KRAJOWA IZBA GOSPODARCZA
ELEKTRONIKI I TELEKOMUNIKACJI

Warszawa, dn. 10.06.2026 r.
KIGEiT/999/06/2026

Ministerstwo Cyfryzacji
ul. Królewska 27,
00-060 Warszawa

STANOWISKO
DO PROJEKTU ZESTAWIENIA WYMAGAŃ DOKUMENTÓW
NORMALIZACYJNYCH (ART. 45 UST. 3 USTAWY O KSC)

W imieniu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji wyrażamy uznanie dla intencji Ministerstwa Cyfryzacji, polegającej na ułatwieniu podmiotom objętym ustawą identyfikacji norm i standardów wspierających System Zarządzania Bezpieczeństwem Informacji (SZBI).

Zestawienie ma charakter pomocniczy i informacyjny i, – zgodnie z informacją zawartą na stronie konsultacji –, nie stanowi źródła powszechnie obowiązującego prawa. W praktyce tego rodzaju dokument staje się faktycznym punktem odniesienia dla oceny „należytej staranności", kształtuje wymagania w łańcuchu dostaw oraz stanowi odniesienie dla audytorów. W konsekwencji jego treść wywołuje realne skutki, w szczególności dla małych i mikroprzedsiębiorców.

W ocenie Izby projekt w obecnym kształcie nie realizuje deklarowanego celu **w odniesieniu do sektora MŚP**.

Zestawienie obejmuje 53 pozycje, z których 36 (68%) ma charakter płatny, przy czym jego zasadniczy trzon stanowią normy rodziny ISO/IEC (33 pozycje) oraz amerykańskie frameworki i wytyczne NIST / NSC / CIS / CISA. Jednocześnie pominięto kluczowy, bezpłatny dokument unijny - wytyczne wdrożeniowe ENISA do rozporządzenia wykonawczego (UE) 2024/2690 – jak również lekkie, krajowe i europejskie ramy przygotowane z myślą o małych przedsiębiorstwach. Prowadzi to do wewnętrznej niespójności: standardy uznane w toku prac legislacyjnych za zbyt złożone dla MŚP powracają jako rdzeń rekomendacji.

Poniżej przedstawiamy szczegółową argumentację oraz zestaw konkretnych propozycji zmian.

1. Sprzeczność: ISO 27001 „za trudne dla MŚP", a stanowi rdzeń zestawienia

Jednym z argumentów towarzyszących pracom nad nowelizacją KSC było odejście od sztywnego, ustawowego nakazu zgodności z normami typu ISO/IEC 27001, m.in. ze względu na ich złożoność, sformalizowanie i koszt, co jest szczególnie dotkliwe dla małych podmiotów nieposiadających wyspecjalizowanych komórek bezpieczeństwa. Jeżeli taka była przesłanka, to oparcie zestawienia pomocniczego właśnie na tych normach jest niespójne z deklarowaną troską o MŚP.

W warstwie oznaczonej jako „Podstawowy" poziom dojrzałości (de facto adresowanej do podmiotów wdrażających SZBI po raz pierwszy) jako pierwsze wskazywane są normy ISO/IEC 27001, ISO/IEC 27002 oraz ISO 22301, wszystkie certyfikowalne lub rozbudowane i odpłatne. Dla mikroprzedsiębiorcy jest to poniesienie kosztów zakupu norm, zdobycia kompetencji niezbędnych do ich interpretacji, a w praktyce rynkowej często również skorzystania ze wsparcia konsultanta. W efekcie stanowi to istotną barierę kosztową i kompetencyjną, zamiast realnego ułatwienia.

Zwracamy również uwagę, że wskazane NIST CSF 2.0 i tłumaczenia NIST SP (serie NSC 800-xx), choć dostępne bezpłatnie, zostały zaprojektowane z myślą o dużych, dojrzałych organizacjach (w tym administracji federalnej USA). Wskazywanie ich obok ISO jako „podstawowego" punktu wyjścia dla małych przedsiębiorstw może być mylące ponieważ cechują się one większą złożonością koncepcyjną, a nie prostotą wdrożenia.

ul. Stępińska 22/30
00-739 Warszawa
tel.: +48 22 8510309,
+48 22 8406522
e-mail: kigeit@kigeit.org.pl

