2025

Fundusze Europejskie

Urząd Zamówień Publicznych

# Zabezpieczenie łańcucha dostaw w zamówieniach publicznych

## Aspekty prawne, organizacyjne i techniczne w świetle przepisów krajowych i unijnych dotyczących cyberbezpieczeństwa

Autorzy:

Monika Bratek-Charzyńska, NASK

Piotr Rolek, NASK

Szymon Skalski, Uniwersytet Jagielloński

# Spis treści

WYKAZ SKRÓTÓW

**Instytucje, organy, organizacje, podmioty**

| | |
|---|---|
| ENISA | European Union Agency for Security Europe |
| GPA | Porozumienie GPA Porozumienie w sprawie Zamówień Rządowych (Government Procurement Agreement) |
| KE | Komisja Europejska |
| KNF | Komisja Nadzoru Finansowego |
| KIO | Izba Krajowa Izba Odwoławcza |
| NIST | National Institute of Science and Technology |
| PCA | Polskie Centrum Akredytacji |
| Prezes KIO, | Prezes Izby Prezes Krajowej Izby Odwoławczej |
| Prezes Urzędu | Prezes Urzędu Zamówień Publicznych |
| TSUE, Trybunał | Trybunał Sprawiedliwości Unii Europejskiej |
| UZP, Urząd | Urząd Zamówień Publicznych |
| WSA | Wojewódzki Sąd Administracyjny |
| WEF | World Economic Forum |

**Definicje operacyjne**

| | |
|---|---|
| CAP | (Corrective Action Plan) plan działań korygujących: zestaw uzgodnionych kroków, terminów i odpowiedzialności służących trwałemu usunięciu przyczyny niezgodności lub incydentu oraz weryfikacji skuteczności wdrożonych zmian |
| CESIRT | (*Computer Security Incident Response Team)* (zespół reagowania na incydenty bezpieczeństwa). Jednostka koordynująca obsługę |

| | |
|---|---|
| | incydentów: przyjmowanie zgłoszeń, triage, analizę, ograniczanie skutków i komunikację |
| CVSS | (Common Vulnerability Scoring System) ujednolicony system oceny istotności podatności; dostarcza liczbowej skali (0–10) i wektorów, na podstawie których priorytetyzuje się wdrażanie poprawek bezpieczeństwa i innych środków zaradczych |
| GRC | (Governance, Risk, Compliance) – ład, ryzyko i zgodność: zintegrowany obszar obejmujący mechanizmy zarządcze, procesy oceny i traktowania ryzyka oraz spełnianie wymagań prawnych i normatywnych |
| KRI | (Key Risk Indicator) kluczowy wskaźnik ryzyka: mierzalna miara sygnalizująca zmianę profilu ryzyka (np. terminowość wdrażania poprawek bezpieczeństwa, wzrost liczby incydentów), powiązana z progami i działaniami reakcyjnym |
| MTTD/MTTR | (Mean Time to Detect / Mean Time to Respond/Recover) średni czas wykrycia oraz średni czas reakcji/odtworzenia: metryki operacyjne SOC/IR pokazujące sprawność detekcji i przywracania działania usług |
| RACI | (Responsible, Accountable, Consulted, Informed) macierz ról i odpowiedzialności: określa, kto wykonuje zadanie, kto ponosi odpowiedzialność, kogo konsultować i kogo informować |
| RTO/RPO | (Recovery Time Objective / Recovery Point Objective) docelowy czas odtworzenia i docelowy punkt odtworzenia: maksymalny akceptowalny czas przerwy oraz dopuszczalna utrata danych liczona wstecz od chwili zdarzenia |
| SBOM | (Software Bill of Materials) wykaz komponentów oprogramowania (biblioteki, zależności, wersje, pochodzenie); ułatwia zarządzanie podatnościami, zgodnością licencyjną i ocenę wpływu zmian |
| SCADA | (Supervisory Control And Data Acquisition) systemy nadzorująco-sterujące wykorzystywane w środowiskach OT/ICS; w kontekście |

| | |
|---|---|
| | bezpieczeństwa wymagają szczególnych zasad segmentacji, |
| SSDLC | monitoringu i aktualizacji<br>(Secure Software Development Life Cycle) bezpieczny cykl życia wytwarzania oprogramowania: zestaw praktyk (m.in. analiza wymagań, modelowanie zagrożeń, SAST/DAST, przeglądy kodu, testy, kontrola zmian), które wbudowują bezpieczeństwo w proces wytwórczy |

**Źródła prawa**

| | |
|---|---|
| Pzp, ustawa Pzp | ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych<br>(Dz. U. z 2024 r. poz. 1320 z późń. zm.) |
| UKSC, KSC, ustawa KSC | ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 z późń. zm.) |
| Ustawa o certyfikacji | Ustawa z 5 sierpnia 2025 r. o certyfikacji wykonawców w zamówieniach publicznych |
| UOIN | ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2025.1209 t.j. z dnia 2025.09.02 |
| dyrektywa 2009/43/WE | dyrektywa Parlamentu Europejskiego i Rady 2009/43/WE z dnia 6 maja 2009 r. w sprawie uproszczenia warunków transferów produktów związanych z obronnością we Wspólnocie (Dz. Urz. UE L 146 z 10.6.2009, str. 1, z późn. zm.) |
| dyrektywa klasyczna | dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz. Urz. UE L 94 z 28.3.2014, str. 65, z późn. zm.) |
| dyrektywa koncesyjna | dyrektywa Parlamentu Europejskiego i Rady 2014/23/UE z dnia 26 lutego 2014 r. w sprawie udzielania koncesji (Dz. Urz. UE L 94 z 28.3.2014, str. 1, z późn. zm.) |
| dyrektywa obronna | dyrektywa Parlamentu Europejskiego i Rady 2009/81/WE z dnia 13 lipca 2009 r. w sprawie koordynacji procedur udzielania |

| | |
|---|---|
| | niektórych zamówień na roboty budowlane, dostawy i usługi przez instytucje lub podmioty zamawiające w dziedzinach obronności i bezpieczeństwa i zmieniająca dyrektywy 2004/17/WE i 2004/18/ WE (Dz. Urz. UE L 216 z 20.08.2009, str. 76, z późn. zm.) |
| dyrektywa sektorowa | dyrektywa Parlamentu Europejskiego i Rady 2014/25/UE z dnia 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylająca dyrektywę 2004/17/WE (Dz. Urz. UE L 94 z 28.3.2014, str. 243, z późn. zm.) |
| TFUE | Traktat o funkcjonowaniu Unii Europejskiej, wersja skonsolidowana 2016 (Dz. Urz. UE C 202 z 7.6.2016, str. 1) TUE Traktat o Unii Europejskiej, wersja skonsolidowana 2016 (Dz. Urz. UE C 202 z 7.6.2016, str. 1) |
| RODO | rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1, z późn. zm.) |
| rozporządzenie w sprawie podmiotowych środków dowodowych | rozporządzenie Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. 2020 poz. 2415 ze zm.) |
| rozporządzenie w sprawie wzoru planu postępowań o udzielenie zamówień | rozporządzenie Ministra Rozwoju, Pracy i Technologii z dnia 18 grudnia 2020 r. w sprawie wzoru planu postępowań o udzielenie zamówień (Dz. U. z 2020 r. poz. 2362) |
| rozporządzenie 428/2009 | rozporządzenie Rady (WE) nr 428/2009 z dnia 5 maja 2009 r. ustanawiające |

| | |
|---|---|
| | wspólnotowy system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania (wersja przekształcona) (Dz. Urz. UE L 134 z 29.05.2009, str. 1, z późn. zm.) |
| Akt ws. Cyberbezpieczeństwa | rozporządzenie parlamentu europejskiego i rady w sprawie „Agencji UE ds. Cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa") COM/2017/0477 final/3 - 2017/0225 (COD) |
| rozporządzenie 2019/881 | rozporządzenie parlamentu europejskiego i rady (ue) 2019/881z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) |
| akt o cyberodporności, „CRA") | rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi |
| rozporządzenie 2024/2690 | wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, |

dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania

# 1. Wprowadzenie do zagadnienia zabezpieczenia łańcucha dostaw w systemie zamówień publicznych

## 1.1. Definicja i znaczenie łańcucha dostaw w kontekście zamówień publicznych.

Zapewnienie bezpieczeństwa łańcucha dostaw pozostaje tematem tak starym jak międzynarodowa wymiana handlowa, jednakże w dynamicznie rozwijającym się świecie cyfrowym pojawiły się nowe wyzwania, z którymi przyjdzie zmierzyć się zamawiającym i wykonawcom.

W celu uporządkowania dalszego wywodu zacząć najlepiej jest od wyjaśnienia podstawowych definicji, które przewijać się będą w dalszej części publikacji. Pojęcie łańcucha dostaw spotka się w ramach dziedziny nauki nazywanej logistyką, którą najkrócej zdefiniować można jako proces planowania, realizowania i kontrolowania sprawnego i efektywnego ekonomicznie przepływu surowców, materiałów, wyrobów gotowych oraz odpowiedniej informacji z punktu pochodzenia do punktu konsumpcji w celu zaspokojenia wymagań klienta, a ważnym elementem tego procesu jest bezsprzecznie łańcuch dostaw.

Pochylając się nad definicjami samego łańcucha dostaw należy zauważyć, że nauka wypracowała ich wiele np. według M. Fertscha, łańcuch dostaw to grupa przedsiębiorstw realizująca działania niezbędne do zaspokojenia popytu na określone produkty w całym łańcuchu przepływu dóbr – od pozyskania surowców po dostawę do ostatecznego odbiorcy. Działania te obejmują: rozwój, produkcję, sprzedaż, serwis, zaopatrzenie, dystrybucję, zarządzanie zasobami i różne procesy wspomagające. W ujęciu tym należy zaakcentować trzy ważne stwierdzenia, które pomagają zrozumieć działanie łańcucha dostaw:

- Łańcuch dostaw to grupa przedsiębiorstw – a więc, żeby istniał łańcuch dostaw potrzebne są przynajmniej dwa osobne przedsiębiorstwa,
- przedsiębiorstwa w łańcuchu dostaw współpracują ze sobą - współpraca ta opiera się przeważnie na długoterminowych umowach, zawieranych przynajmniej na okres roku,

- współpraca przedsiębiorstw w łańcuchu dostaw może dotyczyć różnych sfer ich działania[1].

W kontekście choćby powyższej definicji zamówienia publiczne pozostają jednym z kluczowych narzędzi działających w ramach łańcucha dostaw i na nie oddziałują, gdyż:

- aranżują i regulują współpracę podmiotów biorących udział w realizowaniu zamówień -wykonawców, podwykonawców, konsorcjantów, korzystających z zasobów podmiotów trzecich między sobą i z zamawiającymi,
- regulują stosunki gospodarcze istotnie wpływając na wspólny rynek poprzez zawieranie długoterminowych kontraktów.
- łączą poprzez stymulację rynku różne podmioty, które w celu uzyskania i realizacji zamówienia tworzą struktury organizacyjne współpracujące w cyklu od wytworzenia, rozwoju, poprzez serwis, wsparcie, utrzymanie, aż do zakończenia cyklu życia produktu.

Przytoczona definicja jest tylko jedną i przykładową z wielu funkcjonujących we współczesnej logistyce, która pozostaje dziedziną interdyscyplinarną i kompleksową, co powoduje, że pojęcie łańcucha dostaw posiada różnorodne definicje, w tym także jedną stworzoną na potrzeby zamówień publicznych. Zgodnie z art. 7 pkt 10 ustawy Pzp przez łańcuch dostaw należy rozumieć wszystkie zasoby i działania niezbędne do wykonywania dostaw, usług i robót budowlanych, które są przedmiotem zamówienia. Jednakże nie jest przedmiotem tego opracowania ich przytaczanie, gdyż docelowo omówione zostaną kwestie związane z wyzwaniami pojawiającymi się w cyberprzestrzeni i ze strony cyberprzestrzeni.

Dlatego też na potrzeby niniejszej publikacji używana będzie definicja lepiej dopasowana do zjawisk występujących w cyberprzestrzeni, obejmująca Digital Supply Chain zawarta w NIST SP 800 -161r1 wer. 1.0 PL:

**Cyfrowy łańcuch dostaw** (eng. *Digital Supply Chain*)
[ENG] *linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of digital products and services and extends through development, sourcing, manufacturing, handling, and delivery of digital products and services to the acquirer.*

[1] M. Fertsch, Podstawy logistyki, Wydawnictwo Instytut Logistyki i Magazynowania, Poznań 2008, s. 175.

[PL] zestaw powiązanych zasobów i procesów między nabywcami, integratorami i dostawcami, który rozpoczyna się od projektowania produktów i usług cyfrowych, a następnie obejmuje rozwój, pozyskiwanie, produkcję, obsługę i dostarczanie produktów i usług cyfrowych do nabywcy.

Jednocześnie zauważyć należy, że ryzyko związane z cyberbezpieczeństwem może pojawić się we wszystkich łańcuchach dostaw produktów i usług, w tym zarówno w łańcuchach dostaw ICT, jak i łańcuchach dostaw niezwiązanych z technologią.

**Jakie pojęcia są jeszcze istotne?**

Dla lepszego zrozumienia skomplikowanej materii jaką jest cyberbezpieczeństwo łańcucha dostaw warto wyjaśnić następujące pojęcia:

- **Certyfikacja -** kompleksowa ocena (audyt) zarządzania, operacyjnych i technicznych środków kontroli bezpieczeństwa w systemie informatycznym, przeprowadzana na potrzeby akredytacji bezpieczeństwa, mająca na celu określenie, w jakim stopniu środki kontroli są wdrażane prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądane efekty w zakresie spełnienia wymagań bezpieczeństwa systemu.[2] W obszarze cyberbezpieczeństwa jest narzędziem, które pozwala sprzedawcom produktów i dostawcom usług prezentować i reklamować cyberbezpieczeństwo swoich rozwiązań.
- **Cyberbezpieczeństwo -** odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność, przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.**[3]** lub działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami.[4]

[2] ang. Certification - a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.- NIST Special Publication 800-60 Volume II Revision 1, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, author Kevin Stine Rich Kissel William C. Barker Annabelle Lee Jim Fahlsing, August 2008, [on line] dostępne 12.11.2025 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

[3] UKSC (art. 2 pkt 4)

[4] Rozporządzenie 2019/881

- **Cyberprzestrzeń -** środowisko (na które składa się ląd, woda, powietrze, kosmos oraz pole elektromagnetyczne) i umieszczone w tym środowisku obiekty posiadające zdolność kształtowania pola elektromagnetycznego i wykrywania jego zmian oraz magazynowania informacji o tych zmianach,[5] lub inna definicja - złożone środowisko, powstałe w wyniku interakcji ludzi, oprogramowania i usług w Internecie za pośrednictwem urządzeń technologicznych i sieci z nim połączonych, które nie istnieje w żadnej formie fizycznej[6] .
- **Cyberodporność -** Cyberodporność to zdolność do przewidywania, przetrwania, odbudowy i dostosowania się do niesprzyjających warunków, obciążeń, ataków lub kompromitacji systemów.[7]
  które wykorzystują zasoby cyfrowe lub są przez nie obsługiwane.
- **Cyberhigiena** – zwana także higieną cyfrową to zbiór dobrych praktyk, których celem jest zabezpieczenie użytkowników, urządzeń, sieci i danych przed zagrożeniami, jakie niosą ze sobą cyberataki**.**
- **Cyberzagrożenie -** wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób[8].
- **C-SCRM** - zarządzanie ryzykiem dotyczącym cyberbezpieczeństwa w łańcuchu dostaw cybersecurity supply chain; (ang. cybersecurity supply chain risk management- C-SCRM).
- **Proces ICT** − proces ICT w rozumieniu art. 2 pkt 14 rozporządzenia 2019/881, oznacza zestaw czynności wykonywanych w celu projektowania,

---

[5] Cyberbezpieczeństwo łańcuchów dostaw, Supply chain cybersecurity aut.
Krzysztof Liderman , Artur Księżopolski Cybersecurity & Cybercrime, rocznik 2025, t. 1., Nr 8 [online dostęp 12.11.2025 r.]

[6] ang. cyberspace is the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form - NISTIR 8074, Volume 2, Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity [on line] dostępne 12.11.2025) http://dx.doi.org/10.6028/NIST.IR.8074v2

[7] NIST Special Publication 800-160, Volume 2 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, w oryginale: Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources

[8] art. 2 pkt 7 rozporządzenia 2019/881

rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT np. kolokacja.

- **Produkt ICT**− produkt ICT w rozumieniu art. 2 pkt 12 rozporządzenia 2019/881, oznacza element lub grupę elementów sieci lub systemów informatycznych np.: serwery, rutery, przełączniki sieciowe.
- **Produkt z elementami cyfrowymi** - oprogramowanie komputerowe lub sprzęt komputerowy oraz powiązane z nimi rozwiązania w zakresie zdalnego przetwarzania danych, w tym komponenty oprogramowania lub sprzętu, które są oddzielnie wprowadzane do obrotu w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi (akt o cyberodporności, „CRA").
- **Usługa ICT −** usługa ICT w rozumieniu art. 2 pkt 13 rozporządzenia 2019/881, oznacza usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem sieci i systemów informatycznych np. usługa chmurowa SaaS.

Niemal każdy podmiot publiczny i prywatny w dwudziestym pierwszym wieku wchodzi w skład mniej lub bardziej skomplikowanego ekosystemu korzystającego z Technologii informacyjno-komunikacyjnych (ICT) oraz technologii operacyjnych i procesów przemysłowych (ang. operational technology – OT). Efektem wzajemnych powiązań technologicznych jest wytworzenie różnego rodzaju relacji ekonomicznych pomiędzy podmiotami z sektora publicznego i prywatnego w tym między innymi dostawcami produktów ICT, usług ICT oraz procesów ICT. Te interakcje funkcjonują w bardzo złożonym i wielowymiarowym środowisku kształtowanym przez przepisy prawa, polityki, praktyki, standardy i wytyczne oraz przez samą technologię. Jednym z elementów mającym wpływ na ten łańcuch wzajemnych powiązań jest prawo regulujące sposób nabywania produktów ICT, usług ICT oraz procesów ICT przez podmioty sektora publicznego. Niniejsza publikacja skoncentrowana będzie przede wszystkim na analizie polskiego i europejskiego krajobrazu zamówień publicznych i ich nierozerwalnego związku z zapewnieniem możliwie najlepszego bezpieczeństwa łańcucha dostaw w obszarze cyberbezpieczeństwa.
W tak skomplikowanym otoczeniu zrodziły się liczne zagrożenia, z którymi zarówno poszczególne kraje jak i same podmioty tworzące cyfrowe łańcuchy dostaw muszą się mierzyć.

