ustalenie zasad wymiany informacji wrażliwych i poufnych oraz zasad współpracy w czasie dużych incydentów i przy wspólnej koordynacji kryzysu	- wymiana informacji wrażliwych - wspólna koordynacja kryzysu i dużych incydentów
 Usługi (narzędzia IT, analizy, budowanie zdolności)	lista mailingowa	Uruchomienie szyfrowanej listy mailingowej	szyfrowana lista mailingowa	Uruchomienie platformy do wymiany informacji; organizacja ćwiczeń <i>table top</i> , szkoleń i warsztatów dla członków ISAC	- platforma do wymiany informacji - wspólne ćwiczenia <i>table top</i> dla członków ISAC - organizowanie szkoleń i warsztatów dla członków ISAC	Uruchomienie zaufanego i bezpiecznego chatu do rozmów bezpośrednich; ustalenie procesu przygotowywania raportów i analiz dla członków ISAC	- zaufany i bezpieczny chat do rozmów bezpośrednich w czasie rzeczywistym - wspólne ćwiczenia techniczne dla członków ISAC - przygotowywanie raportów i analiz dla członków ISAC - organizowanie szkoleń i warsztatów dla całego sektora (także dla organizacji nie będących członkami ISAC)	Uruchomienie zaufanej platformy z systemem monitorowania zagrożeń; ustalenie procesu przygotowywania i publikowania raportów dla uczestników krajowego systemu cyberbezpieczeństwa	- zaufana platforma z systemem monitorowania zagrożeń - przygotowywanie raportów i analiz dla uczestników krajowego systemu cyberbezpieczeństwa - organizacja ćwiczeń, szkoleń i warsztatów dla podmiotów krajowego systemu cyberbezpieczeństwa
 Działania zewnętrzne (współpraca z organizacjami zewnętrznymi itp.)	- pozyskanie patronatu ministra właściwego dla danego sektora lub podsektora - współpraca z CSIRT poziomu krajowego - wstępne rozmowy o współpracy z przedstawicielami administracji publicznej - wstępne rozmowy współpracy z przedstawicielami CSIRT sektorowych, innych ISAC oraz firmami świadczącymi usługi z zakresu cyberbezpieczeństwa	Zaproszenie na spotkanie ISAC przedstawicieli administracji publicznej, CSIRT krajowych oraz (jeśli jest taka potrzeba) firm świadczących usługi z zakresu cyberbezpieczeństwa	- doraźne uczestnictwo przedstawicieli administracji publicznej w spotkaniach ISAC - doraźne uczestnictwo przedstawicieli CSIRT sektorowych, innych ISAC oraz firmami świadczącymi usługi z zakresu cyberbezpieczeństwa w spotkaniach ISAC	Przyjęcie zasad współpracy z interesariuszami zewnętrznymi	- jasno określone zasady współpracy z administracją - jasno określone zasady współpracy z CSIRT sektorowymi, innymi ISAC oraz firmami świadczącymi usługi z zakresu cyberbezpieczeństwa - jasno określone zasady współpracy z przedstawicielami sektora/ podsektora którzy nie są członkami ISAC	Przyjęcie planu działalności zewnętrznej i polityki rozwoju ISAC	- zaplanowana działalność zewnętrzna (komunikacja i współpraca z organizacjami trzecimi) - ISAC reprezentuje interesy sektora przed organami właściwymi ds. cyberbezpieczeństwa oraz sektorowymi CSIRT i krajowymi CSIRT - istnieje polityka rozwoju ISAC i pozyskiwania nowych członków - członkowie zarządu reprezentują ISAC w wydarzeniach zewnętrznych (konferencje, warsztaty) - regularna i ustrukturyzowana współpraca z członkami krajowego systemu cyberbezpieczeństwa	Rozwój współpracy ze wszystkimi interesariuszami krajowego systemu cyberbezpieczeństwa oraz innymi podmiotami	- ISAC uczestniczy w budowaniu wyższego poziomu cyberbezpieczeństwa w całym krajowym systemie cyberbezpieczeństwa, a nie tylko w sektorze np. - Oganizuje własne konferencje, warsztaty i spotkania w których mogą brać udział podmioty zewnętrzne - Udostępnia swoje analizy i raporty podmiotom zewnętrznym - Organizuje szkolenia i warsztaty dla podmiotów zewnętrznych

Cztery kroki optymalizacji ISAC – jak wykorzystywać model dojrzałości w praktyce?

Model dojrzałości jest narzędziem praktycznym, którego zadaniem jest osiągnięcie jak największych korzyści z uruchomienia ISAC i jak najszybszy rozwój, w taki sposób aby właściwie zaadresować wszystkie potrzeby członków Centrum. Potrzeby te mogą się zmieniać w czasie i dlatego zalecana jest coroczna weryfikacja, zgodna z modelem.



