Uwagi Polskiej Izby Informatyki i Telekomunikacji do zestawienia wymagań dokumentów normalizacyjnych, których stosowanie wspiera realizację obowiązków wynikających z przepisów ustawy o krajowym systemie cyberbezpieczeństwa

W związku z prowadzonymi przez Ministerstwo Cyfryzacji konsultacjami zestawienia wymagań dokumentów normalizacyjnych, których stosowanie wspiera realizację obowiązków wynikających z przepisów ustawy o krajowym systemie cyberbezpieczeństwa (uKSC), w szczególności dotyczących obowiązków związanych z Systemem Zarządzania Bezpieczeństwem Informacji (SZBI), przekazujemy uwagi PIIT.

W pierwszej kolejności zauważamy, że oparcie organizacji SZBI w danej organizacji na określonych normach i standardach zawsze jest uzależnione od jej specyfiki, profilu ryzyka, a także potrzeb biznesowych. Z tego względu wskazujemy, że zaprezentowane do konsultacji zestawienie, z uwagi na swój przekrojowy charakter nie może być traktowane jako wykaz norm lub standardów, których wykonywanie jest oczekiwane jako realizacja obowiązków wskazanych w znowelizowanej uKSC. Podkreślamy przy tym, że zgodnie z art. 21 ust. 2 dyrektywy NIS2 oraz art. 8 uKSC środki bezpieczeństwa powinny być proporcjonalne do wielkości podmiotu oraz stopnia jego narażenia na ryzyko. Zestawienie nie powinno zatem prowadzić do faktycznego podniesienia poprzeczki dla wszystkich podmiotów ani do „inflacji wymagań" w relacjach rynkowych i w łańcuchu dostaw, w szczególności wobec mikro- i małych przedsiębiorców.

Zauważamy jednocześnie, że zestawienie jest zdecydowanie szersze niż pierwotnie identyfikowane dla uKSC normy ISO27001 i 22301, do których szeroko odwołuje się też konsultowane obecnie rozporządzenie dot. środków technicznych i organizacyjnych do ustawy o zarządzaniu kryzysowym. Widzimy jednocześnie wartość dodaną tak szerokiego zestawienia, które pozwoli bardziej elastycznie korzystać z niego przez organizacje o różnych profilach i poziomach zaawansowania. Dostrzegając tę wartość, zwracamy jednak uwagę, że szerokie zestawienie powinno być czytelnie zhierarchizowane. Wymaga ono wyraźnie wyodrębnionej warstwy wejściowej dla mikro- i małych przedsiębiorców (krótki, bezpłatny i możliwie polskojęzyczny zestaw mierzalnych środków), tak aby domyślnym punktem wyjścia dla najmniejszych podmiotów nie były certyfikowalne i odpłatne normy ISO/IEC ani rozbudowane ramy o rodowodzie pozaeuropejskim. Przypominamy, że w toku prac legislacyjnych odstąpiono od ustawowego odwołania do zgodności z ISO/IEC 27001 m.in. z uwagi na jego złożoność i koszt dla najmniejszych podmiotów. Zestawienie pomocnicze nie powinno tej decyzji w praktyce odwracać.

Z tych względów jednak, za kluczowe uznajemy wprowadzenie jako integralnej części mapowania, publikowanej w BIP na podstawie art. 45 ust. 3 uKSC. Wnosimy więc o wprowadzenie do tej publikacji sformułowania zawartego już w ogłoszeniu konsultacji, tj. że: *Zestawienie będzie miało charakter pomocniczy i informacyjny oraz nie będzie stanowiło źródła powszechnie obowiązującego prawa*. Wnosimy ponadto, aby publikacja wprost zastrzegała, że spełnienie obowiązków wynikających z uKSC nie wymaga wdrożenia wszystkich wymienionych w zestawieniu dokumentów, lecz doboru środków proporcjonalnych do profilu ryzyka i wielkości podmiotu. Zastrzeżenie takie ograniczy uznaniowość w toku kontroli oraz ryzyko nadmiernych żądań w postępowaniach o udzielenie zamówienia.

Zaznaczamy również, że publikacja zestawienia powinna być związana z ustanowieniem procesu jego stałego przeglądu oraz aktualizacji. Postulujemy, aby proces ten obejmował bieżące uzupełnianie zestawienia o lekkie, bezpłatne i polskojęzyczne narzędzia adresowane do mikro- i małych przedsiębiorców (w miarę ich powstawania), a także o europejskie odpowiedniki dokumentów już ujętych w zestawieniu.