### 1.2. Ryzyka i zagrożenia związane z łańcuchem dostaw z perspektywy cyberbezpieczeństwa.

Zagrożenia bezpieczeństwa sieci i systemów teleinformatycznych są niezwykle różnorodne i mogą być zarówno pochodzenia naturalnego jak i wykreowane przez człowieka. Do zdarzeń, które należy uwzględniać budując cyberodporność instytucji ustawodawca unijny zaliczył np. „kradzież, pożar, powódź, awaria telekomunikacyjna bądź awaria zasilania lub nieuprawniony dostęp fizyczny do infrastruktury związanej z informacjami i przetwarzaniem informacji należącej do podmiotu kluczowego lub ważnego, jej uszkodzenie i ingerencja w nią, które to zdarzenia mogłyby naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub też usług oferowanych przez sieci i systemy informatyczne lub dostępnych za pośrednictwem sieci i systemów informatycznych”[9].

Jednym z wyjątkowo newralgicznych obszarów, w którym zdiagnozowano liczne ryzyka, jest właśnie łańcuch dostaw usług ICT, produktów ICT i procesów ICT[10]. W podstawowym dla europejskiego cyberbezpieczeństwa akcie prawnym – dyrektywie NIS 2 podkreślono, że w ostatnich latach kraje UE doświadczają gwałtownego wzrostu liczby cyberataków. Zwłaszcza podatne na ataki są małe i średnie przedsiębiorstwa, czy nieduże podmioty publiczne ze względu na ich ograniczania organizacyjne, finansowe i technologiczne. Podobną diagnozę zaprezentowano w Raporcie “Global Cybersecurity Outlook 2025” przygotowanym na zlecenie Światowego Forum Ekonomicznego wskazując, że

“*Wraz ze wzrostem złożoności cyberprzestrzeni może ona potencjalnie pogłębiać nierówności w cyberprzestrzeni w przypadku organizacji, które nie są w stanie sprostać rosnącym wyzwaniom*.”[11] ,

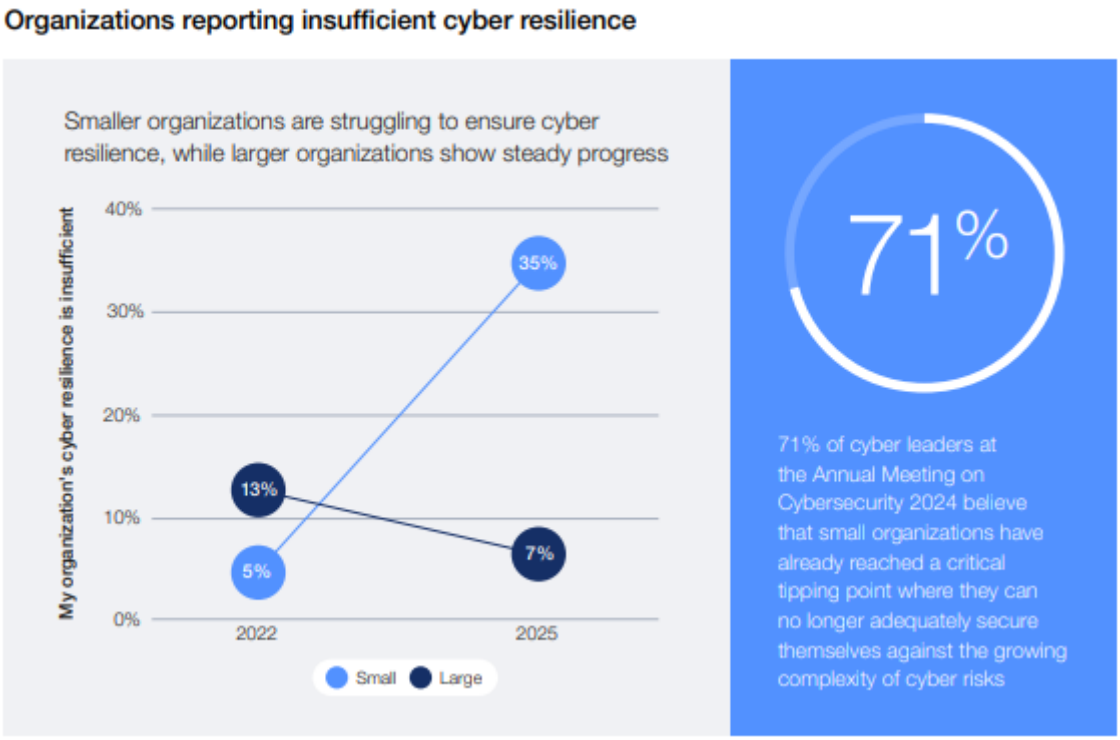
co znajduje odzwierciedlenie w dokonanej dla WEF analizie, której wynik znajduje odzwierciedlenie w poniższej grafice:

---

[9] Motyw 79 NIS2.

[10] Zob. Motyw 54 NIS2.

[11] World Economic Forum, *Global Cybersecurity Outlook 2025. Insight Report*, January 2025, s. 8, [online:] https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ oraz PDF: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf [dostęp: 12.11.2025].




Rys. 1 WEF_Global_Cybersecurity_Outlook_2025

Z powyższego raportu wynika, że 45% bardzo dużych organizacji identyfikuje wyzwania związane z łańcuchem dostaw jako największą barierę w osiągnięciu cyberodporności[12]. Nie ulega zatem wątpliwości, że małym i średnim podmiotom, trudno jest samodzielnie zapewnić odpowiednie zaplecze ekonomiczne, dydaktyczne czy technologiczne, aby mogły bezpiecznie rozwijać się i konkurować swobodnie na rynku europejskim. Także zamawiający pragnący dokonywać bezpiecznych zakupów usług ICT, procesów ICT czy produktów ICT potrzebują holistycznego wsparcia ze względu na skomplikowany wymiar ekosystemu łańcucha dostaw. Dlatego też w ustawodawstwie unijnym znalazły się zalecenia wobec państw członkowskich, aby opracowały krajowe strategie cyberbezpieczeństwa, które pomagałyby reagować na wyzwania związane z zabezpieczeniem łańcucha dostaw w ramach szerszego planu budowy krajowej i unijnej cyberobrony.

Jako fundament formowania szeroko rozumianej cyberobrony przyjmuje się wspieranie i rozwijanie kultury zarządzania ryzykiem, obejmującą szacowanie ryzyka oraz wdrażanie odpowiednich dla minimalizacji danego ryzyka środków

[12] WEF, *Global Cybersecurity Outlook 2025*, 2025, s. 12.

zarządzania. Ustawodawstwo unijne zmierza w kierunku dynamicznego i kompleksowego rozwoju zarządzania ryzykiem w obszarze cyberbezpieczeństwa, a dyrektywa NIS 2 i towarzyszące jej rozporządzenie wykonawcze, czy CRA są tego wyrazistymi przykładami.

Choć sama dyrektywa NIS 2 dotyczy podmiotów uznanych za ważne i kluczowe, to należy się spodziewać, że przewidziane w niej wymagania (w tym zwłaszcza środki zarządzania ryzykiem w cyberbezpieczeństwie) będą kaskadowo stawiane przez zamawiających także wykonawcom oraz podwykonawcom, a tym samym zasady zarzadzania ryzykiem wynikające z NIS 2 zostaną faktycznie implementowane zarówno w przypadku podmiotów objętych Dyrektywą NIS 2 jak również wyłączonych spod tej regulacji.

Transpozycja dyrektywy NIS 2 w polskim porządku prawnym dokona się poprzez nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa (dalej ustawa o KSC), która w momencie redagowania niniejszej publikacji wkracza w etap prac sejmowych, dlatego nie można jeszcze dokładnie określić skali jej wpływu na rynek zamówień publicznych, jednakże mimo że projektowana ustawa nie została jeszcze uchwalona, z lektury jej kolejnych odsłon wyłania się jeden wniosek - liczba podmiotów objętych obowiązkami zadbania o cyberbezpieczeństwo łańcucha dostaw ulegnie znacznemu zwiększeniu i dotknie wielu podmiotów publicznych w tym jednostek administracji publicznej oraz podmiotów im podległych lub przez nie nadzorowanych. Tym samym ustawa – Prawo zamówień publicznych stanie się ważnym narzędziem, którym będą musieli się posługiwać zamawiający i wykonawcy, aby sprostać wymaganiom wynikającym z wymogów prawnych jak również orężem w walce z zagrożeniami związanymi z funkcjonowaniem w złożonym ekosystemie łańcucha dostaw.

### 1.2.1. Klasyfikacja ryzyk

Jak już wspomniano cyfrowy łańcuch dostaw jest ekosystemem wielowymiarowym i skomplikowanym, dlatego też podatnym na zagrożenia o różnym charakterze. Wrogie podmioty wykorzystują najnowsze technologie, które obniżają koszty kampanii phishing'owych, czy socjotechnicznych, co powoduje, że skala zagrożeń, jak również ich kwalifikacja będzie ewoluować uwzględniając chociażby wykorzystanie narzędzi SI, do projektowania ataków. Szybko rosnącym modelem biznesowych cyberprzestępczości jest chociażby oferowanie usług w modelu Cybercrime-as-a-Service (CaaS), które umożliwia przeprowadzanie ataków

nawet podmiotom pozbawionym technologicznych kompetencji[13]. Skupiając się przede wszystkim na zagrożeniach płynących z działalności lub zaniechań człowieka, podejmowane są próby dokonania ich klasyfikacji. Za cyberzagrożenie uznaje się zgodnie z Rozporządzeniem 2019/881 wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób. Jednym z głównych zagrożeń są cyberataki.

Istnieją różne klasyfikacje cyberataków na łańcuch dostaw, przy czym ENISA[14] proponuje podział na cztery części:

1. Techniki ataków stosowanych wobec dostawców (infekcja złośliwym oprogramowaniem (malware), inżynieria społeczna, atak siłowy (brute-force), wykorzystanie luk w oprogramowaniu, wykorzystanie luk w konfiguracji, atak fizyczny lub modyfikacja fizyczna, OSINT (wywiad z otwartych źródeł), fałszowanie (np. dokumentów, komponentów).
2. Zasoby atakowane u dostawców (istniejące oprogramowanie, biblioteki programistyczne, kod źródłowy, konfiguracje, dane, procesy, sprzęt, ludzie),
3. Techniki ataków stosowane wobec klientów (wykorzystanie zaufanej relacji, kompromitacja przez odwiedzenie zainfekowanej strony (drive-by), phishing, infekcja złośliwym oprogramowaniem, atak fizyczny lub modyfikacja fizyczna, fałszowanie.
4. Zasoby atakowane u klientów (dane, dane osobowe, procesy, oprogramowanie, zasoby finansowe, ludzie, przepustowość (np. sieciowa).[15]

---

[13] Europol. (2024, April 18). International investigation disrupts phishing-as-a-service platform LabHost. https://www.europol. europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost.

[14]ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, *Threat Landscape for Supply Chain Attacks*, 29 lipca 2021, s. 6–7, [online:] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks oraz PDF: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf [dostęp: 12.11.2025].

[15] W oryginale:

1. Attack techniques used on the supplier (ex. maleware Infection, Social Engeneering, Brute - Force Attack, Exploiting Software Vulnerability, Exploiting Configuration Vulnerability, Physical Attack or Modification, OSINT, Counterfiting,

Wspólną cechą wszystkich ataków na cyfrowy łańcuch dostaw jest ich dwuetapowość. W pierwszej kolejności celem jest dostawca, producent danego rozwiązania, aby za jego pośrednictwem zaatakować docelowy podmiot – klienta. Odwrotny wektor ataku przewiduje skompromitowanie klienta, aby wykorzystać jego infrastrukturę do przeprowadzenia ataku na np. informacje strategiczne, dane osobowe, własność intelektualną, oprogramowanie, środki finansowe, personel dostawcy/producenta. Inne podejście do kwalifikacji prezentuje MITRE ATT&CK®[16].

Nie ulega wątpliwości, że każdy zamawiający czy wykonawca dokonujący analizy podatności swojej infrastruktury IT/OT na cyberzagrożenia powinien uwzględniać ryzyka materializujące się w różnych obszarach.

### 1.2.2. Obszar korzystania z oprogramowania, w którym spotyka się:

**Ataki na oprogramowanie wykonawców lub podwykonawców w celu dotarcia do infrastruktury ich klientów**

**Opis:** Cyberprzestępcy już jakiś czas temu zauważyli, że uzyskując dostęp do infrastruktury producenta oprogramowania mogą włamać się do jego systemów, wstrzyknąć złośliwy kod, który następnie będzie dystrybuowany do odbiorców końcowych użytkującego konkretny program. Celem takich ataków jest zazwyczaj szpiegostwo lub uzyskanie okupu poprzez atak typu ransomware. Wykorzystywanie systemów podmiotów znajdujących się w łańcuchu dostaw oprogramowania, którzy nie zabezpieczyli się wystarczająco przed takim ryzykiem, staje się coraz częstszym wektorem ataków. Ofiarami padają nawet podmioty profesjonalnie podchodzące do zagadnień cyberbezpieczeństwa.

Zagrożenie tego typu dotyczyć może także oprogramowania zamkniętego, zawierającego podatności 0-day, jak również otwartego, gdzie nie tylko cyberprzestępcy, ale nawet programiści producenta celowo lub przypadkowo na

2. Assets attacked in the supplier (ex. Pre-existing Software, Software Libraries, Code,Configurations, Data, Processes, Hardware, people,
3. Attack techniques used on the customer (ex. Trusted Relationship, Drive-by Compromise, Phishing, Malware Infection, Physical Attack or Modification, Counterfiting
4. Assets attacked in the customer (ex. Data, Peronal Data, Processes, Software, financial, people, Bandwidth)

ENISA, *Threat Landscape for Supply Chain Attacks*, 2021, s. 6–7.

[16] MITRE, *ATT&CK Matrix for Enterprise*, [online:] https://attack.mitre.org/ [dostęp: 12.11.2025].

potrzeby testowania mogą zainstalować ukryty mechanizm dający nieautoryzowany dostęp do systemów. Dlatego też zamawiający powinni zwracać uwagę na takie ryzyko przy wyborze wykonawcy i uwzględniać je w projektowanych strategiach bezpieczeństwa łańcucha dostaw. Ważne przy współpracy z dostawcami oprogramowania/sprzętu/procesów jest ich udokumentowane doświadczenie. Ponadto istotne jest też ustalenie, kto ponosi odpowiedzialność za dane oprogramowanie/urządzenie (czasami są to fundacje lub organizacje typu non – profit). Posiadanie takiej wiedzy, pozwala zarządzić ryzykiem geopolitycznym (np. producent oprogramowania/urządzenia pochodzi z kraju objętego sankcjami lub uznanego za wrogi).

**Przykład:** Jednym z najbardziej spektakularnych incydentów typu atak na łańcuch dostaw (Supply Chain Attack) był atak na amerykańską firmę technologiczną SolarWinds produkującą oprogramowanie "Orion" do zarządzania sieciami. Hakerzy uzyskali dostęp do wewnętrznej infrastruktury deweloperskiej firmy i wstrzyknęli złośliwy kod do aktualizacji oprogramowania służącego do administrowaniem siecią IT. Następnie zainfekowana aktualizacja została pobrana przez klientów firmy i zainstalowana na ich infrastrukturze. Przez miesiące niewykryte, złośliwe oprogramowanie (tzw. Sunburst backdoor), zbierało informacje o wytypowanych przez przestępców instytucjach w tym amerykańskich agencjach rządowych. Ślady prowadziły do rosyjskiej grupy APT Cozy Bear[17], która przeprowadziła ten niezwykle skomplikowany atak w celach szpiegowskich, na co wskazuje brak wyrządzonych szkód w infrastrukturze ofiar.

**Nieaktualne oprogramowanie u podmiotów trzecich**

**Opis:** Dostawcy, którzy nie aktualizują używanego oprogramowania, pozostawiają znane wrogim podmiotom luki bezpieczeństwa, a te mogą zostać użyte do ataku.

**Przykład**: Wykorzystanie przez wrogie podmioty niezaktualizowanego oprogramowania używanego w KNF. Przestępcy wykorzystali tę podatność by zaatakować instytucje finansowe, które były ich głównym celem. Wykorzystując nieaktualizowaną aplikację strony umieszczono w niej dodatkowy kod, który był wykonywany na każdym komputerze odwiedzającym daną stronę, oprócz

[17] APT - (Advanced Persistent Threat) -zorganizowane grupy hakerów używające wyrafinowanych technik cyberataków.

wyświetlenia jej standardowej zawartości. Tego typu dystrybucja malware nosi nazwę metody wodopoju (ang. watering hole). Polega na tym, że przestępca zamiast próbować bezpośrednio dotrzeć do ofiary, kompromituje miejsca, które ona zazwyczaj odwiedza, przez co atakowany nie zachowuje typowej podejrzliwości i realizuje scenariusz zgodnie z oczekiwaniami agresora („każdy kto przyjdzie i skorzysta z zatrutego źródła zostanie zatruty"). Ta metoda infekcji wykorzystuje przeświadczenie użytkownika Internetu o tym, że serwis, z którego korzysta jest bezpieczny. W tym konkretnym przypadku wykorzystano zaufanie użytkowników do regulatora rynku (jakim jest KNF).[18]

**Ryzyko**: Atakujący może dostać się do systemu przez podatność, która została dawno załatana, ale nie u dostawcy. Mając tego typu ryzyko na uwadze zamawiający i wykonawcy powinni weryfikować przed nawiązaniem relacji biznesowej, czy dany dostawca przykłada należytą wagę do cyberbezpieczeństwa w swojej organizacji np. szkoli pracowników w zakresie cyberhigieny, stosuje standardy typu NIST SP 800-218, zezwala na wgląd w proces wytwarzania oprogramowania (Secure Software Development Life Cycle (SSDLC) itp.

### 1.2.3. Obszar korzystania z komponentów, w którym ma miejsce:

**Podrabianie lub umieszczanie komponentów służących wrogim podmiotom**

**Opis**: Urządzenia i ich komponenty fizyczne dostarczane zamawiającym przez wykonawców/podwykonawców mogą zawierać ukryte funkcje umożliwiające zdalne sterowanie lub wyciek danych. Zagrożona tego typu elementami jest zwłaszcza infrastruktura krytyczna (np. telekomunikacja, energetyka).