NIP 5260029121
Konto: BNP PARIBAS O/Warszawa
nr: 52 1600 1374 0003 0052 2279 1
(e-Doręczenia): AE:PL-65582-55850-ADFTJ-12

kigeit.org.pl

Struktura zestawienia w liczbach

Wymiar	Liczba	Udział
Wszystkie dokumenty	53	100%
Dokumenty płatne (ISO/IEC i PN-EN, CEN/CENELEC, PCI)	36	68%
Dokumenty bezpłatne	17	32%
Normy rodziny ISO/IEC (międzynarodowe, płatne)	33	62%
Dokumenty o rodowodzie amerykańskim (NIST/NSC, CIS, CISA, OWASP, PCI)	13	25%
Dokumenty ENISA	3	6%
Pozostałe europejskie / międzynarodowe (ETSI, CENELEC, TIBER-EU, 3GPP)	4	8%
Poziom „Podstawowy" (de facto dla MŚP / pierwsze wdrożenie)	13	25%

Źródło: własna analiza pliku „Zestawienie_art_45_ust_3_KSC_projekt_do_konsultacji_publicznych.xlsx".

2. Brak odniesienia do wytycznych ENISA do rozporządzenia (UE) 2024/2690

ENISA „*Technical Implementation Guidance on cybersecurity risk-management measures*" (wersja 1.0, czerwiec 2025), powinien – w naszej ocenie – stanowić podstawowy punkt odniesienia dla administracji, jako dokument wdrożeniowy do rozporządzenia wykonawczego Komisji (UE) 2024/2690, doprecyzowującego art. 21 ust. 2 dyrektywy NIS2.

Dokument ten ma cechy, których brakuje pozostałym pozycjom zestawienia, a które są bezcenne właśnie dla małych przedsiębiorstw:

- jest bezpłatny i dostępny na licencji Creative Commons (CC BY 4.0);
- dla każdego wymagania podaje praktyczne wskazówki (guidance), a także przykłady dowodów zgodności (examples of evidence) i „tips", czyli pokazuje, co konkretnie trzeba mieć, by uznać wymóg za spełniony;
- zawiera gotowe mapowania wymagań na normy międzynarodowe ORAZ na krajowe frameworki (Aneks I „National frameworks");
- jego 13 obszarów wymagań pokrywa się z 6 obszarami KSC (zarządzanie ryzykiem, obsługa incydentów, łańcuch dostaw, ciągłość działania, testy i audyty, bezpieczeństwo systemów), mapowanie 1:1 byłoby trywialne;
- wprost wskazuje, że wymaganie posiadania wszystkich wymienionych dowodów byłoby „bardzo restrykcyjnym" podejściem do nadzoru, co jest zachętą do proporcjonalności.

Zestawienie wymienia trzy inne, mniej istotne dla pierwszego wdrożenia dokumenty ENISA (IoT, łańcuch dostaw, MSP), pomijając jednocześnie dokument o charakterze systemowym. W naszej ocenie to właśnie on stanowi najbardziej adekwatny, spójny z podejściem unijnym i praktyczny punkt wyjścia dla sektora MŚP.

3. Pominięcie lekkich ram dla małych firm i doświadczeń innych państw UE

Projekt nie uwzględnia narzędzi zaprojektowanych specjalnie dla mikro- i małych podmiotów. Pomija inicjatywy oddolne (np. bezpłatny, otwarty framework ShieldNet dla MŚP i NGO, z szablonami do RODO i NIS2) jak również sprawdzone rozwiązania państwowe z innych krajów UE.

Wbrew ewentualnemu wrażeniu, że oparcie się na ISO i NIST to „droga europejska", wiodące państwa członkowskie poszły dokładnie w przeciwnym kierunku: zbudowały własne, bezpłatne, proporcjonalne ramy z wyraźnym poziomem wejściowym dla najmniejszych podmiotów, traktując normy ISO jako opcjonalną ścieżkę zaawansowaną, a nie domyślny rdzeń.