W ramach uwag szczegółowych sygnalizujemy:

- Podawane tytuły dokumentów powinny umożliwiać jednoznaczną identyfikację dokumentu. Przykładowo trudny do identyfikacji jest: *ENISA Guidelines for MSPs*. Sugerujemy też używanie pełnych nazw. Przykładowo: OWASP Application Security Verification Standard (ASVS) w miejsce OWASP ASVS. Wnosimy o weryfikację listy pod tym kątem. Dodatkowo wnosimy, aby przy każdej pozycji wskazywać informację o jej dostępności (dokument płatny/bezpłatny), orientacyjnym nakładzie kompetencyjnym (np. potrzeba wsparcia konsultanta, możliwość certyfikacji) oraz o dostępności wersji lub odpowiedników polskojęzycznych. Informacje te pozwolą podmiotom, w szczególności MŚP, realnie ocenić koszt skorzystania z danej rekomendacji.
- Nie odnotowujemy w zestawieniu: ISO/IEC 27018:2025 Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors.
- Dokument pn. *ENISA Guidelines for MSPs,* niezależnie od trudności z jego jednoznaczną identyfikacją, został przypisany jako właściwy dla sektora telekomunikacyjnego (filtrowanie w kolumnie: Sektor). Sygnalizujemy, że jest to przypisanie niewłaściwe i powinno ono być wskazane jako ogólne lub przypisane do niewymienionego jeszcze sektora usług zarządzanych.
- Odnotowujemy, że zestawienie nie identyfikuje sektorów stosujących rozporządzenie wykonawcze do NIS2. Do niego zaś wydane zostało szczegółowe mapowanie oraz wytyczne ENISA. Wnosimy o wyjaśnienie, jaka jest relacja konsultowanego zestawienia do wytycznych i mapowania ENISA. Niezależnie od potrzeby wyjaśnienia tej relacji wnosimy, aby same „Technical Implementation Guidance on cybersecurity risk-management measures" ENISA (wytyczne wdrożeniowe do rozporządzenia wykonawczego Komisji (UE) 2024/2690) zostały włączone do zestawienia jako jeden z kluczowych, wyjściowych punktów odniesienia. Dokument ten jest bezpłatny (licencja CC BY 4.0), dla każdego wymagania podaje praktyczne wskazówki oraz przykłady dowodów zgodności, a także zawiera mapowanie na normy międzynarodowe i krajowe ramy (Aneks I). Celowe byłoby uzupełnienie zestawienia o mapowanie 13 obszarów wymagań tych wytycznych na 6 obszarów uKSC.
- Rekomendujemy uzupełnienie zestawienia o sprawdzone w innych państwach UE, lekkie i bezpłatne ramy adresowane do najmniejszych podmiotów – m.in. belgijski CyberFundamentals (CyFun, z poziomami Small/Basic), niemiecki DIN SPEC 27076 / CyberRisikoCheck oraz francuski model wsparcia MonAideCyber. Mogą one stanowić wzorzec krajowej, lekkiej ścieżki dokumentowania należytej staranności, dzięki której małe firmy nie będą de facto zmuszane do pełnej certyfikacji ISO/IEC 27001, w szczególności pod presją wymagań kaskadowanych w łańcuchu dostaw.
- Wnosimy o dowartościowanie zasobów europejskich i krajowych (m.in. ENISA, ETSI, CEN/CENELEC, materiały NASK/CSIRT oraz ewentualne polskie tłumaczenia). Tam, gdzie dla dokumentów o rodowodzie pozaeuropejskim istnieją równoważne odpowiedniki europejskie, sugerujemy wskazywanie tych ostatnich jako preferowanych – z uwagi na ich spójność z ewoluującym prawem UE (NIS2, akt o cyberodporności) – bez postulatu usuwania pozostałych, użytecznych materiałów.
- Wnosimy o wskazanie (lub docelowo utworzenie) bezpłatnych, polskojęzycznych źródeł wsparcia i diagnostyki cyberbezpieczeństwa dla MŚP, na wzór francuskiego MonAideCyber, obniżających barierę kompetencyjną i językową dla najmniejszych podmiotów.