**Zagrożenie:** wrogie podmioty mogą w sposób zdalny doprowadzić do awarii lub zniszczenia infrastruktury krytycznej, przejęcia wrażliwych danych, wykradzenia środków finansowych. Przykładem tego typu zdarzeń jest wykrycie w maju 2025 roku przez amerykańskich urzędników w inwerterach i bateriach słonecznych (producentów takich jak Huawei, Sungrow, Ginlong Solis) ukrytych urządzeń komunikacyjnych. Komponenty te potencjalnie umożliwiały omijanie zapór i

[18] Artur Maciąg, Ireneusz Tarnowski, *Atak teleinformatyczny na polski sektor finansowy*, Rządowe Centrum Bezpieczeństwa, [online:] https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [dostęp: 12.11.2025].

zdalną kontrolę nad infrastrukturą zasilającą[19]. To sytuacja klasyfikowana jako możliwy hardware-based backdoor w panelach fotowoltanicznych - urządzenia telekomunikacyjne, które nie były opisane w żaden sposób w dokumentacji technicznej urządzeń[20]. Niezwykle trudno bronić się przed tak zaawansowanymi atakami, które opierają się na zainstalowaniu w najróżniejszych urządzeniach (od chipów w płytach głównych, specjalnych układów w sprzęcie korzystającym z bluetooth, sprzęcie medycznym, po urządzenia wchodzące w infrastrukturę energetyczną) komponentów niewiadomego użycia. Zarówno zamawiający jak i wykonawcy winni wdrażać takie mechanizmy proceduralne i rozwiązania prawne, aby zamawiając sprzęt byli w stanie kontrolować komponenty. Zwłaszcza budując środowiska infrastruktury krytycznej należy wprowadzać do postępowań o udzielenie zamówienia mechanizmy preferujące sprawdzonych wykonawców, których rozwiązania są transparentne (służyć temu ma rozwijający się proces certyfikacji Common Criteria). Jest to jedno z najtrudniejszych wyzwań stojących przed zamawiającymi i wykonawcami. W skali światowej obserwuje się konsolidację technologiczną w potężnych gospodarczo i infrastrukturalnie przedsiębiorstwach, od których bardzo prosto użytkownicy w tym instytucje potrafią się uzależniać. Ich skala działania i możliwości ekonomiczne pozwalają na stawianie skutecznego oporu przed udostępnianiem swoich rozwiązań technologicznych do oceny.

**Uzależnienie od komponentów tego samego dostawcy**

**Opis.** Zamawiający i wykonawcy kreując systemy IT/OT, np. budując sieci telekomunikacyjne mogą poprzez swoją politykę zakupową i dotychczasowe praktyki doprowadzić do sytuacji, w której dostawcą urządzeń lub istotnych ich komponentów zostanie jeden podmiot. Tego typu uzależnienie będzie generowało wiele ryzyk dla zapewnienia ciągłości i bezpieczeństwa łańcucha dostaw. W sytuacji zagrożenia geopolitycznego typu: wojna, nałożenie sankcji, działania regulacyjne wpływające na dostawy, ale także katastrofa naturalna może dojść do zmaterializowania się szeregu różnych zagrożeń, które

[19] POLITICO, *Huawei's solar tech sparks fears of Europe's next dependency crisis*, [online:] https://www.politico.eu/article/europe-solar-industry-having-huawei-moment/ [dostęp: 12.11.2025].

[20] Sarah McFarlane, „Rogue communication devices found in Chinese solar power inverters", Reuters, 14 maja 2025, [online:] https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/ [dostęp: 12.11.2025].

negatywnie wpłyną na możliwość odtworzenia elementów uszkodzonych lub ulegających naturalnemu zużyciu, rozbudowę infrastruktury.
**Skutek:** Może dojść do przerwania łańcucha dostaw, wycieku danych i kradzieży własności intelektualnej, opóźnień w produkcji, problemów ze skutecznym świadczeniem usług, ale również do zagrożenia geopolitycznego, jeżeli komponenty będę elementami składowymi infrastruktury krytycznej. Przerwa w świadczeniu usług wyłącznego dostawcy, może wpływać na świadczenie usług publicznych przez uzależnionego od nich zamawiającego, natomiast w przypadku wykonawców może podważyć zaufanie do jakości świadczeń.

### 1.2.4. Obszar monitorowania wykonawców i podwykonawców, gdzie może występować

**Brak kontroli nad bezpieczeństwem u dostawców, partnerów, producentów oprogramowania**
**Opis**. Według Raportu Global Cybersecurity Outlook 2025 brak nadzoru nad poziomem dojrzałości bezpieczeństwa u dostawców stanowi poważny problem dla wielu organizacji. Zwiększenie przejrzystości w ocenie jak wyglądają zależności od podmiotów trzecich jest priorytetem dla poprawy łańcucha dostaw[21]. Zadanie to wydaje się jednak nie lada wyzwaniem, gdyż egzekwowanie standardów bezpieczeństwa od dostawców zewnętrznych nie jest łatwe. W przypadku zamówień publicznych zamawiający wchodząc w relację biznesową z dostawcą praktycznie może mieć jeszcze wgląd w najbliższych podwykonawców, jednak skomplikowanie współczesnych łańcuchów dostaw, czyni głębszy wgląd w stopień cyberodporności podwykonawców trzeciego lub czwartego poziomu niemal fikcyjnym. Zapobiegać temu zagrożeniu ma certyfikacja i ujednolicanie zasad zarządzania ryzykiem w oparciu o standardy (standaryzacja opisana została w rozdziale 4 i 5). Zamawiający czy też wykonawcy nie mają pełnej kontroli nad polityką bezpieczeństwa kontrahentów (podmiotów trzecich). Brak wiedzy czy i jak chronione są dane lub systemy po stronie dostawcy, może prowadzić do wyboru wykonawcy, u którego występują luki w zabezpieczeniach prowadzące do wycieku danych lub wrogiego przejęcia systemów. Dlatego też przed uczestnikami postępowania o udzielenie zamówienia publicznego związanego z wykorzystaniem technologii IT/OT stoi istotne i trudne zadanie polegające na wyborze partnerów biznesowych, u

[21] WEF, *Global Cybersecurity Outlook 2025*, 2025, s. 6.

których stosuje się odpowiedzialne podejście do cyberbezpieczeństwa. Niezbędne staje się uzupełnienie dotychczasowych wymagań stosowanych przez zamawiających wobec wykonawców jak i podwykonawców właśnie w obszarze ochrony łańcucha dostaw zarówno na etapie wyboru najkorzystniejszej oferty jak również na etapie realizacji kontraktu. Takie podejście wiąże się z uwzględnianiem w warunkach udziału w postępowaniu, w opisie przedmiotu zamówienia, a także w treści umowy odpowiednich wymogów oraz zobowiązań względem wykonawców czy podwykonawców, które pozwolą zamawiającemu wybrać podmiot realnie i konsekwentnie dbający o swoje bezpieczeństwo.

**Niewystarczająca transparentność i monitorowanie**

**Opis**: Brak pełnej widoczności w działaniach i bezpieczeństwie w całym ekosystemie dostawców czy producentów utrudnia wykrycie zagrożeń i reagowanie na incydenty.

Ponadto organizacje stają się jak wynika z Raportu Global Cybersecurity Outlook 2025[22] coraz bardziej zależne od ograniczonej liczby kluczowych dostawców, którym udało się zdobyć pozycję liderów w swojej dziedzinie, a to oznacza, że każda luka w zabezpieczeniach wprowadzona przez tychże dostawców będzie miała nie tylko skutki domina w całej ich rozległej bazie klientów, ale także spowoduje efekt domina w ekosystemie łańcucha dostaw.

**Zagrożenie**: Dostawcy stają się systemowymi punktami awarii, zwłaszcza gdy pozostawione przez nich luki bądź błędy ludzkie (o czym poniżej) mogą spowodować efekt domina, który rozlewa się po całym łańcuchu dostaw. Opóźnione wykrycie ataku może prowadzić do dużych strat finansowych, wizerunkowych, utraty danych wrażliwych, wycieku danych osobowych.

**Przykład**: Błąd popełniony przez firmę CrowdStrike - podwykonawcę firmy Microsoft spowodował, że wadliwa aktualizacja oprogramowania doprowadziła do masowej awarii systemów informatycznych w najróżniejszych instytucjach na całym świecie.

**Zagrożenia ze strony personelu wykonawcy**

**Opis**: Pracownicy wykonawcy lub podwykonawcy mogą nieświadomie lub celowo naruszyć zasady bezpieczeństwa.

[22] WEF, *Global Cybersecurity Outlook 2025*, (on line) udostępnione 12.11.2025, s. 6.

**Zagrożenie**: Nieprzeszkoleni i nieświadomi jak powinna wyglądać służbowa cyberhigiena pracownicy wykonawcy/ podwykonawcy mogą dokonywać ryzykownych działań takich jak przesyłanie danych przez niezabezpieczone kanały, korzystanie z nieautoryzowanych nośników USB, wchodzenie w linki spreparowane w celu dokonania ataku typu phishing. Zdarzają się przypadki zatrudniania się hakerów u dostawców lub wytwórców oprogramowania w celu penetracji systemów i instalowania złośliwego kodu.

**Brak zgodności z normami i regulacjami**

**Opis**: Nawet jeżeli Zamawiający będzie restrykcyjnie przestrzegał wszystkich przepisów prawa i znanych wytycznych w obszarze cyberbezpieczeństwa może paść ofiarą ataku, gdyż to wykonawca lub jego podwykonawca może nie przestrzegać wymaganych norm bezpieczeństwa (np. ISO 27001, NIS2, RODO), co naraża zamawiającego lub wykonawcę na sankcje prawne i szkody wizerunkowe.

**Zagrożenia**: Organizacja może być współodpowiedzialna za naruszenia, a także za powstałe w wyniku zmaterializowania się ryzyka szkody w majątku zaatakowanego podmiotu.

**Zbyt pochopne zaufanie w bezpieczeństwo certyfikowanych partnerów i automatycznych procesów**

**Opis**: Żadna instytucja nie powinna polegać bezrefleksyjnie na posiadanych certyfikatach (np. ISO/IEC 27001) zarówno u siebie jak i u dostawcy (partnera/klienta/kontrahenta/wykonawcy), gdyż nie istnieje certyfikat, który gwarantuje pełne bezpieczeństwo. Zawsze należy stosować zasadę ograniczonego zaufania i stosować także własne mechanizmy weryfikacji dostosowane do nabywanych dóbr oraz podmiotów, z którymi się wchodzi w relacje biznesowe. Podobne ostrożnościowe podejście powinno znaleźć zastosowanie także wobec certyfikowanych produktów zwłaszcza oprogramowania. Nawet po certyfikacji oprogramowania pochodzącego z państwa trzeciego przez właściwą krajową jednostkę przy najbliższej aktualizacji może okazać się, że znajduje się w nim nowy kod, który wprowadzają np. Backdoor'y (oprogramowanie umożliwiające podmiotom trzecim penetrację systemów).

**Zagrożenia:** Dobrze widać opisywane powyżej nadmierne zaufanie w sytuacji wykorzystywania zewnętrznych usług chmurowych lub zewnętrznej pomocy technicznej. Renomowani dostawcy takich usług dysponują często silniejszymi i lepiej zorganizowanymi zabezpieczeniami niż byłby sobie w stanie zorganizować zamawiający bądź wykonawca, jednakże korzystanie z takich usług wiąże się z ograniczoną kontrolą nad przekazywanymi danymi czy konfiguracją. W takich przypadkach atak na takiego dostawcę to poważne ryzyko wstrzymania działalności podmiotów korzystających z jego usług.

**Przykład:** Amerykańska międzynarodowa firma Clorox wydała ponad 500 milionów dolarów na modernizację systemów informatycznych. Znalazła się nawet na liście najbezpieczniejszych cyfrowo firm magazynu Forbes w 2023 r. Mimo to padła ofiarą cyberincydentu, który skutkował wstrzymaniem działalności firmy, z poważnymi skutkami dla łańcuch dostaw i jej działalności biznesowej. Pracownicy firmy Cognizant, świadczący pomoc techniczną Clorox sami podali cyberprzestępcom hasła bez wcześniejszej weryfikacji rozmówców. W trakcie rozmów pracownicy pomocy technicznej przekazywali podszywającym się pod pracowników Clorox'a oszustom hasła i resetowali uwierzytelnianie wieloskładnikowe (MFA), bez sprawdzania tożsamości dzwoniących. Clorox pozwał Cognizant o odszkodowanie w wysokości 380 milionów dolarów.[23]

## 2. Regulacje prawne w Polsce i UE dotyczące cyberbezpieczeństwa

### 2.1. NIS2

#### 2.1.1. Identyfikacja aktu

| | |
|---|---|
| **Pełna nazwa** | Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. „w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148" (tzw. „dyrektywa NIS 2"). Tekst opublikowano w Dz.U. L 333 dnia 27.12.2022. (https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng) |

[23] Dorota Kwaśniewska, „Zhakowani mimo wydania 500 mln na IT. Clorox pozywa Cognizant", CyberDefence24, 24.07.2025, [online:] https://cyberdefence24.pl/cyberbezpieczenstwo/zhakowani-mimo-wydania-500-mln-na-it-clorox-pozywa-cognizant [dostęp: 12.11.2025].

| | |
|---|---|
| **Rodzaj aktu** | • Przyjęta: 14 grudnia 2022 r.; opublikowana: 27 grudnia 2022 r. (Dz.U. L 333).<br>• Akty wykonawcze (m.in. doprecyzowanie środków zarządzania ryzykiem i kryteriów „poważnego incydentu" dla wybranych usług cyfrowych) zostały przyjęte rozporządzeniem wykonawczym Komisji (UE) 2024/2690 z 17.10.2024 r., opublikowanym 18.10.2024 r. (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R2690) |
| **Status / terminy** | • NIS 2 obejmuje podmioty w sektorach wskazanych w załącznikach I i II (podmioty „kluczowe" i „ważne"), przy czym dodatkowe progi/warunki obejmują m.in. dostawców publicznych sieci i usług łączności elektronicznej, dostawców usług zaufania, rejestry TLD oraz dostawców DNS; objęcie może też wynikać ze znaczenia usługi na poziomie krajowym lub transgranicznego ryzyka systemowego.<br>• W obszarze usług cyfrowych szczególną wagę (również na potrzeby aktów wykonawczych) mają: dostawcy usług DNS, rejestry TLD, usługi chmurowe, ośrodki przetwarzania danych, sieci dostarczania treści (CDN), dostawcy usług zarządzanych (MSP) i usług bezpieczeństwa zarządzanego (MSSP), internetowe platformy handlowe, wyszukiwarki internetowe, platformy usług sieci społecznościowych oraz dostawcy usług zaufania.<br>• Dyrektywa rozróżnia kategorie podmiotów (kluczowe/ważne) i przewiduje zróżnicowany nadzór i egzekwowanie. |
| **Właściwe organy** | • Państwa członkowskie wyznaczają właściwe organy, pojedynczy punkt kontaktowy oraz CSIRT, które współpracują między sobą oraz z innymi organami (m.in. ochrony danych, regulacyjnymi łączności, właściwymi na gruncie dyrektywy o odporności podmiotów krytycznych).<br>• Na poziomie UE funkcjonują Grupa Współpracy oraz sieć CSIRT (z udziałem ENISA i Komisji - odpowiednio wsparcie/sekretariat i obserwator), zapewniające wymianę informacji i koordynację. |

### 2.1.2. Cel i zakres przedmiotowy

NIS2 ma na celu ograniczenie fragmentacji wymogów cyberbezpieczeństwa w Unii Europejskiej oraz podniesienie wspólnego poziomu odporności przez ustanowienie minimalnych wymogów, skoordynowanych mechanizmów współpracy i skuteczniejszych środków nadzoru oraz egzekwowania[24]. W tym zamyśle uchylono dyrektywę NIS1 i zastąpiono ją NIS2[25], jednocześnie aktualizując wykaz sektorów i rodzajów działalności objętych obowiązkami, aby odzwierciedlić postępującą cyfryzację i transgraniczne współzależności usług[26]. Zakres dyrektywy opiera się w pierwszej kolejności na kryterium wielkości: co do zasady dyrektywa obejmuje podmioty kwalifikujące się co najmniej jako przedsiębiorstwa średnie (lub większe) prowadzące działalność w sektorach i usługach wskazanych w jej załącznikach; przewidziano przy tym możliwość objęcia niektórych małych podmiotów ze względu na ich szczególną rolę dla społeczeństwa, gospodarki bądź określonych sektorów[27]. Zróżnicowano dwie kategorie adresatów (podmioty kluczowe i podmioty ważne) przy wspólnym trzonie obowiązków, lecz odmiennym modelu nadzoru (bardziej proaktywnym wobec podmiotów kluczowych)[28].

W porównaniu z NIS1 zakres został znacząco poszerzony, co szczególnie istotne z perspektywy zamówień publicznych, o infrastrukturę cyfrową i wybrane usługi cyfrowe[29]. Obejmuje to w szczególności rejestry nazw domen najwyższego poziomu (TLD) i dostawców usług DNS, usługi chmurowe, ośrodki przetwarzania danych, sieci dostarczania treści (CDN), dostawców usług zarządzanych (MSP) i zarządzanych w zakresie bezpieczeństwa (MSSP), a także duże platformy internetowe, internetowe platformy handlowe, wyszukiwarki internetowe, platformy usług sieci społecznościowych, oraz dostawców usług zaufania i publiczne sieci/usługi łączności elektronicznej[30]. Ponadto do zakresu dyrektywy

[24] Zob. art. 1 Dyrektywy NIS2.

[25] Komisja Europejska, *Commission Staff Working Document. Impact Assessment Report. Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*, Brussels, 16.12.2020, SWD(2020) 345 final, PART 1/3, {COM(2020) 823 final} – {SEC(2020) 430 final} – {SWD(2020) 344 final}, s. 31; 87-91, [online:] https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union [dostęp: 10.11.2025].

[26] Ibid. s. 86-87.

[27] Zob. motyw 7 NIS2 oraz art. 2 ust. 1 NIS2.

[28] Zob. art. 3 NIS2; Komisja Europejska, *Commission Staff Working Document. Impact Assessment Report*, SWD(2020) 345 final, PART 1/3, s. 57, 57-59.

[29] Komisja Europejska, *Commission Staff Working Document. Impact Assessment Report*, SWD(2020) 345 final, PART 1/3, s. 57-59.

[30] Ibid.

wchodzą podmioty administracji publicznej (z wyłączeniami wskazanymi niżej), co ma bezpośrednie znaczenie dla sposobu organizacji zamówień publicznych i ich bezpieczeństwa[31].

Jednocześnie NIS2 przewiduje wyłączenia. Poza zakresem pozostają podmioty, których działalność dotyczy głównie bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa (w tym zapobiegania, wykrywania i ścigania przestępstw); wyłączenie nie obejmuje jednak podmiotów administracji, których działalność jedynie w niewielkim stopniu wiąże się z tymi obszarami[32]. Dyrektywa nie ma zastosowania do misji dyplomatycznych i konsularnych państw członkowskich w państwach trzecich[33]. Państwa członkowskie mogą ponadto zwolnić określone podmioty realizujące działania w ww. obszarach z niektórych obowiązków NIS2 w odniesieniu do tych działań. Poza tym usługi zaufania wykorzystywane wyłącznie w zamkniętych systemach wynikających z prawa krajowego lub porozumień danej grupy uczestników nie podlegają dyrektywie.