1. Definiowanie obecnego poziomu dojrzałości (Gdzie jesteśmy?)

Pierwszym etapem jest określenie obecnego poziomu dojrzałości organizacji. W tym celu należy uzupełnić powyższą check-listę, aby zweryfikować w którym miejscu znajduje się ISAC na każdym z 5 obszarów: budowa zaufania, zarządzanie i organizacja, wymiana informacji, usługi, działania zewnętrzne.

2. Wyznaczenie celów (Gdzie chcemy być?)

Po uzupełnieniu listy kontrolnej warto zastanowić się nad tym, gdzie ISAC powinien się znaleźć, aby jak najlepiej adresować potrzeby członków. Czy poziom zaufania między członkami jest zadowalający? Czy narzędzia i usługi świadczone przez ISAC adresują rzeczywiste potrzeby i ułatwiają współpracę oraz wymianę informacji? Jeśli tak – warto wrócić do tych pytań za rok. Jeśli nie – wykorzystując check-listę, należy zastanowić się, co warto zmienić i zaplanować wprowadzenie zmian w tej z kategorii, w której rozwój ISAC nie jest zadowalający. W tym celu należy określić cele ISAC i zaplanować czas na ich realizację.

3. Działanie

Aby zrealizować cele należy określić priorytety działań. Nie zawsze możliwe jest działanie we wszystkich obszarach równocześnie. Czasem konieczne jest najpierw uruchomienie nowego narzędzia, aby móc wymieniać nowy typ informacji, albo w pierwszej kolejności pozyskanie budżetu, żeby zorganizować wspólne ćwiczenia.

Trzy opisane powyżej kroki można zrealizować posługując się poniższą tabelą:

Obszary działalności ISAC	Poziom ISAC	Poziom, do którego dąży ISAC	Planowane działanie (wyznaczenie priorytetów)	Czas realizacji działań
 Budowa zaufania				
 Zarządzanie i organizacja				
 Wymiana informacji				
 Usługi (narzędzia IT, analizy, budowanie zdolności)				
 Działania zewnętrzne (współpraca z organizacjami zewnętrznymi itp.)				

4. Weryfikacja

Po realizacji celów warto sprawdzić, czy ISAC znajduje się etapie rozwoju zgodnym z założeniami. Warto zrobić podsumowanie na spotkaniu i dać szansę wypowiedzieć się wszystkim członkom Centrum tak, aby mieć pewność że wszystkie potrzeby zostały właściwie zaadresowane.

PAMIĘTAJ

Przy korzystaniu z modelu należy pamiętać o 3 zasadach:

1. Model nie zawiera wytycznych, a jedynie propozycję działań.

Opracowany model nie składa się z obowiązkowych punktów, który każdy ISAC musi zrealizować, a jedynie z propozycji działań, stworzonych na podstawie doświadczeń innych organizacji. Należy traktować go elastycznie, jako inspiracje i wskazówki na drodze do rozwoju własnego ISAC. Można również dostosowywać go do własnych potrzeb.

Przykład: Może ambicją członków ISAC nigdy nie było budowanie platformy internetowej do współpracy i zamiast tego wolą skupić się na spotkaniach osobistych, wspieranych komunikacją za pośrednictwem szyfrowanej listy mailingowej.

2. Każdy z ISAC może wybrać, które obszary rozwoju są dla niego priorytetowe

Nie ma dwóch takich samych ISAC. Każde centrum posiada własne cele, dopasowane do potrzeb danego sektora. Nie ma obowiązku dążenia do równego rozwoju organizacji w każdym z obszarów. Na przykład, funkcjonujące w Europie ISAC w sektorze finansowym koncentrują się na współpracy z organami ścigania, a te w sektorze energetyki na aspektach badawczych i rozwojowych (R&D).

Przykład: Jeżeli współpraca zewnętrzna nie jest priorytetem dla ISAC, można zostać na poziomie 2 w tym obszarze, a zamiast tego dążyć do poziomu 5 w rozwoju zdolności i kompetencji.

3. Metoda małych kroków

Podział każdego obszaru na 5 poziomów dojrzałości służy temu, aby każdy ISAC, mógł rozwijać się „metodą małych kroków”. Czasami różnice pomiędzy poszczególnymi poziomami są naprawdę niewielkie. Dzięki temu organizacja może w łatwy sposób przejść na kolejny etap, co może okazać się motywujące do dalszej pracy. Zalecamy realizowanie poszczególnych poziomów w opisanej kolejności, chyba że zaproponowane kryteria nie odpowiadają potrzebom ISAC.

Lektura dodatkowa:

- *Information Sharing and Analysis Center (ISACs) – Cooperative models*
(<https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models>)
- *A practical guide: Benefit more from your ISAC*
(<https://english.ncsc.nl/publications/publications/2020/february/24/a-practical-guide-benefit-more-from-your-isac>)

Przydatne adresy:

- www.cyberpolicy.nask.pl; cyberpolicy@nask.pl
- pdcc@nask.pl

NASK



Cyber POLICY