Kraj	Rozwiązanie krajowe	Charakterystyka istotna dla MŚP
Belgia	CyberFundamentals (CyFun), Centre for Cybersecurity Belgium	Bezpłatny, 4 poziomy: Small (ok. 7 środków dla mikrofirm bez działu IT), Basic (34 środki dla MŚP), Important, Essential. Daje domniemanie zgodności z NIS2. Mapuje na ISO 27001/NIST CSF/CIS, ale jest dostosowany do kontekstu krajowego.
Niemcy	DIN SPEC 27076 / CyberRisikoCheck (BSI + BVMW)	Stworzony, bo ISO 27001 i IT-Grundschutz uznano za zbyt złożone i kosztowne dla firm do 50 osób. 27 wymagań / 54 pytania w 6 obszarach, bezpłatne narzędzie webowe, często dofinansowane przez państwo, język zrozumiały dla nietechnicznego przedsiębiorcy. Stanowi etap wstępny do ISO 27001.
Francja	MonAideCyber / MesServicesCyber, Guide d'hygiène, ANSSI	Bezpłatny diagnostyk dla TPE/PME (<250 osób), associations i samorządów, realizowany przez przeszkolonych „aidants". Spersonalizowany plan działań. Uzupełniony przewodnikami (m.in. „cyberbezpieczeństwo w 13 pytaniach").
UE	ENISA Technical Implementation Guidance do rozp. (UE) 2024/2690	Bezpłatny, z przykładami dowodów i mapowaniem na normy oraz frameworki krajowe (Aneks I). Wprost zaleca proporcjonalność nadzoru.

Wniosek z porównania: tam, gdzie **państwa UE myślą o MŚP, tworzą krótki, darmowy, krajowy zestaw mierzalnych środków** (7–34 pozycje) i dopiero ponad nim sytuują ISO. Polski projekt odwraca tę logikę, zaczyna od ISO i NIST.

4. Frameworki amerykańskie a europejska suwerenność cyfrowa

Zwracamy uwagę, że około jednej czwartej zestawienia (NIST CSF, serie NSC/NIST SP 800-xx, CIS Controls, CISA, OWASP, PCI DSS) ma pochodzenie amerykańskie. Część z tych materiałów ma wysoką wartość merytoryczną i jest dostępna bezpłatnie, dlatego **nie postulujemy ich eliminacji**. Problem dotyczy jednak proporcji oraz przyjętej hierarchii: rozwiązania amerykańskie pełnią w praktyce rolę podstawowej, bezkosztowej ścieżki odniesienia, podczas gdy europejskie odpowiedniki (ENISA, ETSI, CEN/CENELEC) są niedostatecznie reprezentowane lub mają charakter marginalny.

Z perspektywy europejskiej suwerenności cyfrowej rekomendowanie ram amerykańskich jako domyślnego punktu odniesienia rodzi trzy ryzyka. Po pierwsze, uzależnienie metodyczne od dokumentów tworzonych pod nadzorem instytucji innego porządku prawnego (NIST działa m.in. w reżimie amerykańskich rozporządzeń wykonawczych). Po drugie, rozbieżność z ewoluującym prawem UE (NIS2, akt o cyberodporności, AI Act), którego oficjalne wykładnie tworzy ENISA. Po trzecie, sygnał rynkowy, że europejski ekosystem jest mniej wartościowy niż amerykański. Skoro UE inwestuje we własne ramy, krajowe zestawienie powinno tę autonomię wzmacniać, a nie osłabiać.

5. Wpływ na konkurencyjność polskich MŚP

Obecny kształt zestawienia może osłabić pozycję konkurencyjną małych polskich firm na kilka sposobów:

- **Koszt wejścia**. Polski przedsiębiorca, który potraktuje zestawienie jako wskazówkę, zaczyna od zakupu norm ISO i (zwykle) usług konsultanta. Jego belgijski czy niemiecki konkurent korzysta z bezpłatnego, krajowego narzędzia.
- Różnica w kosztach związanych z zapewnieniem zgodności przekłada się bezpośrednio na poziom cen i marż, a w skrajnych przypadkach może wpływać na zdolność przedsiębiorstwa do utrzymania się na rynku.
- **Efekt łańcucha dostaw**. Duże podmioty KSC będą kaskadować wymagania na dostawców. Jeśli jedynym czytelnym „dowodem" pozostanie certyfikat ISO 27001, małe firmy bez taniego, uznanego, lekkiego dowodu zgodności (jak belgijski CyFun Basic) zostaną wypchnięte z przetargów i z roli poddostawcy.