Relacja NIS2 do prawa sektorowego UE została rozstrzygnięta w sposób zapewniający spójność: jeżeli akt sektorowy nakłada na dany typ podmiotów wymogi zarządzania ryzykiem i zgłaszania incydentów co najmniej równoważne co do skutku obowiązkom z NIS2, stosuje się przepisy sektorowe (wraz z właściwym reżimem nadzoru i egzekwowania), a NIS2 znajduje zastosowanie w obszarach nieobjętych danym aktem[34].

Na poziomie wykonawczym kluczowe znaczenie ma rozporządzenie wykonawcze Komisji (UE) 2024/2690, które doprecyzowuje techniczno-metodyczne wymagania środków z art. 21 ust. 2 NIS2 oraz określa przesłanki uznania incydentu za „poważny" w odniesieniu do wybranych usług cyfrowych (DNS, rejestry TLD, chmura, ośrodki przetwarzania danych, CDN, MSP, MSSP, internetowe platformy handlowe, wyszukiwarki, platformy sieci społecznościowych oraz usługi zaufania)[35]. Z perspektywy zamówień publicznych

[31] Ibid. str. 48.

[32] Zob. motyw 8 NIS2.

[33] Ibid.

[34] Zob. motywy 22, 24-27 NIS2; art. 4; jako przykład motywy: 15-20 DORA oraz art. 19 ust. 1 *in fine* DORA.

[35] Komisja Europejska, Rozporządzenie wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny..., C/2024/7151, Dz.U.

akty te wyznaczają jednoznaczny punkt odniesienia dla kształtowania wymagań wobec wykonawców i ich podwykonawców oraz dla weryfikacji spełnienia tych wymagań na etapie oceny ofert i w trakcie realizacji umów.

### 2.1.3. Obowiązki podmiotów kluczowych i ważnych

**Zarządzanie ryzykiem (trzon wymagań NIS2)[36]**

- Podmiot powinien stosować systemowe podejście „all-hazards", obejmujące identyfikację ryzyka wystąpienia incydentów, zapobieganie, wykrywanie, reagowanie, odtwarzanie oraz łagodzenie skutków, z uwzględnieniem bezpieczeństwa fizycznego i środowiskowego systemów i danych oraz czynnika ludzkiego.
- Podmiot powinien wdrożyć środki, o których mowa w art. 21 dyrektywy NIS2, w szczególności: polityki analizy ryzyka i bezpieczeństwa informacji; organizację obsługi incydentów; rozwiązania zapewniające ciągłość działania i zarządzanie kryzysowe (w tym kopie zapasowe i odtwarzanie); mechanizmy bezpieczeństwa łańcucha dostaw; zasady bezpiecznego nabywania, rozwoju i utrzymania systemów (w tym zarządzania podatnościami); okresową ocenę skuteczności środków (testy i audyty); działania w obszarze cyberhigieny i szkolenia; odpowiednie mechanizmy kryptograficzne; kontrolę dostępu i bezpieczeństwo zasobów ludzkich; uwierzytelnianie wieloskładnikowe (MFA) oraz bezpieczną komunikację.
- Podmiot powinien dobrać środki w sposób proporcjonalny do poziomu narażenia na ryzyko, zgodny z aktualnym stanem wiedzy, z uwzględnieniem właściwych standardów europejskich i międzynarodowych oraz racjonalnych kosztów wdrożenia.
- Podmiot powinien stosować te środki niezależnie od modelu świadczenia usług, obejmując nimi zarówno systemy własne, jak i systemy utrzymywane przez dostawców zewnętrznych (w tym MSP/MSSP).

**Wymogi łańcucha dostaw[37]**

---

L, 2024/2690, 18.10.2024, [online:] ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj; CELEX: 32024R2690, dostęp: 10.11.2025.

[36] ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, *NIS2 Technical Implementation Guidance*, Luxembourg: Publications Office of the European Union, czerwiec 2025, wersja 1.0, ISBN 978-92-9204-704-7, DOI: 10.2824/2702548, s. 21–30, [online:] https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance [dostęp: 10.11.2025].

[37] ENISA, *NIS2 Technical Implementation Guidance*, 2025, s. 66-73.

- Podmiot powinien systematycznie oceniać i adresować ryzyko związane z dostawcami, obejmując ocenę ogólnej jakości i odporności produktów oraz usług, a także praktyk bezpieczeństwa dostawców (w tym bezpieczeństwa procesu wytwórczego i rozwoju), oraz włączać środki C-SCRM do postanowień umownych z bezpośrednimi dostawcami i usługodawcami.
- Podmiot powinien dochować szczególnej staranności przy wyborze dostawców usług zarządzanych (MSP/MSSP), z uwagi na ścisłą integrację operacyjną i wynikające z niej podwyższone ryzyko.
- Podmiot powinien uwzględniać czynniki pozatechniczne i zależności systemowe w ocenie łańcuchów dostaw, w tym wpływ państw trzecich, ryzyko występowania backdoorów, pojedyncze punkty awarii (single point of failure), blokady technologiczne oraz zależności od konkretnego dostawcy.
- Podmiot powinien brać pod uwagę wyniki skoordynowanych, wspólnotowych ocen ryzyka krytycznych łańcuchów dostaw w Unii Europejskiej, na wzór „toolboxu 5G", wraz z identyfikowanymi środkami zaradczymi i najlepszymi praktykami.

**Operacje i ciągłość działania[38]**

- Podmiot powinien utrzymywać ciągłość działania i gotowość poprzez wykonywanie kopii zapasowych, testowane procedury odtwarzania po awarii, aktualne plany zarządzania kryzysowego oraz regularne ćwiczenia. Powinien także stosować dobre praktyki cyberhigieny, w szczególności segmentację sieci, zarządzanie tożsamością i dostępem oraz działania podnoszące świadomość użytkowników.
- Podmiot powinien stosować nowoczesne mechanizmy kryptograficzne właściwie dobrane do poziomu ryzyka oraz zapewniać bezpieczną łączność. W sektorze łączności publicznej podmiot powinien promować szyfrowanie typu end-to-end oraz mechanizmy kontroli dostępu i zarządzania danymi.

**Ujawnianie i zarządzanie podatnościami[39]**

- Podmiot powinien stosować dojrzałe procesy zarządzania podatnościami, obejmujące przyjmowanie zgłoszeń od osób trzecich, diagnozowanie i usuwanie podatności oraz promowanie skoordynowanego ujawniania podatności. Jako dobre praktyki warto odwoływać się do norm ISO/IEC 30111 oraz ISO/IEC 29147.

[38] Ibid., s. 51-56.

[39] Ibid., s. 103.

- Podmiot powinien współpracować z wyznaczonym CSIRT pełniącym funkcję koordynatora, który działa jako zaufany pośrednik, identyfikuje podmioty dotknięte podatnością, wspiera zgłaszających, uzgadnia harmonogram publikacji oraz prowadzi wielostronne procesy skoordynowanego ujawniania.
- Podmiot powinien rozważyć dobrowolną rejestrację publicznie znanych podatności w europejskiej bazie ENISA, korzystając z procedury publikacji zapewniającej czas na wdrożenie środków łagodzących, z uwzględnieniem współpracy z rejestrami CVE.

**Raportowanie incydentów i współpraca**[40]

Podmiot kluczowy lub ważny powinien aktywnie korzystać ze wsparcia wyznaczonego CSIRT oraz współpracować z właściwym organem i pojedynczym punktem kontaktowym ustanowionymi przez państwo członkowskie na podstawie NIS2. W przypadku poważnego incydentu zgłasza go bez zbędnej zwłoki, przekazując wczesne ostrzeżenie w ciągu 24 godzin, następnie w ciągu 72 godzin bardziej szczegółowe zgłoszenie, a potem sprawozdania okresowe i sprawozdanie końcowe najpóźniej miesiąc po zgłoszeniu lub zakończeniu obsługi incydentu.
CSIRT lub właściwy organ udziela podmiotowi szybkiej informacji zwrotnej i, na jego wniosek, wytycznych oraz wsparcia technicznego, w miarę możliwości w ciągu 24 godzin od otrzymania wczesnego ostrzeżenia. NIS2 przewiduje także współpracę transgraniczną: w razie poważnych incydentów o skutkach międzysektorowych lub dotyczących kilku państw członkowskich właściwe organy i pojedyncze punkty kontaktowe wymieniają informacje między sobą i z ENISA, z poszanowaniem poufności danych i interesów handlowych podmiotu. Jeżeli ma to zastosowanie, podmiot informuje odbiorców swoich usług o poważnych cyberzagrożeniach i środkach zaradczych, a także o poważnych incydentach wpływających na świadczenie usług.

**Governance, nadzór i zgodność**[41]

- Podmiot powinien budować kulturę zarządzania ryzykiem, w której odpowiedzialność za bezpieczeństwo jest jasno przypisana, a decyzje opierają się na systematycznej ocenie ryzyka i wdrażaniu adekwatnych środków.
- Podmiot powinien uwzględniać, że choć trzon obowiązków jest wspólny dla podmiotów kluczowych i ważnych, model nadzoru i egzekwowania różni się intensywnością na niekorzyść podmiotów kluczowych.

[40] Ibid., s. 32-35.
[41] ENISA, *NIS2 Technical Implementation Guidance*, 2025, s. 122-127.

- Podmiot powinien stosować właściwe normy europejskie i międzynarodowe oraz, w razie potrzeby, korzystać z dostępnych programów certyfikacji. W braku odpowiednich programów unijnych powinien rozważyć wymaganie certyfikowanych produktów, usług lub procesów ICT.
- Podmiot powinien identyfikować relacje między NIS2 a aktami sektorowymi i stosować zasadę lex specialis w sytuacjach, gdy wymogi sektorowe są co najmniej równoważne co do skutku, przy czym NIS2 ma zastosowanie do podmiotów pozostających poza zakresem regulacji sektorowych.

**Dodatkowe elementy operacyjne**

- Podmiot powinien rozwijać cyberhigienę i kompetencje personelu, w szczególności stosować zasady zero trust, utrzymywać aktualizacje i właściwą konfigurację, prowadzić segmentację oraz budować świadomość zagrożeń phishingowych i inżynierii społecznej.
- Podmiot powinien współpracować w ramach inicjatyw publiczno-prywatnych oraz korzystać z krajowych punktów kontaktowych i usług wsparcia dla MŚP, zwłaszcza w obszarze ryzyk w łańcuchu dostaw.

**Uwagi dla zamówień publicznych**

*Powyższe obowiązki przekładają się na konieczność precyzyjnego adresowania wymagań bezpieczeństwa w relacjach z dostawcami (umowne odzwierciedlenie środków z art. 21, due diligence MSP/MSSP, mechanizmy raportowania i współpracy z CSIRT) oraz na ciągły nadzór nad spełnianiem tych wymogów w trakcie realizacji zamówienia (audytowalność, testy, przeglądy ryzyka i łańcucha dostaw).*

### 2.1.4. Wymogi dotyczące łańcucha dostaw

NIS2 (art. 21 ust. 2 lit. d) – doprecyzowana rozporządzeniem wykonawczym 2024/2690 – wymaga, aby podmiot ustanowił, wdrożył i stosował politykę bezpieczeństwa łańcucha dostaw wobec swoich bezpośrednich dostawców i usługodawców, z określeniem własnej roli w łańcuchu i celem ograniczenia zidentyfikowanego ryzyka dla sieci i systemów informatycznych[42]. Polityka musi zawierać kryteria wyboru i zawierania umów obejmujące m.in.:

- praktyki cyberbezpieczeństwa u dostawców (w tym procedury bezpiecznego opracowywania),

[42] ENISA, *NIS2 Technical Implementation Guidance*, 2025, s. 66-73; Komisja Europejska, Rozporządzenie wykonawcze (UE) 2024/2690, C/2024/7151, Dz.U. L, 18.10.2024, Załącznik pkt. 5.

- zdolność spełnienia specyfikacji bezpieczeństwa zamawiającego,
- jakość i odporność produktów/usług ICT (wraz z wbudowanymi środkami zarządzania ryzykiem),
- możliwość dywersyfikacji źródeł dostaw i ograniczenia uzależnienia od jednego dostawcy

Przy ustanawianiu polityki należy – gdy to konieczne– uwzględniać wyniki skoordynowanych ocen ryzyka na poziomie UE dla krytycznych łańcuchów dostaw (art. 22 NIS2).

### 2.1.5. Obowiązkowe elementy umów z dostawcami/usługodawcami.

Na podstawie polityki i własnej oceny ryzyka umowy powinny określać (także poprzez SLA), w szczególności[43]:

- wymogi cyberbezpieczeństwa (w tym wymogi przy nabywaniu usług/produktów ICT);
- wymogi dot. świadomości, umiejętności i szkoleń oraz – gdy właściwe – certyfikatów personelu;
- sprawdzanie przeszłości pracowników dostawcy/usługodawcy (tam, gdzie uzasadnione);
- obowiązek niezwłocznego zgłaszania incydentów zagrażających sieciom i systemom zamawiającego;
- prawo do audytu lub do otrzymywania sprawozdań z audytu;
- postępowanie z podatnościami dotyczącymi usług/produktów świadczonych zamawiającemu;
- zasady podwykonawstwa (w tym przeniesienie wymogów bezpieczeństwa na podwykonawców);
- obowiązki przy rozwiązaniu umowy (wyszukiwanie i przekazanie informacji powstałych w toku świadczenia).

Wskazane elementy są częściowo wyliczone w załączniku do rozporządzenia 2024/2690.

### 2.1.6. Włączenie do procedur zakupowych i nadzoru.

Podmiot powinien stosować niniejsze wymagania w procesie wyboru nowych dostawców, w tym w procedurach udzielania zamówień[44]. Powinien także objąć je

[43] Komisja Europejska, Rozporządzenie wykonawcze (UE) 2024/2690, C/2024/7151, Dz.U. L, 18.10.2024, Załącznik pkt. 6.

[44] ENISA, *NIS2 Technical Implementation Guidance*, 2025, s. 76-79

stałym monitorowaniem oraz okresowymi przeglądami praktyk bezpieczeństwa dostawców[45]. Działania korygujące powinien podejmować w zaplanowanych odstępach oraz każdorazowo po poważnych incydentach lub istotnych zmianach profilu ryzyka.

Podmiot powinien prowadzić i aktualizować rejestr swoich bezpośrednich dostawców i usługodawców, obejmujący co najmniej dane kontaktowe oraz wykaz dostarczanych produktów i usług ICT, a także procesów ICT[46]. W procesach nabywania produktów i usług ICT podmiot powinien wdrożyć zarządzanie ryzykiem „od zakupu do wycofania" dla komponentów krytycznych, obejmujące w szczególności:

- określenie wymagań bezpieczeństwa na etapie postępowania,
- wymagania dotyczące aktualizacji zabezpieczeń w całym cyklu życia albo wymiany komponentu po zakończeniu wsparcia producenta,
- pozyskanie informacji o elementach sprzętu i oprogramowania oraz o wdrożonych funkcjach bezpieczeństwa i wymaganej konfiguracji,
- zdefiniowanie metod walidacji zgodności wraz z dokumentowaniem wyników.

**Elementy należytej staranności i ciągłego nadzoru (wybrane przykłady)**

- Podmiot powinien zapewnić szkolenia z zakresu podstawowych praktyk bezpieczeństwa oraz jasne przypisanie ról i odpowiedzialności po stronie własnych pracowników i, w razie potrzeby, bezpośrednich dostawców[47]. Przypisania te powinien okresowo przeglądać.

- Podmiot powinien zagwarantować prawo do audytu oraz do pozyskiwania raportów od dostawców, a także testować plany ciągłości działania i zarządzania kryzysowego[48]. Powinien wykorzystywać informacje o podatnościach i zagrożeniach przekazywane przez CSIRT oraz właściwe organy.

- Podmiot powinien prowadzić ciągłe zarządzanie podatnościami[49], w tym monitorować komunikaty CSIRT oraz informacje przekazywane przez

[45] Ibid.
[46] Ibid, s. 73-74.
[47] Motyw 50 NIS2, zob. również ENISA, *NIS2 Technical Implementation Guidance*, 2025, s. 111.
[48] Komisja Europejska, Rozporządzenie wykonawcze (UE) 2024/2690, C/2024/7151, Dz.U. L, 18.10.2024, Załącznik pkt. 5.1.4.
[49] ENISA, *NIS2 Technical Implementation Guidance*, 2025, s. 27, 30.

dostawców i usługodawców, oceniać narażenie na ryzyko i podejmować adekwatne środki zaradcze.

**Uwagi interpretacyjne dla zamówień publicznych.**

- Powyższe obowiązki wynikają z terminologii unijnych regulacji z zakresu cyberbezpieczeństwa (dostawcy, usługodawcy, produkty/usługi ICT, umowy/SLA, podwykonawstwo) i powinny być odzwierciedlone w opisie przedmiotu zamówienia, warunkach umowy oraz monitoringu realizacji.
- W przypadku zakupów usług należących do katalogu 2024/2690 (np. chmura, MSP/MSSP) specyficzne wymogi techniczno-metodyczne i progi „poważnego incydentu" dostarczają jasnych punktów odniesienia dla oceny ofert i nadzoru kontraktowego.

*(NIS2 i Rozporządzenie 2024/2690 nie nakładają wprost obowiązku posiadania SBOM/VEX; mogą one jednak zostać uzgodnione umownie jako sposób dokumentowania wymogów dotyczących informacji o komponentach i podatnościach, w ramach sekcji o „nabywaniu usług/produktów ICT" oraz „postępowaniu z podatnościami".)*

### 2.1.7. Wpływ NIS2 na cykl zamówień publicznych (Pzp)

NIS2 wprowadza horyzontalne obowiązki w zakresie zarządzania ryzykiem i zgłaszania incydentów, a rozporządzenie wykonawcze Komisji (UE) 2024/2690 doprecyzowuje wymagania techniczne/metodyczne oraz – dla wybranych typów dostawców (m.in. chmura, centra danych, CDN, MSP/MSSP, duże platformy) – określa przypadki, gdy incydent należy uznać za „poważny". W konsekwencji dokumentacja postępowania[50] i umowy w sprawie zmówienia publicznego stają się jednym z podstawowych instrumentów wdrażania obowiązków NIS2 po stronie zamawiających i wykonawców.

#### 2.1.7.1. OPZ/SWZ (wymogi techniczne, funkcjonalne i bezpieczeństwa)

Przy formułowaniu wymagań należy powiązać katalog środków z art. 21 NIS2, obejmujący między innymi ciągłość działania i odtwarzanie, bezpieczeństwo łańcucha dostaw, bezpieczne nabywanie, rozwój i utrzymanie, zarządzanie podatnościami, testy i audyty, szkolenia, kryptografię oraz kontrolę dostępu, z ich

[50] Jako dokumentacja postępowania rozumiane są tutaj wszystkie dokumenty sporządzane w tym procesie, które mogą mieć wpływ na kształtowanie wymogów stron. Nie ogranicza się to zatem do pojęcia dokumentów zamówienia z art. 7 pkt 3 PZP.

konkretną specyfikacją wdrożeniową przewidzianą w rozporządzeniu 2024/2690. W praktyce OPZ/SWZ powinny co najmniej:

- precyzować wymagania bezpieczeństwa,
- obowiązek aktualizacji zabezpieczeń w całym cyklu życia oraz
- zakres informacji o komponentach sprzętowo-programowych, funkcjach i konfiguracji bezpieczeństwa,
- a także określać metody walidacji zgodności wraz z dokumentowaniem wyników; ustanawiać politykę obsługi incydentów, spójną z planem ciągłości i zarządzania kryzysowego, obejmującą detekcję, analizę, reagowanie, usuwanie skutków, dokumentowanie i raportowanie, z przewidzianymi testami i przeglądami;
- definiować zabezpieczenia sieci, w tym zapory, ograniczanie połączeń, VPN dla zdalnego dostępu oraz kontrolowane połączenia serwisowe, a także zasady kontroli nieuprawnionego oprogramowania z uwzględnieniem narzędzi EDR lub XDR adekwatnie do ryzyka.

Dopuszcza się żądanie produktów, usług lub procesów certyfikowanych w ramach programów certyfikacji przyjmowanych na podstawie rozporządzenia (UE) 2019/881.

#### 2.1.7.2. Warunki udziału (zdolności techniczne i zawodowe, normy, doświadczenie, kadry, procedury)

Warunki udziału obejmują w szczególności wymaganie posiadania wdrożonych procesów odpowiadających art. 21 NIS2, takich jak zarządzanie podatnościami, wykonywanie kopii zapasowych i odtwarzanie, kontrola dostępu, wraz z przedstawieniem dowodów w postaci polityk i procedur, wyników testów oraz raportów audytowych. Zgodnie z rozporządzeniem 2024/2690 umowy określają wymogi dotyczące świadomości, umiejętności oraz, jeśli jest to zasadne, certyfikatów personelu wykonawcy i podwykonawców.

**Kryteria oceny ofert mogą obejmować:**

- Punktacja za politykę bezpieczeństwa łańcucha dostaw, zdefiniowane kryteria doboru dostawców, mechanizmy dywersyfikacji i ograniczania zależności od jednego dostawcy (w uzasadnionych przypadkach).
- Rejestr bezpośrednich dostawców/usługodawców wraz z zakresem dostarczanych usług/produktów ICT oraz planem cyklicznych przeglądów i reagowania na zmiany ryzyka.

- Czas reakcji, parametry wykrywania i eskalacji incydentów, spójność z terminami raportowania NIS2 (wczesne ostrzeżenie 24 h, zgłoszenie 72 h, raport końcowy), gotowość do współpracy z CSIRT/właściwym organem.
- Metody i częstotliwość walidacji spełnienia wymagań (testy, audyty, przeglądy), sposób dokumentowania wyników i wniosków doskonalących.

#### 2.1.7.3. Klauzule umowne (SLA/OLA, audyty, prawo wglądu, incydenty, podwykonawcy, dane/transfery, exit, sankcje)

Rozporządzenie 2024/2690 wymienia elementy, które – stosownie do ryzyka – powinny znaleźć się w umowach z dostawcami/usługodawcami[51]; poniżej ich przełożenie na praktykę:

- Wymagania bezpieczeństwa (w tym dla produktów/usług nabywanych – zgodnie z pkt 6.1 załącznika), SLA na poziomie adekwatnym do krytyczności usługi.
- Kompetencje personelu: obowiązki dot. świadomości, umiejętności, szkoleń i – tam gdzie zasadne – certyfikatów personelu wykonawcy/podwykonawcy.
- Weryfikacja personelu krytycznego (background checks) w zakresach proporcjonalnych do ryzyka.
- Zgłaszanie incydentów bez zbędnej zwłoki przez wykonawcę do zamawiającego (także zdarzeń rodzących ryzyko dla systemów zamawiającego), wraz z mapowaniem na terminy NIS2 (24 h/72 h/raport końcowy), aby zamawiający mógł wypełnić własne obowiązki raportowe.
- Prawo audytu / prawo do otrzymywania sprawozdań z audytów, w tym audyty ukierunkowane na obszary wysokiego ryzyka; zastrzeżenie sankcji za niewspółpracowanie oraz mechanizmu działań naprawczych.
- Postępowanie z podatnościami (proces przyjmowania, klasyfikacji, remediacji oraz komunikacji – również dla podatności ujawnionych publicznie).
- Zarządzanie podwykonawstwem: warunki dopuszczalności, obowiązek przełożenia wymagań bezpieczeństwa na podwykonawców oraz informowania o zmianach w łańcuchu dostaw.

[51] Komisja Europejska, Rozporządzenie wykonawcze (UE) 2024/2690, C/2024/7151, Dz.U. L, 18.10.2024, Załącznik pkt. 6.

- Obowiązki na wyjściu z umowy („exit”): uporządkowane przekazanie informacji i artefaktów, wsparcie migracji/portowalności (minimalizacja ryzyka „lock-in”).
- Lokalizacja i transfer danych: uregulowanie przepływów transgranicznych i udziału dostawców z państw trzecich – w oparciu o ocenę ryzyka (w tym pozatechnicznych czynników ryzyka).
- Sankcje i środki zaradcze: kary umowne i prawo do żądania określonych działań naprawczych w razie stwierdzenia niezgodności z art. 21 lub naruszenia obowiązków zgłaszania incydentów z art. 23 (spójnie z reżimem nadzoru NIS2).

**Dlaczego to ważne?**

*Po pierwsze, część wykonawców i usług (szczególnie cyfrowych) jest objęta aktem 2024/2690, który szczegółowo określa zarówno środki z art. 21 NIS2, jak i progi „poważnych incydentów”. Przełożenie tych wymagań na OPZ/SWZ i umowy minimalizuje ryzyko niezgodności i ułatwia nadzór ex post. Po drugie, NIS2 pozwala – poprzez art. 24 – odwoływać się do europejskich programów certyfikacji cyberbezpieczeństwa, co może stanowić przejrzysty i weryfikowalny punkt odniesienia dla warunków udziału i dokumentów potwierdzających. Po trzecie, obowiązki terminowego raportowania wymagają zsynchronizowania procesów wykonawcy i zamawiającego już na etapie projektowania zamówienia i konstruowania komunikacji/SLA.*

#### 2.1.7.4. Dowody zgodności / walidacja

**Na wejściu (oferta / kwalifikacja wykonawcy)**

- Deklaracja i wykaz polityk/procedur pokrywających katalog środków z art. 21 NIS2 (m.in. obsługa incydentów, ciągłość działania/odtwarzanie, bezpieczeństwo łańcucha dostaw, bezpieczne nabywanie i utrzymanie, zarządzanie podatnościami, szkolenia, kontrola dostępu).
    - Można żądać zwięzłego mapowania istniejących procedur do punktów art. 21.
- Polityka bezpieczeństwa łańcucha dostaw (ustalona i wdrożona) wraz z kryteriami doboru dostawców/usługodawców (np. praktyki w zakresie cyberbezpieczeństwa, zdolność spełnienia specyfikacji, odporność produktów/usług, dywersyfikacja).

    - Jest to wprost wymagane w 2024/2690 dla podmiotów objętych tą regulacją.
- Rejestr bezpośrednich dostawców/usługodawców (kontakt + wykaz produktów/usług ICT przekazywanych zamawiającemu).
    - Jest to wprost wymagane w 2024/2690 dla podmiotów objętych tą regulacją.
- Informacje o komponentach sprzętowo-programowych oraz funkcjach i konfiguracji bezpieczeństwa nabywanych rozwiązań (można opisać w formie listy komponentów – praktycznie często SBOM – oraz wymogów konfiguracyjnych); plus metody walidacji zgodności z wymaganiami bezpieczeństwa i dokumentacja wyników walidacji.
    - Jest to wprost wymagane w 2024/2690 dla podmiotów objętych tą regulacją.
- Dowody certyfikacyjne lub równoważne: jeżeli istnieje adekwatny europejski program certyfikacji cyberbezpieczeństwa (na mocy rozporządzenia 2019/881), można żądać produktów/usług/procesów certyfikowanych albo dopuścić równoważność; Rozporządzenie 2024/2690 zaleca wprost odniesienie do programów UE i „zasadniczych wymogów" horyzontalnego rozporządzenia o produktach z elementami cyfrowymi.

**W realizacji (po podpisaniu umowy)**

- Raporty z walidacji spełnienia wymogów bezpieczeństwa (metody i wyniki – zgodnie z pkt 6.1.2 lit. f 2024/2690) oraz raporty z testów/ćwiczeń używanych do oceny skuteczności środków (w tym testów bezpieczeństwa).
    - Jest to wprost wymagane w 2024/2690 dla podmiotów objętych tą regulacją.
- Sprawozdania z incydentów i zdarzeń oraz notyfikacje „bez zbędnej zwłoki" w rytmie NIS2 (wczesne ostrzeżenie ≤ 24 h; zgłoszenie ≤ 72 h; raport końcowy ≤ 1 miesiąc) – tak, by zamawiający mógł wypełnić własne obowiązki.
- Potwierdzenia postępowania z podatnościami (przyjmowanie, klasyfikacja, remediacja, komunikacja), w tym względem podatności publicznie ujawnionych – jako wymagany element kontraktu.
- Aktualizacje polityki obsługi incydentów i przeglądy po-incydentowe.
    - Jest to wprost wymagane w 2024/2690 dla podmiotów objętych tą regulacją.

**Okresowo (zgodnie z umową i ryzykiem)**

- Niezależne przeglądy (ang. independent reviews) polityk i środków – w zaplanowanych odstępach i po poważnych incydentach/istotnych zmianach.
- Przeglądy polityki łańcucha dostaw oraz monitorowanie SLA i incydentów u dostawców wraz z aktualizacją rejestru dostawców.
- Dowody zgodności z normami/wytycznymi – gdy brak adekwatnego programu certyfikacji UE, NIS2 przewiduje promowanie norm europejskich/międzynarodowych (np. ISO/IEC 27000-series).

#### 2.1.7.5. Rola i obowiązki po stronie zamawiającego

Po stronie zamawiającego leży zapewnienie ładu organizacyjnego w obszarze bezpieczeństwa, co obejmuje zatwierdzanie przez organ zarządzający środków zarządzania ryzykiem, nadzór nad ich wdrożeniem oraz regularne szkolenia kierownictwa, zgodnie z odpowiedzialnością wynikającą z art. 20 NIS2. Polityka bezpieczeństwa łańcucha dostaw musi być odzwierciedlona w procedurach udzielania zamówień, w szczególności w kryteriach wyboru oraz warunkach umów; rozporządzenie 2024/2690 wprost nakazuje uwzględniać te elementy w ramach procedury udzielania zamówień. Zamawiający prowadzi i aktualizuje rejestr bezpośrednich dostawców i usługodawców, obejmujący dane kontaktowe oraz wykaz produktów i usług ICT, a rejestr ten powinien być spójny z ewidencją umów. Utrzymywana jest metodyka oceny ryzyka z określonymi kryteriami i poziomem tolerancji oraz z przypisaniem odpowiedzialności za wdrożenie środków, zgodnie z pkt 2.1 załącznika do 2024/2690.

Zamawiający ustanawia i utrzymuje procedury obsługi incydentów, obejmujące detekcję, analizę, reagowanie, usuwanie skutków, dokumentowanie oraz raportowanie, z mapowaniem na terminy wymagane przez NIS2 i integracją z planami ciągłości działania. W zakresie koordynacji reżimów prawnych proces zgłoszeń naruszeń danych osobowych zgodnie z art. 33 RODO synchronizuje się z obowiązkami wynikającymi z NIS2, co w praktyce wymaga ścisłej współpracy z inspektorem ochrony danych. Współpraca międzysektorowa obejmuje wymianę informacji z CSIRT i ENISA, a w sektorze finansowym także z organami właściwymi dla DORA, tak aby wymagania były spójne z tym aktem i aby zapewnione było informowanie forum nadzoru. Jako narzędzi można używać odwołań do europejskich programów certyfikacji cyberbezpieczeństwa przewidzianych w rozporządzeniu 2019/881 lub, w braku adekwatnych programów, do norm europejskich.

### 2.1.7.6. Sankcje i odpowiedzialność

W reżimie publicznoprawnym przewidzianym przez NIS2 organ nadzoru stosuje wobec podmiotów kluczowych i ważnych środki egzekwowania obejmujące ostrzeżenia, wiążące polecenia i nakazy, w tym doprowadzenie środków z art. 21 do zgodności, nakazy informacyjne, publikację naruszeń oraz wyznaczenie urzędnika monitorującego, a ponadto administracyjne kary pieniężne. Wysokość kar dla podmiotów kluczowych wynosi co najmniej 10 000 000 EUR lub 2 procent globalnego obrotu za poprzedni rok obrotowy, przy czym stosuje się kwotę wyższą. Dla podmiotów ważnych minimalne progi wynoszą 7 000 000 EUR lub 1,4 procent globalnego obrotu. Nakładając kary, organ kieruje się zasadą proporcjonalności oraz bierze pod uwagę między innymi skalę i czas trwania naruszenia, wielkość szkody, zawinienie lub zaniedbanie oraz poziom współpracy z organem. Zapewnia się koordynację z przepisami o ochronie danych osobowych, tak aby unikać podwójnego karania za to samo zachowanie.

W zakresie odpowiedzialności kontraktowej umowa przewiduje adekwatne kary umowne i środki naprawcze za naruszenia wymagań bezpieczeństwa, na przykład za brak zgłoszenia incydentu w terminie, niewywiązanie się ze zobowiązań dotyczących podatności, odmowę przeprowadzenia audytu, naruszenie warunków dotyczących podwykonawstwa lub zasad wyjścia. Postanowienia te pozostają spójne z katalogiem elementów umownych wskazanych w akcie 2024/2690.

**Typowe „czerwone flagi”**

- Brak/niekompletny rejestr dostawców lub jego nieaktualizowanie – naruszenie pkt 5.2 rozporządzenia 2024/2690.
- Brak procedur i testów incydentowych albo brak przeglądów po-incydentowych – wbrew pkt 3.1.1–3.1.3 rozporządzenia 2024/2690.
- Odmowa prawa audytu lub nieprzekazanie raportów z audytu – sprzeczne z pkt 5.1.4 lit. e rozporządzenia 2024/2690.
- Brak procesu zarządzania podatnościami (także wobec publicznie ujawnionych) – sprzeczne z pkt 5.1.4 lit. f rozporządzenia 2024/2690.
- Niespójne zgłaszanie incydentów (opóźnienia, niekompletne treści) względem reżimu NIS2 (24 h/72 h/1 miesiąc).

### 2.5.9. Zależności z innymi aktami (matryca zbieżności/kolizji)

| Akt | Relacja do NIS2 | Implikacje dla zamówień publicznych |
|---|---|---|
| **DORA** (rozporządzenie 2022/2554) | Współpraca organów NIS2 z forum nadzoru DORA; dla podmiotów finansowych DORA działa jako reżim sektorowy; NIS2 przewiduje, że gdy akty sektorowe nakładają równoważne obowiązki (środki + raportowanie), mają one pierwszeństwo dla objętych podmiotów. | Zapewnić zgodność OPZ/umowy z wymaganiami DORA; weryfikować, czy kryteria i klauzule umowne ustanawiają wymogi dla krytycznych dostawców ICT i nadzór trzeciej linii. |
| **eIDAS** (rozp. 910/2014; usługi zaufania) | NIS2 rozszerza horyzontalne obowiązki cyber (zarządzanie ryzykiem i raportowanie) na dostawców usług zaufania – uzupełnienie względem wymogów eIDAS (kwalifikowani dostawcy nadal podlegają art. 24 eIDAS). | W zakupach usług zaufania przewidywać wymagania i klauzule spójne zarazem z eIDAS i NIS2 (w tym notyfikacje incydentowe i ciągłość). |
| **RODO/GDPR** (rozp. 2016/679) | Zsynchronizowane raportowanie (single reporting point); unikanie podwójnych kar za to samo zachowanie; ścisła współpraca organów NIS2 i DPA. | Wymaga integracji procedur incydentowych (NIS2 + RODO) i roli IOD/DPO w łańcuchu eskalacji. |
| **CRA** (horyzontalne wymogi cyber dla produktów z elementami cyfrowymi) | 2024/2690 zaleca, by przy określaniu wymogów dla nabywanych produktów ICT uwzględniać zasadnicze wymogi CRA; dopuszcza oparcie się na programach certyfikacji UE i deklaracjach zgodności. | W OPZ można wymagać zgodności produktów z zasadniczymi wymogami (gdy obowiązują) lub równoważności; ułatwia walidację i porównywalność ofert. |

NIS2 wprost przewiduje relację lex specialis: jeśli sektorowy akt UE przewiduje obowiązki co najmniej równoważne (środki/raportowanie), stosuje się reżim sektorowy; NIS2 działa uzupełniająco dla nieobjętych.

## 2.2. CRA

### 2.2.1. Identyfikacja aktu

| | |
|---|---|
| **Pełna nazwa** | Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi (akt o cyberodporności, „CRA"). |
| **Rodzaj aktu** | • Rozporządzenie (bezpośrednio stosowane we wszystkich państwach członkowskich).<br>• Opublikowane 20.11.2024; wchodzi w życie 20. dnia po publikacji; stosuje się co do zasady od 11.12.2027 r. Wyjątki: art. 14 od 11.09.2026 r., rozdział IV (art. 35–51) od 11.06.2026 r. Przepisy przejściowe m.in. utrzymują ważność istniejących certyfikatów do 11.06.2028 r. oraz określają zasady dla produktów wprowadzonych przed 11.12.2027 r. |
| **Status / terminy** | • Akt ma charakter horyzontalny (nie ogranicza się do konkretnych sektorów), obejmuje produkty z „elementami cyfrowymi" udostępniane na rynku UE i wymagania bezpieczeństwa na etapie projektowania, wytwarzania oraz obsługi podatności; przewiduje też nadzór rynku.<br>• Jednocześnie wyłącza m.in. wyroby objęte przepisami o wyrobach medycznych, pojazdach i lotnictwie oraz pozwala ograniczać/zawieszać stosowanie tam, gdzie przepisy sektorowe zapewniają co najmniej równoważny poziom ochrony. |
| **Właściwe organy** | • Nadzór rynku sprawują organy wyznaczone zgodnie z rozporządzeniem (UE) 2019/1020; dla systemów SI wysokiego ryzyka właściwe są organy nadzoru wyznaczone na mocy aktu o SI (UE) 2024/1689, we współpracy z organami CRA, CSIRT-ami (w zakresie zgłoszeń z art. 14) i ENISA; działa też grupa koordynacyjna ADCO. |

### 2.2.2. Cel i zakres przedmiotowy

Dotychczasowe prawo UE obejmowało wybrane aspekty cyberbezpieczeństwa (np. Uprawnienia ENISA i certyfikację z rozporządzenia 2019/881, obowiązki organizacyjne z NIS2, sektorowe wymogi dla sektora finansowego w DORA), ale brakowało obowiązkowych, horyzontalnych wymagań bezpieczeństwa dla samych

produktów z elementami cyfrowymi[52]. CRA wypełnia tę lukę: ustanawia zasadnicze wymagania projektowo-wytwórcze i eksploatacyjne dla produktów oraz powiązane procedury oceny zgodności i nadzoru rynku[53].