- **Bariera kompetencyjna i językowa**. Większość pozycji jest anglojęzyczna i pisana językiem ekspertów. Brakuje wskazania zasobów polskojęzycznych i „przetłumaczonych na działanie", co utrwala lukę między dużymi a małymi podmiotami.
- **Brak proporcjonalności**. NIS2 (art. 21) wymaga środków proporcjonalnych do wielkości podmiotu i ekspozycji na ryzyko. Zestawienie nie różnicuje wyraźnie minimum dla mikrofirmy od oczekiwań wobec dużej organizacji, przez co rynek może „domyślnie" podnieść poprzeczkę dla wszystkich. Z tego powodu m.in. wskazanie ISO27001 jako standardu zostało usunięte w jednej z iteracji projektu ustawy zmieniającej KSC. Zaskakuje, że już po przyjęciu ustawy pomysł dużych frameworków napędzany przez ten sam aparat urzędniczy wraca w formie „soft law".

6. Propozycje konkretnych zmian

Wnosimy o uwzględnienie następujących zmian w projekcie zestawienia:

1. Dodać wyraźną warstwę „wejściową dla mikro- i małych przedsiębiorstw". Powinien to być krótki, bezpłatny i polskojęzyczny zestaw mierzalnych środków (wzorem CyFun Small / Basic oraz DIN SPEC 27076), wyraźnie odseparowany od pozycji zaawansowanych.
2. Umieścić jako pierwszy, kluczowy punkt odniesienia wytyczne ENISA do rozporządzenia (UE) 2024/2690, wraz z mapowaniem ich 13 obszarów na 6 obszarów KSC oraz wykorzystaniem zawartych w nich „przykładów dowodów".
3. Dowartościować zasoby europejskie i krajowe (ENISA, ETSI, CEN/CENELEC; inicjatywy typu ShieldNet; materiały NASK/CSIRT, ewentualne polskie tłumaczenia) i tam, gdzie istnieją europejskie odpowiedniki dokumentów amerykańskich: powinny być wskazywane jako preferowane.
4. Wprowadzić dla każdej pozycji informację o koszcie i nakładzie kompetencyjnym (cena zakupu normy, potrzeba konsultanta, certyfikacja), aby MŚP mogły świadomie ocenić realny koszt „pójścia za rekomendacją".
5. Oznaczyć wyraźnie „minimalny zestaw dla mikro/MŚP", mimo ich zakwalifikowania jako kluczowe, realizując zasadę proporcjonalności z art. 21 NIS2.
6. Rozważyć, wzorem belgijskiego CyFun, krajową, lekką ścieżkę dokumentowania należytej staranności dla MŚP, tak aby małe firmy nie były de facto zmuszane do pełnej certyfikacji ISO 27001, zwłaszcza pod presją łańcucha dostaw.
7. Dodać do dokumentu jednoznaczne zastrzeżenie o proporcjonalności i o tym, że spełnienie obowiązków KSC nie wymaga wdrożenia wszystkich wymienionych dokumentów, aby zapobiec uznaniowości podczas kontroli oraz „inflacji wymagań" na rynku i w przetargach.
8. Wskazać polskojęzyczne, bezpłatne źródła wsparcia i diagnostyki dla MŚP (odpowiednik francuskiego MonAideCyber), nawet jeśli miałyby dopiero powstać.

Izby pozytywnie ocenia samą ideę opracowania zestawienia jako narzędzia o charakterze orientacyjnym. W obecnej formie sprzyja ono jednak dużym, dojrzałym organizacjom, podczas gdy małym przedsiębiorstwom – w imię których odstąpiono od ustawowego wymogu stosowania norm ISO – w praktyce wskazuje powrót do tych samych kosztownych i złożonych standardów, uzupełnionych dodatkowo o bardziej wymagające ramy amerykańskie. Jednocześnie pominięto najważniejszy, bezpłatny i unijny punkt odniesienia (wytyczne ENISA do rozporządzenia 2024/2690), a także nie odzwierciedlono lekkich ram dla MŚP stosowanych w innych państwach europejskich, takich jak Belgia, Niemcy czy Francja.

W związku z powyższym postulujemy przeprojektowanie zestawienia w oparciu o zasadę proporcjonalności, priorytetowe uwzględnienie bezpłatnych zasobów europejskich oraz wyraźne wskazanie ścieżki wejściowej dla mikro- i małych przedsiębiorstw. Takie podejście lepiej odpowiada celom ustawy, sprzyja podniesieniu poziomu cyberbezpieczeństwa w gospodarce oraz wspiera konkurencyjność polskiego sektora MŚP.

Pozostajemy do dyspozycji na dalszych etapach prac konsultacyjnych.

Prezes Zarządu

Stefan Kamiński

Signature Not Verified
Dokument podpisany przez Stefan Kamiński
Data: 2026.06.10 10:00:50 CEST
Powód: Złożenie podpisu