CRA ma charakter horyzontalny – stosuje się do „produktów z elementami cyfrowymi" udostępnianych na rynku UE (sprzęt i oprogramowanie, w tym komponenty), określając wymagania na etapie projektowania, opracowania, produkcji i obsługi podatności, a także ramy nadzoru rynku[54]. Akt przewiduje też mechanizmy spójności z innym prawem harmonizacyjnym UE (np. ogólne bezpieczeństwo produktów, gdy dane zagrożenie nie jest objęte CRA)[55].

W zakresie relacji z AI Act (2024/1689): jeśli produkt z elementami cyfrowymi jest jednocześnie systemem SI wysokiego ryzyka, uznaje się jego zgodność z wymogami cyber CRA, o ile spełnia zasadnicze wymagania z załącznika I oraz procedury producenta odpowiadają wymaganiom części II tego załącznika; w takich przypadkach stosuje się odpowiednie procedury oceny zgodności z AI Act, z zastrzeżeniami opisanymi w CRA[56].

**Wyłączenia i doprecyzowania zakresu**

- Wolne i otwarte oprogramowanie (OSS): CRA obejmuje wyłącznie OSS udostępniane na rynku w ramach działalności handlowej; samo opracowywanie/utrzymywanie OSS co do zasady nie stanowi działalności handlowej na potrzeby CRA[57].
- Reżimy sektorowe o równoważnym poziomie ochrony: dla sprzętu objętego szczegółowymi przepisami sektorowymi (np. wyroby medyczne, diagnostyka in vitro, pojazdy – homologacja i regulaminy ONZ 155, lotnictwo) CRA przewiduje ograniczenia/wyłączenia lub rozdział

[52] Zob. Motyw 2 CRA; Komisja Europejska, *Commission Staff Working Document. Impact Assessment Report. Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*, Brussels, 15.9.2022, SWD(2022) 282 final, PART 1/3, {COM(2022) 454 final}, {SEC(2022) 321 final}, {SWD(2022) 283 final}, s. 18–20, [online:] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment [dostęp: 11.11.2025].

[53] Komisja Europejska, *Impact Assessment Report* do wniosku CRA, SWD(2022) 282 final, s. 4-5.

[54] Zob. Motyw 11-13 CRA.

[55] Zob. Motyw 13 CRA.

[56] Zob. Motyw 51 CRA.

[57] Zob. art. 13 CRA.

kompetencji, aby unikać dublowania wymogów i zachować spójność norm technicznych i ocen zgodności[58].

- Powiązanie z ogólnym bezpieczeństwem produktów (GPSR 2023/988): w odniesieniu do zagrożeń nieobjętych CRA stosuje się odpowiednie rozdziały GPSR (na zasadzie odesłania), o ile produkt nie podlega innemu prawu harmonizacyjnemu[59].
- Odstępstwa i doprecyzowania techniczne: Komisja może – w drodze aktów delegowanych – wskazywać produkty/obszary, dla których stosuje się ograniczenia lub wyłączenia; przewidziano też szczególne rozwiązania dla części zamiennych oraz powiązania z regulacjami dot. urządzeń radiowych i ich norm[60].

CRA tworzy wspólne minimum wymagań produktowych (załącznik I) oraz przewiduje możliwość obowiązkowej certyfikacji UE dla wybranych kategorii produktów krytycznych (z odpowiednim poziomem uzasadnienia zaufania), co ma bezpośrednie znaczenie dla OPZ i weryfikacji zgodności w postępowaniach.

### 2.2.3. Obowiązki z perspektywy nabywcy

**Typowa sytuacja: zamawiający = użytkownik końcowy**

W typowej sytuacji zamówień publicznych zamawiający pełni rolę użytkownika końcowego: instytucja publiczna nabywa produkt z elementami cyfrowymi na własne potrzeby, nie wprowadza go do obrotu pod własną marką, nie importuje go samodzielnie spoza UE i nie prowadzi dalszej dystrybucji. W konsekwencji na gruncie CRA nie staje się adresatem obowiązków właściwych producentom, importerom ani dystrybutorom. Ciążą na nim jednak obowiązki po stronie nabywcy, polegające na egzekwowaniu zgodności od wykonawcy na etapie postępowania i realizacji, tak aby przedmiot zamówienia spełniał wymagania CRA oraz był utrzymywany w zgodności w okresie eksploatacji.

**W praktyce zamówień publicznych**

*W OPZ/SWZ i umowie należy wymagać m.in. deklaracji zgodności UE i oznakowania CE potwierdzających spełnienie zasadniczych wymagań CRA, właściwej procedury oceny zgodności (samodzielnej albo z udziałem strony trzeciej – zależnie od*

[58] Zob. Motyw 27.
[59] Zob. Motyw 50.
[60] Zob. Motyw 47 oraz art. 7 i 8 CRA.

*kategorii/krytyczności), spełnienia obowiązków producenta dot. obsługi podatności i aktualizacji bezpieczeństwa w całym cyklu życia.*

**Kiedy zamawiający wejdzie w reżim CRA**

Poniższe scenariusze są w administracji publicznej rzadkie, ale „podnoszą" zamawiającego do rangi adresata obowiązków CRA:

1. **Producent**
    a. Zamawiający zleca wytworzenie pod własną marką („white-label"), istotnie modyfikuje produkt[61] już udostępniony na rynku (w stopniu mogącym wpływać na zgodność), albo integruje komponenty w „nowy" wyrób i udostępnia go na rynku (np. przekazuje innym jednostkom jako produkt)[62].
    b. Skutek: pełne obowiązki producenta (zasadnicze wymagania z załącznika I, ocena zgodności, dokumentacja techniczna, nadzór rynku, CE, deklaracja zgodności, proces obsługi podatności i zgłaszania określonych incydentów/podatności).
2. **Importer**
    a. Zamawiający sprowadza produkt spoza UE we własnym imieniu, a następnie udostępnia go na rynku w UE (np. dystrybuuje do innych jednostek, oddziałów)[63].
    b. Skutek: obowiązki importera (weryfikacja, czy producent przeprowadził ocenę zgodności, sporządził deklarację i oznakował CE; zapewnienie, że warunki magazynowania/transportu nie naruszają zgodności; działania korygujące/wycofania, współpraca z nadzorem rynku)[64].
3. **Dystrybutor**
    a. Zamawiający przekazuje dalej zakupione wyroby na rynek UE (np. centralny zamawiający kupuje, a następnie dystrybuuje jednostkom podległym)[65].

[61] Zob. art. 3 pkt. 13 i 30 CRA.
[62] Zob. art. 13, 14 i 21 CRA.
[63] Zob. art. 13 ust. 15, 16 i 19 CRA.
[64] Zob. art. 19 ust. 3, 4, 8 CRA.
[65] Zob. art. 20 ust. 1-6.

b. Skutek: obowiązki dystrybutora (należyta staranność: CE, deklaracja, identyfikowalność; reagowanie na niezgodności, współpraca z nadzorem).

**Wniosek:** w przeważającej większości postępowań podmiotem „objętym PZP" będzie zwykły zamawiający-użytkownik, który nie jest adresatem sankcji CRA, ale ma obowiązek tak prowadzić zakupy, by na rynek/na użytek publiczny trafiały produkty zgodne z CRA i by umowy zapewniały utrzymanie tej zgodności w eksploatacji.

## Co z tego wynika „dla nabywcy" — minimalny zestaw wymagań do postępowań

Na etapie planowania oraz w OPZ i SWZ należy wymagać od wykonawcy dostarczenia wyrobu zgodnego z CRA, właściwej klasy lub kategorii, jeśli ma zastosowanie, oznakowanego CE i z deklaracją zgodności UE wskazującą zastosowane normy zharmonizowane lub specyfikacje[66]. W przypadku wyrobów należących do kategorii krytycznych trzeba przewidzieć odpowiednią procedurę oceny zgodności z udziałem strony trzeciej albo, jeżeli zostanie nałożona, obowiązkową certyfikację unijną[67]. W umowie trzeba uregulować aktualizacje i łatanie, w tym czas, zakres i kanał dystrybucji poprawek, a także obsługę podatności, w szczególności przyjmowanie zgłoszeń, informowanie użytkownika, ponadto informowanie o incydentach bezpieczeństwa produktu, identyfikowalność komponentów istotnych dla bezpieczeństwa w zakresie adekwatnym do wyrobu, współpracę przy działaniach korygujących, takich jak wycofanie czy ostrzeżenia bezpieczeństwa, oraz prawo zamawiającego do audytu dokumentacji zgodności w uzasadnionym zakresie[68]. Na etapie odbioru i w trakcie eksploatacji weryfikuje się kompletność dokumentów zgodności, działanie mechanizmu aktualizacji i kanałów powiadomień oraz spełnianie deklarowanych właściwości bezpieczeństwa przy użyciu testów i inspekcji proporcjonalnych do ryzyka[69].

---

[66] Zob. wymogi załącznika VIII CRA i konieczność zgodności z modelem A, B + C lub H.

[67] Zob: art. 8 ust. 1–2 w zw. z załącznikiem IV (obowiązek unijnej certyfikacji oraz delegowane akty; w braku programu certyfikacji zastosowanie procedur z art. 32 ust. 3), art. 32 ust. 3–4 oraz art. 32 ust. 2 ak. 2 (moduły B+C lub H i „fallback" gdy brak norm/specyfikacji/programu), art. 7 ust. 4 (opis techniczny kat. ważnych i krytycznych), motywy 44, 48, 91.

[68] Zob. zał. I część II pkt 1–2; art. 13; art. 14; art. 31 i zał. VII; art. 19–20 CRA.

[69] Zob. art. 28–31; zał. VII; zał. I część II pkt 1–2; art. 13 ust. 3–4 CRA.

**Które „produkty z elementami cyfrowymi" będą krytyczne dla PZP**

Na etapie planowania oraz w OPZ i SWZ należy wymagać od wykonawcy dostarczenia wyrobu zgodnego z CRA, właściwej klasy lub kategorii, jeśli ma zastosowanie, oznakowanego CE i z deklaracją zgodności UE wskazującą zastosowane normy zharmonizowane lub specyfikacje. Jeżeli wyrób należy do kategorii krytycznych, należy przewidzieć odpowiednią procedurę oceny zgodności z udziałem strony trzeciej lub, gdy zostanie nałożona, obowiązkową certyfikację unijną[70]. Postanowienia umowy powinny regulować aktualizacje i łatanie, w tym czas, zakres i kanał dystrybucji poprawek, a także obsługę podatności obejmującą przyjmowanie zgłoszeń, remediację i informowanie użytkownika; dodatkowo powinny określać zasady informowania o incydentach bezpieczeństwa produktu, identyfikowalności komponentów istotnych dla bezpieczeństwa w zakresie adekwatnym do wyrobu, współpracy przy działaniach korygujących, takich jak wycofanie czy ostrzeżenia bezpieczeństwa, oraz prawo zamawiającego do audytu dokumentacji zgodności w uzasadnionym zakresie[71]. Na etapie odbioru i w trakcie eksploatacji weryfikuje się kompletność dokumentów zgodności, działanie mechanizmu aktualizacji i kanałów powiadomień oraz spełnianie deklarowanych właściwości bezpieczeństwa, z wykorzystaniem testów i inspekcji proporcjonalnych do ryzyka.

**Podsumowanie**

Domyślnie zamawiający występuje jako użytkownik końcowy i egzekwuje zgodność z rozporządzeniem CRA od wykonawcy, sam natomiast nie jest adresatem obowiązków producenta, importera ani dystrybutora. Wyjątki pojawiają się wtedy, gdy zamawiający dokonuje rebrandingu lub projektowania, wprowadza istotne modyfikacje, importuje albo dystrybuuje wyrób; w takich sytuacjach przyjmuje rolę operatora gospodarczego i odpowiednie obowiązki wynikające z CRA, co należy uwzględnić w strukturze projektu oraz w treści umów. W dokumentach zamówienia należy wprowadzić twarde wymagania zgodności, w szczególności oznakowanie CE, deklarację zgodności UE, właściwą procedurę oceny zgodności oraz mechanizmy aktualizacji i obsługi podatności, a następnie kontrolować ich spełnienie na etapie odbioru i w okresie eksploatacji.

### 2.2.4. Wymogi dotyczące łańcucha dostaw produktu (CRA)

[70] Zob. zał. I część I–II; art. 28–31; zał. V, VII CRA.

[71] Zob. zał. I część II pkt 1–2; art. 13 (w tym ust. 24) CRA.

#### 2.2.4.1. Odpowiedzialność podstawowa (kto co wnosi do łańcucha).

Podstawowy podział ról w łańcuchu dostaw kształtuje odpowiedzialność każdego uczestnika. Producent odpowiada za spełnienie zasadniczych wymagań bezpieczeństwa na etapie projektowania, wytwarzania i utrzymania wyrobu, sporządza dokumentację techniczną, przeprowadza ocenę zgodności, wystawia unijną deklarację zgodności i umieszcza oznakowanie CE[72]. Zapewnia również obsługę podatności i dostarcza aktualizacje bezpieczeństwa przez zadeklarowany okres wsparcia. Jeżeli ustanowiono upoważnionego przedstawiciela, działa on w imieniu producenta w zakresie powierzonych zadań. Importer, wprowadzając produkt spoza Unii Europejskiej, weryfikuje dopełnienie obowiązków producenta, w szczególności kompletność dokumentów, prawidłowość oznakowania CE, dostępność instrukcji i danych kontaktowych. Dystrybutor zapewnia, aby do obrotu nie trafiały produkty niezgodne, reaguje na sygnały o niezgodności i współpracuje z organami nadzoru rynku[73].

W odniesieniu do składników i podwykonawców producent zarządza ryzykiem pochodzącym od komponentów sprzętowych i programowych, w tym komponentów stron trzecich, tak aby wyrób końcowy spełniał zasadnicze wymagania z załącznika I do CRA[74]. W praktyce obejmuje to dobór dostawców według kryteriów bezpieczeństwa, w szczególności zgodności praktyk wytwarzania oprogramowania i zdolności do zapewnienia wsparcia aktualizacyjnego, pozyskiwanie od nich informacji niezbędnych do oceny ryzyka produktu, kontrolę zmian, w tym substytucji komponentów, a także zapewnienie, że podatności w komponentach są obsługiwane i w sposób właściwy komunikowane użytkownikom.

Obsługa podatności i incydentów po stronie produktu wymaga ustanowienia publicznie dostępnego kanału przyjmowania zgłoszeń, prowadzenia klasyfikacji zgłoszeń, niezwłocznej remediacji oraz publikowania informacji o poprawkach i ich wpływie, przy jednoczesnym utrzymywaniu rejestru działań. W razie poważnych zagrożeń bezpieczeństwa produktu stosuje się procedury wycofania lub publikowania ostrzeżeń, a producent współpracuje z właściwymi organami, w tym z nadzorem rynku oraz, gdy występuje związek z NIS2, z właściwymi CSIRT.

[72] Zob. zał. I; art. 13; art. 31 i zał. VII CRA.

[73] Zob. art. 13–14; art. 18; art. 19; art. 20; art. 28–31 CRA.

[74] Zob. art. 13 ust. 5–8; art. 13 ust. 24; zał. I część II pkt 1 oraz pkt 3–8 CRA.

W łańcuchu dostaw funkcjonują zarówno artefakty obowiązkowe, jak i dodatkowe, uzasadnione kontraktowo. Do obowiązkowych należą unijna deklaracja zgodności, oznakowanie CE, dokumentacja oraz instrukcje dla użytkownika, obejmujące zasady instalacji, konfiguracji i aktualizacji, informacja o okresie wsparcia bezpieczeństwa oraz opis procesu zgłaszania podatności. W zależności od specyfiki projektu można uzgodnić dodatkowe materiały, na przykład wykaz istotnych dla bezpieczeństwa komponentów w poziomie szczegółowości adekwatnym do wyrobu, raport z oceny zgodności, jeżeli uczestniczyła strona trzecia, wykaz norm zharmonizowanych lub specyfikacji zastosowanych do wykazania zgodności oraz raporty z testów bezpieczeństwa. Zestawienia SBOM i komunikaty VEX nie są wymagane wprost przez CRA, mogą jednak zostać przewidziane umownie jako instrumenty przejrzystości i ułatwienia walidacji.

W zakresie nadzoru rynku i działań korygujących operatorzy gospodarczy współpracują z organami, udostępniają wymaganą dokumentację, wykonują wydane polecenia oraz prowadzą działania korygujące, w tym wycofania, jeśli zachodzi taka potrzeba. Informacja o działaniach korygujących powinna być przekazywana w całym łańcuchu aż do użytkowników końcowych, w tym do zamawiających publicznych.

### 2.2.5. Wpływ CRA na cykl zamówień publicznych

#### 2.2.5.1. Planowanie / analiza potrzeb

Na etapie planowania ustala się kwalifikację przedmiotu zamówienia, w szczególności czy nabywany wyrób jest „produktem z elementami cyfrowymi” w rozumieniu CRA oraz czy należy do kategorii wymagających oceny zgodności z udziałem strony trzeciej lub, w przyszłości, obowiązkowej certyfikacji unijnej. Równolegle ocenia się krytyczność i ryzyko, określając wpływ wyrobu na usługi publiczne i infrastrukturę, przewidywany okres wsparcia bezpieczeństwa, czyli liczbę lat aktualizacji, a także ryzyko lock-in, na przykład zależność od zamkniętego kanału aktualizacji jednego wykonawcy. Analizie poddaje się zależności od komponentów oraz od podmiotów z państw trzecich, identyfikując potencjalne pojedyncze punkty awarii, i planuje wymagania dotyczące przenoszalności lub możliwości zastąpienia komponentów w zakresie, w jakim jest to realistyczne. Jeżeli zamawiający sam podlega NIS2, przygotowuje się synchronizację procesów po stronie dostawcy produktu z własnymi procedurami obsługi incydentów i

podatności, w tym terminami i formatami raportowania, tak aby zapewnić pełne wywiązanie się z obowiązków wynikających z NIS2.

#### 2.2.5.2. OPZ / SWZ (wymogi techniczne, funkcjonalne i bezpieczeństwa)

Weź pod uwagę co najmniej:

- Zgodność z CRA
  - produkt musi spełniać zasadnicze wymagania (załącznik I do CRA) , mieć CE i UE-deklarację zgodności; wskaż normy zharmonizowane lub dopuszczalną równoważność (dla przejrzystości oceny).
- Okres wsparcia bezpieczeństwa
  - minimalny czas zapewniania aktualizacji bezpieczeństwa (np. x lat), maks. czasy dostarczenia łatki na podatności wysokiej/krytycznej, sposób powiadamiania (RSS, mailing, portal).
- Obsługa podatności
  - wymagany publiczny kanał zgłoszeń, SLA na potwierdzenie przyjęcia i publikację informacji, procedury komunikowania skutków i zaleceń.
- Instrukcje i konfiguracja
  - dostarczenie wytycznych bezpiecznej konfiguracji/eksploatacji, listy wymagań środowiskowych (np. twardnienie systemu, kontrola dostępu, logowanie).
- Informacje o komponentach istotnych dla bezpieczeństwa
  - na poziomie adekwatnym do wyrobu (np. biblioteki kryptograficzne, komponenty zewnętrzne wymagające niezależnych aktualizacji), wraz z zasadami informowania o ich zmianie.
- Ocena zgodności
  - gdy wymagana jest jednostka notyfikowana – wskaż akceptowalne moduły/procedury; przewidź dostarczenie raportu/świadectwa (lub dostępu do niego).

#### 2.2.5.3. Warunki udziału (zdolności techniczne i zawodowe)

- Zdolność zapewnienia wsparcia bezpieczeństwa
  - wymóg potwierdzenia, że wykonawca (lub producent) zapewnia aktualizacje przez wskazany okres i posiada proces zarządzania podatnościami (z publicznym VDP).
- Kompetencje personelu
  - osoby odpowiedzialne za utrzymanie/aktualizacje mają odpowiednie kwalifikacje/certyfikaty (gdzie zasadne).

- Doświadczenie
    - referencje w dostawach/utrzymaniu produktów analogicznej klasy bezpieczeństwa (np. urządzenia sieciowe, oprogramowanie systemowe).
- Zgodność/certyfikacja
    - jeśli dla danej klasy istnieje program certyfikacji UE lub specyfikacje wspólne – można żądać certyfikatu albo równoważności; w pozostałych przypadkach – zgodności z normami zharmonizowanymi.

#### 2.2.6. Kryteria oceny ofert (jakościowe „pro-security")

Ocena obejmuje długość i jakość wsparcia bezpieczeństwa, w szczególności liczbę lat utrzymania, politykę EOL/EOS oraz gwarantowane czasy reakcji na podatności krytyczne i wysokie. Brana jest pod uwagę przejrzystość oraz gotowość na zgłoszenia, to jest publiczna polityka VDP, sposób publikacji biuletynów bezpieczeństwa i jakość dokumentacji aktualizacji. Istotna jest przenoszalność oraz ograniczenie ryzyka lock-in, w tym możliwość eksportu konfiguracji i danych, użycie otwartych formatów oraz dostępność narzędzi aktualizacyjnych bez dodatkowych licencji. Dodatkowym kryterium jest walidacja bezpieczeństwa obejmująca zakres i częstotliwość testów oraz dostępność raportów z oceny zgodności lub testów penetracyjnych w granicach uzasadnionych ochroną tajemnicy.

#### 2.2.7. 5.5. Klauzule umowne (SLA/OLA, audyt, wgląd, incydenty, podwykonawcy, dane/transfery, „exit", sankcje)

Wpisz do umowy co najmniej:

1. Zgodność z CRA zachowana przez cały okres wsparcia; obowiązek aktualizacji i informowania o podatnościach/ryzykach bezpieczeństwa produktu.
2. SLA dla aktualizacji bezpieczeństwa (np. krytyczne: ≤ x dni; wysokie: ≤ y dni), kanały powiadomień i sposób dystrybucji łatek.
3. VDP i kontakt bezpieczeństwa: działający kanał zgłoszeń (adres/portal), terminy potwierdzeń i publikacji biuletynów.
4. Prawo audytu/inspekcji w zakresie dokumentów zgodności (UE-deklaracja, wyniki oceny zgodności, raporty z testów w uzasadnionym zakresie) oraz prawo żądania działań korygujących.

5. Zarządzanie komponentami i podwykonawcami: obowiązek informowania o zmianach komponentów istotnych dla bezpieczeństwa; przełożenie wymagań bezpieczeństwa na podwykonawców; zasady dla części zamiennych.
6. Procedura wycofania/ostrzeżeń: obowiązki informacyjne i wsparcie działań korygujących, w tym dostarczenie alternatyw/obejść do czasu poprawki.
7. „Exit plan" i przenoszalność: przekazanie informacji/dokumentów potrzebnych do dalszego utrzymania bezpieczeństwa po zakończeniu umowy (w tym historii aktualizacji, konfiguracji).
8. Sankcje: kary umowne za opóźnione łatki krytyczne/wysokie, brak powiadomienia o podatności, odmowę udostępnienia UE-deklaracji/raportów; możliwość rozwiązania umowy w razie stwierdzonej niezgodności z prawem (decyzja organu nadzoru, zakaz udostępniania na rynku).

### 2.2.8. Dowody zgodności / walidacja

**Co można żądać i kiedy w cyklu postępowania**

**Na wejściu (oferta / kwalifikacja)**

- UE-deklaracja zgodności (albo oświadczenie, że zostanie dostarczona najpóźniej przy odbiorze, jeśli produkt jest nowy), oraz oznaczenie CE na wyrobie/opakowaniu/dokumentacji.
- Identyfikacja zastosowanych norm zharmonizowanych (lub innych specyfikacji technicznych) użytych do wykazania zgodności z zasadniczymi wymaganiami bezpieczeństwa z załącznika I CRA.
- Wskazanie zastosowanej procedury oceny zgodności (czy z udziałem strony trzeciej, jakiej jednostki; w przypadku wyrobów z grup zwiększonego ryzyka – odpowiednia „modułowa" procedura).
- Informacja o okresie wsparcia bezpieczeństwa (czas dostarczania aktualizacji) i polityka obsługi podatności (kanał zgłoszeń, czasy reakcji/napraw).
- Instrukcje bezpiecznej instalacji/konfiguracji/eksploatacji (w tym wymagania środowiskowe systemu, warunki bezpiecznej aktualizacji).
- W razie importu spoza UE – dowody wykonania obowiązków importera (weryfikacja dokumentacji producenta).

**W realizacji (po podpisaniu umowy)**

- Kopia deklaracji zgodności UE i pełna dokumentacja wydania (wersja, data, zakres).
- Raport/świadectwo z oceny zgodności (jeśli brała udział jednostka notyfikowana) albo dostęp do niego.
- Biuletyny bezpieczeństwa i harmonogramy aktualizacji (dowody, że mechanizm aktualizacji działa i jest utrzymywany).
- Rejestr zgłoszeń podatności/incydentów produktowych dotyczących dostarczonego wyrobu oraz dowody reakcji (naprawy, „work-aroundy", wycofania).

**Okresowo (w toku eksploatacji)**

- Aktualne oświadczenie o utrzymaniu zgodności po znaczących aktualizacjach funkcjonalnych/bezpieczeństwa.
- Dowody utrzymania wsparcia (statystyki łatek, czasu reakcji, publikacji biuletynów).
- Na żądanie: przeglądy zgodności po poważnym incydencie lub istotnej zmianie komponentu.

### 2.2.9. Rola i obowiązki po stronie zamawiającego

Po stronie zamawiającego leży utrzymanie ładu organizacyjnego w obszarze bezpieczeństwa produktów z elementami cyfrowymi, z jednoznacznym przypisaniem odpowiedzialności, na przykład sponsora po stronie kierownictwa oraz właściciela bezpieczeństwa produktu po stronie IT lub OT, a także prowadzenie regularnych przeglądów zgodności dostaw. Procedura zakupowa jest powiązana z bezpieczeństwem produktu i obejmuje włączenie wymogów CRA do OPZ i SWZ, do kryteriów oceny oraz do umowy, w szczególności w zakresie oznakowania CE, deklaracji zgodności, okresu wsparcia oraz zasad obsługi podatności. Zamawiający prowadzi rejestr produktów z elementami cyfrowymi i dostawców, obejmujący informacje o dostawcy, wersji i konfiguracji, okresie wsparcia oraz kanałach VDP i biuletynach bezpieczeństwa, a rejestr ten jest powiązany z ewidencją umów i konfiguracji.

Procedury incydentowe integrują zgłoszenia produktowe wynikające z CRA z wewnętrzną ścieżką reagowania i są mapowane na potencjalne obowiązki z NIS2, jeżeli zamawiający sam podlega tej dyrektywie. W ramach oceny ryzyka i zarządzania zmianą analizuje się wpływ modyfikacji komponentów i wersji na zgodność oraz podejmuje decyzje dotyczące przyjmowania poprawek i planów wycofania, z uwzględnieniem EoL i EoS. Nadzór nad podwykonawcami wykonawcy zapewnia przeniesienie w łańcuchu kontraktowych obowiązków producenta,

importera lub dystrybutora, w szczególności w zakresie informowania o podatnościach oraz prowadzenia działań korygujących.

### 2.2.10. Sankcje i odpowiedzialność

**Reżim publicznoprawny (administracyjny)**

- Nadzór rynku może żądać dokumentacji, nakazywać usunięcie niezgodności, ograniczać lub zakazać udostępniania produktu, zarządzać wycofania/wezwania do naprawy; za naruszenia grożą administracyjne kary pieniężne (wysokość określona w CRA i przepisach krajowych wykonujących nadzór rynku).
- Wytwórcy/importerzy/dystrybutorzy odpowiadają za brak zgodności (np. brak CE, brak deklaracji, niewłaściwa procedura oceny zgodności, niewywiązywanie się z obsługi podatności).

**Reżim kontraktowy (umowny)**

- Kary umowne i/lub potrącenia za: niedostarczenie CE/deklaracji, opóźnione łatki bezpieczeństwa (zwłaszcza „krytyczne/wysokie"), brak biuletynów/komunikacji, odmowę udostępnienia raportu z oceny zgodności, niewykonanie działań korygujących/wycofania.
- Prawo do odstąpienia/rozwiązania umowy w razie decyzji nadzoru rynku zakazującej udostępniania produktu lub stwierdzającej istotną niezgodność.

**„Czerwone flagi" w nadzorze realizacji**

- Brak deklaracji zgodności UE lub deklaracja bez wskazania norm/specyfikacji; rozbieżność między deklaracją a stanem dostawy.
- Brak działającego mechanizmu aktualizacji (niedostarczanie poprawek w deklarowanym czasie).
- Niepubliczny lub fikcyjny kanał zgłaszania podatności; brak reakcji na zgłoszenia.
- Częste „ciche" zmiany komponentów krytycznych bez informacji dla użytkownika i bez ponownej oceny zgodności (ryzyko utraty zgodności).
- Komunikaty nadzoru rynku (ostrzeżenia, wycofania) ignorowane przez wykonawcę.

### 2.2.11. Zależności z innymi aktami (zbieżności/kolizje)

| Akt | Relacja do CRA | Implikacje dla zamówień publicznych |
|---|---|---|

| | | |
|---|---|---|
| **NIS2** | NIS2 adresuje organizacyjne/operacyjne środki bezpieczeństwa i obowiązki incydentowe u podmiotów świadczących usługi, CRA – wymogi dla samego produktu. | Dla usług + produktów wymagaj obu perspektyw: środki NIS2 (procesy, incydenty) oraz zgodność produktu z CRA (CE, deklaracja, aktualizacje). |
| **RODO (GDPR)** | Jeśli produkt przetwarza dane osobowe, bezpieczeństwo z CRA współgra z zasadą „privacy by design/by default"; naruszenie produktu może skutkować naruszeniem danych. | Zsynchronizuj procedury: ścieżka naruszeń danych (RODO) + ścieżka błędów/podatności produktu (CRA). |
| **AI Act** | Dla systemów SI wysokiego ryzyka istnieją specjalne procedury oceny zgodności; ich spełnienie może pokrywać wymogi cyber z CRA (w określonych warunkach). | W OPZ określ, czy produkt podpada pod AI Act; odpowiednio dobierz dokumenty zgodności (raporty, certyfikaty). |
| **Radio Equipment, ETSI/RED** | Część urządzeń radiowych podlega wymaganiom bezpieczeństwa wg RED i norm ETSI; CRA zapewnia spójność i nie dubluje, gdy poziom ochrony jest równoważny. | Dla urządzeń radiowych żądaj zgodności z właściwymi normami ETSI + CRA (w razie zbiegu – zgodność sektorowa ma pierwszeństwo w zakresie pokrycia). |
| **Cybersecurity Act (2019/881)** | Ramy europejskiej certyfikacji cyberbezpieczeństwa; CRA może odwoływać się do programów certyfikacji dla wybranych klas produktów. | Jeśli istnieje program certyfikacji UE dla danej klasy – można żądać certyfikatu lub równoważności. |

## 2.3. Ustawa o krajowym systemie cyberbezpieczeństwa

### 2.3.1. Cel i zakres nowelizacji ustawy KSC

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) jest bezpośrednio związana z wdrożeniem unijnej Dyrektywy NIS 2 (UE 2022/2555) do polskiego prawa[75]. Głównym celem nowelizacji jest rozszerzenie zakresu podmiotów objętych obowiązkami cyberbezpieczeństwa oraz zaostrzenie wymagań dotyczących ochrony systemów informacyjnych w kluczowych sektorach[76]. Ustawa w znowelizowanym brzmieniu znacząco zwiększa liczbę podmiotów objętych KSC – z około 400 (jakich dotyczyła ustawa z 2018 r.) do szacunkowo ponad 10 000 podmiotów, w tym wielu jednostek sektora publicznego. Nowe przepisy mają skuteczniej chronić obywateli, firmy i instytucje przed rosnącą liczbą cyberataków oraz wzmocnić odporność państwa na zagrożenia cyfrowe. W nowelizacji przewidziano także utworzenie nowych struktur i mechanizmów (np. Krajowy Plan Reagowania na Incydenty Cybernetyczne, wzmocnienie roli CSIRT) oraz doprecyzowano zasady nadzoru i egzekwowania przepisów.

Ustawa rozszerza katalog sektorów i podmiotów objętych KSC. Obok dotychczasowych sektorów (energia, transport, zdrowie, bankowość, infrastruktura finansowa, zaopatrzenie w wodę, infrastruktura cyfrowa) dodano m.in. sektor ścieków, zarządzania ICT, przestrzeni kosmicznej, usług pocztowych, produkcji chemikaliów oraz produkcji żywności[77]. Najbardziej istotną zmianą jest jednak włączenie do krajowego systemu cyberbezpieczeństwa szeroko pojętej administracji publicznej (zarówno rządowej, jak i samorządowej) jako nowego sektora kluczowego. Oznacza to, że administracja publiczna – wcześniej w niewielkim stopniu regulowana przez KSC – stanie się jednym z filarów krajowego ekosystemu bezpieczeństwa cyfrowego[78].

Nowelizacja wprowadza również nowy podział kategorii podmiotów objętych ustawą: zamiast „operatorów usług kluczowych" i „dostawców usług cyfrowych" ustawa posługuje się kategoriami podmiotów kluczowych oraz podmiotów ważnych[79]. W kolejnych punktach omówiono szczegółowo te pojęcia, a także

[75] Zob. art. 8 ust. 1 w zw. z art. 8b ust. 1–2; art. 12 ust. 4–5; art. 69 ust. 2 pkt 3; art. 8 ust. 1 pkt 2 lit. e UKSC wprost odsyła do dyrektywy (UE) 2022/2555.
[76] Zob. art. 5a ust. 1–4; art. 8 ust. 1–2 UKSC.
[77] Zob. art. 5 ust. 1–2, w zw. z zał. nr 1 i 2; zał. nr 2 UKSC: sektor „usługi pocztowe", „produkcja, wytwarzanie i dystrybucja chemikaliów", „produkcja, przetwarzanie i dystrybucja żywności".
[78] Zob. art. 16d–16e [Rozdział 3b, wspólne wykonywanie obowiązków przez podmioty publiczne]; Zob. art. 8 ust. 3–4 [podmiot ważny będący podmiotem publicznym, wymogi z załącznika nr 4]; Zob. załącznik nr 2: „Podmioty publiczne" [wyliczenie JST i innych jednostek].
[79] Zob. art. 4 pkt 1–2; art. 5 ust. 1–2; art. 7l ust. 1–2 UKSC.

obowiązki i ryzyka, jakie z nowelizacji wynikają dla podmiotów publicznych zobowiązanych do przestrzegania ustawy.

### 2.3.2. Nowe kategorie podmiotów: podmioty kluczowe i podmioty ważne

Podmioty kluczowe i podmioty ważne to dwie nowe kategorie określające podmioty objęte ustawą, zróżnicowane ze względu na znaczenie danego podmiotu dla bezpieczeństwa państwa oraz sektor działalności. Podmioty te są wskazane odpowiednio w załączniku nr 1 (kluczowe) i nr 2 (ważne) projektowanej nowelizacji UKSC. Co do zasady, za *podmiot kluczowy lub ważny* uznaje się jednostkę organizacyjną (osobę prawną, fizyczną lub jednostkę nieposiadającą osobowości prawnej) prowadzącą główną działalność w jednym z sektorów wymienionych w ustawie oraz spełniającą kryterium wielkości (tzw. zasada size-cap – musi to być podmiot co najmniej średniej wielkości wg definicji unijnych)[80]. Zasada ta wyłącza automatycznie większość mikro i małych firm spod obowiązków, jednak nie dotyczy wielu podmiotów publicznych – co omówiono poniżej. Ustawa przewiduje też wyjątki: niezależnie od wielkości automatycznie objęci jako podmioty kluczowe są m.in. dostawcy usług DNS, kwalifikowani dostawcy usług zaufania (podpis elektroniczny) oraz dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa.

- Podmioty kluczowe (załącznik 1) obejmują większość sektorów krytycznych wymienionych w NIS 2, m.in.: energia, transport, ochrona zdrowia (np. szpitale), zaopatrzenie w wodę pitną, infrastruktura cyfrowa, zarządzanie usługami ICT, przestrzeń kosmiczna, a także – co nowe – administrację publiczną.
- Podmioty ważne (załącznik 2) obejmują sektory o nieco mniejszym krytycznym znaczeniu, jak: usługi pocztowe i kurierskie, gospodarka odpadami, produkcja żywności i chemikaliów, badania naukowe oraz szkolnictwo wyższe (uczelnie), a nawet niektóre elementy administracji lokalnej.

Nowelizacja wprowadza szczegółowy podział administracji publicznej między podmioty kluczowe a ważne, w zależności od szczebla i wielkości jednostki samorządu terytorialnego (JST)[81]. Centralne organy administracji rządowej (np. ministerstwa, urzędy centralne) oraz naczelne organy państwa zostały zaliczone do *podmiotów kluczowych publicznych*. Administracja samorządowa została ujęta w

[80] Zob. art. 5 ust. 1 pkt 1; art. 5 ust. 2 pkt 1–2 UKSC.

[81] Zob. art. 5 ust. 2 pkt 3–4 UKSC.

dwóch kategoriach: większe jednostki jako kluczowe, mniejsze jako ważne, co odzwierciedla kompromis wypracowany z samorządami. Przykładowo:

- Urzędy marszałkowskie (wojewódzkie) oraz jednostki i zakłady budżetowe województw – zaliczono do podmiotów kluczowych publicznych (z pewnymi wyłączeniami, np. szkół czy instytucji pomocy rodzinie).
- Starostwa powiatowe (powiaty) – wszystkie zostały uznane za *podmioty kluczowe publiczne*, niezależnie od wielkości.
- Urzędy gmin – status zależy od wielkości urzędu: gmina, która na 1 stycznia danego roku zatrudnia ≥50 pracowników, zostaje zaliczona do *podmiotów kluczowych* (jeśli <50 osób – nie jest kluczowa jako urząd). Mniejsze urzędy gmin nie spełniające kryterium 50 etatów nie wchodzą do kategorii kluczowych – jednak podlegają one przepisom jako *podmioty ważne* lub poprzez jednostki organizacyjne (patrz niżej).
- Jednostki organizacyjne gmin, powiatów i województw (posiadające osobowość prawną lub nie) takie jak samorządowe instytucje kultury, samorządowe zakłady budżetowe, samorządowe jednostki budżetowe, spółki komunalne realizujące zadania użyteczności publicznej – zostały zakwalifikowane do kategorii *podmiotów ważnych będących podmiotami publicznymi*. Oznacza to, że np. gminne muzea, biblioteki, domy kultury, przedszkola, szkoły, ośrodki pomocy społecznej oraz spółki komunalne (np. wodociągi, komunikacja miejska) będą uznane za podmioty ważne. Dzięki temu niemal cała administracja lokalna oraz jej jednostki zostają objęte systemem KSC, przy czym zróżnicowano poziom obowiązków i nadzoru (patrz pkt 5–7) w zależności od kategorii podmiotu.

**Podsumowując:**

Nowelizacja obejmuje swoim zakresem prawie wszystkie jednostki sektora publicznego. Administracja rządowa i większe samorządy traktowane są jako podmioty kluczowe, natomiast pomniejsze jednostki samorządowe i instytucje lokalne – jako podmioty ważne. Dla każdej z tych kategorii ustawa określa katalog obowiązków, zaś dla organów nadzoru – zakres uprawnień kontrolnych (szerszy wobec podmiotów kluczowych, ograniczony w przypadku ważnych). W rezultacie np. szpitale publiczne, urzędy centralne, urzędy marszałkowskie, powiaty i większe gminy znajdą się wśród podmiotów kluczowych, natomiast mniejsze gminy (urzędy <50 etatów), szkoły, instytucje kultury, spółki komunalne – wśród podmiotów ważnych. Każdy z tych podmiotów będzie musiał spełnić określone ustawą wymagania z zakresu cyberbezpieczeństwa.

### 2.3.3. Obowiązki ogólne podmiotów objętych ustawą

Nowelizacja nakłada na *podmioty kluczowe* i *podmioty ważne* szereg obowiązków, mających na celu zapewnienie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych. W praktyce oznacza to konieczność wdrożenia kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz procedur zarządzania ryzykiem w cyberbezpieczeństwie[82]. Ustawa (w art. 8) opisuje wymagania dla systemu bezpieczeństwa informacji, które w dużej mierze odpowiadają standardom znanym z norm ISO/IEC 27001 i wytycznych NIS 2. Do kluczowych ogólnych obowiązków należą m.in.:

- **Analiza ryzyka i wdrożenie środków bezpieczeństwa:** Podmiot musi regularnie identyfikować ryzyka dla swoich systemów informacyjnych i wdrażać adekwatne środki techniczne oraz organizacyjne, proporcjonalne do oszacowanego ryzyka (wymóg art. 8 ust. 1 pkt 2 KSC). Należy stosować rozwiązania zapobiegające incydentom oraz ograniczające wpływ incydentów na ciągłość działania usług (art. 8 ust. 1 pkt 5). Przykładowo, szpital jako podmiot kluczowy w sektorze zdrowia powinien zidentyfikować zagrożenia (np. atak ransomware na system rejestracji pacjentów) i zastosować adekwatne zabezpieczenia (kopie zapasowe danych, segmentacja sieci, aktualizacje systemów itp.), aby zminimalizować skutki potencjalnego ataku.
- **Organizacja bezpieczeństwa i zasoby:** Podmioty kluczowe muszą posiadać wyodrębnione struktury ds. cyberbezpieczeństwa lub dedykowane osoby odpowiedzialne za to zadanie[83]. Powinny ustanowić wewnętrzne procedury i polityki bezpieczeństwa informacji, określające m.in. zarządzanie dostępami, bezpieczną eksploatację systemów, reagowanie na incydenty oraz utrzymanie ciągłości działania (disaster recovery)[84]. W sektorze publicznym często oznacza to wyznaczenie np. Administratora Bezpieczeństwa Informacji / Inspektora Bezpieczeństwa Teleinformatycznego lub analogicznej funkcji oraz utworzenie zespołu odpowiedzialnego za cyberbezpieczeństwo urzędu.
- **Szkolenia i świadomość:** Ustawa wymaga zapewnienia personelowi odpowiednich szkoleń i budowania kultury bezpieczeństwa[85]. Pracownicy

[82] Zob. art. 8 ust. 1 pkt 1–3 UKSC.
[83] Zob. art. 8 ust. 1 pkt 2 lit. a–d UKSC.
[84] Zob. art. 8 ust. 1 pkt 2 lit. F UKSC.
[85] Zob. art. 8 ust. 1 pkt 2 lit. i–j UKSC.

podmiotów kluczowych i ważnych powinni być świadomi polityk bezpieczeństwa, zasad ochrony informacji oraz procedur zgłaszania incydentów. Np. urząd gminy (podmiot kluczowy publiczny, jeśli >50 pracowników) musi przeszkolić kadrę z rozpoznawania ataków (phishing, malware) i postępowania w razie incydentu[86].

- **Współpraca z właściwymi organami:** Każdy podmiot kluczowy i ważny ma obowiązek współdziałać z organami odpowiedzialnymi za cyberbezpieczeństwo – m.in. udzielać na żądanie informacji i dostępu do dokumentów potrzebnych do oceny spełniania wymogów[87]. W praktyce organ nadzorczy (np. minister cyfryzacji lub właściwy minister branżowy) może zażądać przedstawienia dokumentacji SZBI, raportów z audytów, polityk bezpieczeństwa itp., a podmiot ma prawny obowiązek je udostępnić.

Warto podkreślić, że przepisy nowelizacji nie uchylają równoległych obowiązków wynikających z innych aktów prawnych dotyczących bezpieczeństwa informacji w sektorze publicznym. Przykładowo stopnie alarmowe CRP nakładane na podstawie ustawy antyterrorystycznej czy wymogi Krajowych Ram Interoperacyjności (KRI) nadal obowiązują jednostki administracji, o ile znajdują zastosowanie. Ustawa KSC dodaje więc nowy, jednolity zestaw wymagań, a w razie pokrywania się kilku reżimów – należy stosować surowsze lub specyficzne zasady wynikające z KSC, szczególnie jeśli dana jednostka jest zakwalifikowana jako podmiot publiczny sektorowy (reguła kolizyjna z nowelizacji: gdy podmiot spełnia kryteria kilku kategorii, w tym kategorii publicznej, stosuje wymogi przypisane dla kategorii podmiotu publicznego).

### 2.3.4. System Zarządzania Bezpieczeństwem Informacji (SZBI) – szczegółowe wymagania

System Zarządzania Bezpieczeństwem Informacji (SZBI) to fundamentalny element, który każdy podmiot kluczowy oraz ważny musi ustanowić i utrzymywać zgodnie z art. 8 ustawy[88]. SZBI obejmuje zbiór procedur, polityk, procesów i zasobów służących utrzymaniu cyberbezpieczeństwa organizacji. Nowelizacja precyzuje wymogi SZBI, które pokrywają cały cykl zarządzania bezpieczeństwem – od zapobiegania, przez wykrywanie i reagowanie, po przywracanie ciągłości

[86] Zob. art. 8d ust. 1 pkt 4 UKSC.

[87] Zob. art. 42, 52 oraz np. art. 15 ust. 1a-1c w zakresie obowiązku przekazania raportu z audytu.

[88] Zob. art. 8 ust. 1 pkt 1–2 oraz art. 8 ust. 3 (dla podmiotów publicznych).

działania po incydentach. Poniżej wyszczególniono główne składowe SZBI wymagane przez ustawę, wraz z przykładami praktycznymi dla podmiotów publicznych:

- **Polityka bezpieczeństwa informacji**
  - Podmiot musi posiadać formalną politykę lub zestaw polityk bezpieczeństwa, zatwierdzonych przez kierownictwo.
  - Dokumenty te powinny określać cele bezpieczeństwa, role i obowiązki personelu, procedury ochrony danych i systemów, a także zgodność z przepisami.
  - Np. w urzędzie miasta polityka bezpieczeństwa będzie regulować zasady dostępu do systemów ePUAP, obsługi korespondencji elektronicznej, korzystania z nośników USB, szyfrowania dokumentów niejawnych itp.
- **Analiza ryzyka i planowanie zabezpieczeń**
  - SZBI musi zawierać proces ciągłego szacowania ryzyka (art. 8 ust. 1 pkt 2) – identyfikowania zagrożeń i podatności, oceny skutków potencjalnych incydentów oraz określania na tej podstawie środków zaradczych.
  - Ustawa wymaga, by wdrożone środki techniczne i organizacyjne były odpowiednie i proporcjonalne do zidentyfikowanych ryzyk.
  - Przykładowo szpital powiatowy (podmiot kluczowy) powinien przeprowadzić analizę ryzyka dla systemu HIS (Hospital Information System) i na podstawie jej wyników wdrożyć mechanizmy zabezpieczające (np. segmentację sieci szpitalnej, system wykrywania włamań IDS, silne uwierzytelnianie dla dostępu do danych medycznych).
- **Zarządzanie dostępem i tożsamością**
  - W SZBI należy uregulować nadawanie, modyfikację i odbieranie uprawnień użytkowników systemów, zasadę minimalnych uprawnień, stosowanie silnych haseł lub uwierzytelniania wieloskładnikowego.
  - Jednostki publiczne często wykorzystują systemy kadrowo-płacowe lub rejestry mieszkańców – dostęp do nich musi być ograniczony do upoważnionych osób, a każde konto użytkownika zarządzane wg procedury (np. w starostwie konto pracownika jest niezwłocznie usuwane lub blokowane po rozwiązaniu stosunku pracy).

- **Bezpieczeństwo infrastruktury teleinformatycznej**
    - Ustawa nakłada obowiązek wdrożenia środków zapobiegawczych przed incydentami i ograniczających ich skutki (art. 8 ust. 1 pkt 5) – dotyczy to ochrony sieci, serwerów, stacji roboczych, urządzeń mobilnych etc.
    - W ramach SZBI powinny funkcjonować rozwiązania takie jak: zapory sieciowe (firewalle), systemy antywirusowe i EDR, szyfrowanie komunikacji i danych wrażliwych, regularne aktualizacje i łatki bezpieczeństwa, redundancja krytycznych elementów infrastruktury.
    - Np. urząd marszałkowski jako podmiot kluczowy publiczny musi zapewnić odpowiednio zabezpieczone centrum danych dla swoich systemów (klimatyzowane pomieszczenia serwerowe z kontrolą dostępu, zasilanie awaryjne UPS, kopie zapasowe baz danych na wypadek awarii lub ataku szyfrującego).
- **Monitorowanie, detekcja i reagowanie**
    - SZBI musi obejmować mechanizmy ciągłego monitorowania zdarzeń w systemach oraz wykrywania incydentów bezpieczeństwa.
    - Powinny być wdrożone procedury obsługi incydentów (tzw. IR – Incident Response), określające kroki postępowania w razie wykrycia incydentu, odnotowywania go, eskalacji, usuwania skutków, aż po raportowanie do właściwych organów (zgodnie z ustawą – do CSIRT, patrz pkt 5).
    - Przykładowo, w uczelni będącej podmiotem ważnym należy ustanowić zespół reagowania na incydenty (lub wyznaczyć administratorów IT do tej roli), którzy w przypadku np. wykrycia ataku phishingowego na konto e-mail pracownika podejmą natychmiastowe działania: zablokują zagrożone konto, przeanalizują logi, zgłoszą incydent dalej zgodnie z procedurą.
- **Ciągłość działania i odtwarzanie po awarii**
    - Ustawa wymusza przygotowanie organizacji na sytuacje kryzysowe – plan utrzymania ciągłości działania (BCP) oraz plan odtwarzania po awarii (DRP) powinny być częścią SZBI.
    - Podmiot musi zapewnić, że kluczowe usługi będą mogły być kontynuowane lub szybko przywrócone w razie poważnego incydentu (np. awarii systemu, ataku ransomware).
    - Dla instytucji publicznej, takiej jak duże miasto (urząd gminy >50 osób), oznacza to konieczność posiadania zapasowych serwerów lub

chmury na wypadek utraty systemu dziedzinowego (np. ewidencji ludności), regularnego tworzenia kopii zapasowych i testowania procedur odtwarzania danych.

- **Bezpieczeństwo łańcucha dostaw ICT**
  - Bardzo istotnym nowym elementem jest obowiązek badania bezpieczeństwa łańcucha dostaw na etapie zamówień infrastruktury IT. W praktyce oznacza to, że publiczne jednostki objęte KSC, realizując zamówienia publiczne na sprzęt, oprogramowanie czy usługi IT, muszą brać pod uwagę kryteria cyberbezpieczeństwa dostawców i produktów.
  - Podmiot kluczowy powinien oceniać swoich dostawców pod kątem ryzyka (np. wymagać certyfikatów bezpieczeństwa, oceny zgodności z normami) oraz unikać komponentów, które mogą stanowić zagrożenie (patrz też punkt 8 dotyczący dostawców wysokiego ryzyka).
  - Ten wymóg integruje ustawę o KSC z procesem zamówień publicznych – organizacja zamawiająca przed wyborem oferty powinna dokonać analizy ryzyka dostawcy i produktu.
  - Przykład: duże miasto planujące zakup systemu miejskiego monitoringu musi na etapie postępowania ocenić, czy oferowany sprzęt i oprogramowanie spełniają standardy bezpieczeństwa i nie pochodzą od producentów uznanych za stwarzających zagrożenie.
  - Wymóg analizy bezpieczeństwa dostaw znajduje potwierdzenie w art. 8 ust. 1 pkt 6 ustawy, który obliguje do uwzględnienia bezpieczeństwa dostawców usług i produktów ICT w ramach SZBI.
- **Audyt i testowanie zabezpieczeń**
  - Zgodnie z nowelizacją, podmioty kluczowe muszą przeprowadzać regularne audyty bezpieczeństwa swoich systemów, wykonywane przez niezależne podmioty trzecie.
  - Celem jest okresowa weryfikacja zgodności z wymaganiami ustawy i skuteczności zastosowanych środków.
  - Ponadto dobre praktyki (i pośrednio wymagania ustawy) wskazują na potrzebę testowania zabezpieczeń, np. poprzez testy penetracyjne systemów czy symulacje ataków, zwłaszcza w największych podmiotach kluczowych.
  - U podmiotów ważnych obowiązek audytu zewnętrznego może być złagodzony, lecz w praktyce również one powinny dokonywać

samooceny i audytów wewnętrznych, by wykazać spełnienie ustawowych wymogów.

Wdrożenie powyższych elementów SZBI stanowi znaczne wyzwanie organizacyjne i finansowe, zwłaszcza dla jednostek sektora publicznego, które dotychczas nie musiały spełniać rygorystycznych standardów cyberbezpieczeństwa. Ryzykiem po stronie podmiotów publicznych jest tu m.in. konieczność poniesienia dodatkowych kosztów (np. na zatrudnienie specjalistów IT, zakup systemów bezpieczeństwa, audyty) oraz dostosowania struktur organizacyjnych. Należy jednak podkreślić, że niewdrożenie SZBI i zaniedbanie obowiązków będzie groziło dotkliwymi sankcjami (o czym w punkcie 7), a także zwiększa ryzyko wystąpienia poważnego incydentu z konsekwencjami dla ciągłości działania danej jednostki (np. sparaliżowanie pracy urzędu przez atak).

### 2.3.5. Zgłaszanie i obsługa incydentów cyberbezpieczeństwa

Nowelizacja szczegółowo reguluje obowiązki podmiotów kluczowych i ważnych w zakresie obsługi incydentów oraz ich zgłaszania właściwym organom. Każdy podmiot objęty ustawą musi posiadać procedury pozwalające na identyfikację incydentu, jego kategoryzację (ustalenie istotności) i skuteczną reakcję, a także zapewnić terminowe przekazywanie informacji o incydentach do odpowiednich CSIRT. Ustawa definiuje różne poziomy incydentów, z których kluczowe są incydent poważny oraz incydent krytyczny (najpoważniejszy).

Zgodnie z art. 11 ustawy, *podmiot kluczowy* (oraz analogicznie podmiot ważny) ma obowiązek zgłaszania incydentów poważnych do właściwego zespołu CSIRT (sektorowego lub CSIRT NASK/MON/GOV) w ustalonych terminach. Procedura meldowania incydentu jest wieloetapowa:

| **Wczesne ostrzeżenie** |
| --- |
| Niezwłocznie, nie później niż w ciągu 24 godzin od wykrycia incydentu poważnego, podmiot przekazuje do CSIRT wstępne zgłoszenie (tzw. early warning) zawierające podstawowe informacje o zdarzeniu. Celem jest szybkie powiadomienie organów, że doszło do poważnego incydentu, co umożliwia np. ostrzeżenie innych podmiotów oraz wsparcie reagowania. Przykład: Uniwersytet (podmiot ważny) wykrył groźny atak ransomware szyfrujący serwery – w ciągu 24h powinien wysłać do CSIRT GOV lub CSIRT NASK zgłoszenie zawierające informacje, że incydent nastąpił, jaki typ (np. ransomware), jaki ma potencjalny wpływ (np. wstrzymanie działania dziekanatów). |
| **Właściwe zgłoszenie incydentu (raport wstępny)** |

| |
|---|
| W ciągu maksymalnie 72 godzin od wykrycia incydentu poważnego podmiot musi przekazać do CSIRT bardziej szczegółowe informacje o incydencie. Zgłoszenie to (art. 11 ust. 1 pkt 4a) zawiera zapewne opis incydentu, wstępne ustalenia co do przyczyny, podjęte środki zaradcze i skalę wpływu incydentu. Kontynuując przykład uczelni: do 72h od wykrycia ataku ransomware uniwersytet uzupełnia wcześniejsze zgłoszenie o szczegóły – które serwery zostały zaszyfrowane, czy doszło do wycieku danych, jaki wariant malware'u, jakie kroki podjęto (odłączenie sieci, informowanie użytkowników, itp.). |
| **Sprawozdanie z obsługi incydentu (raport końcowy)** |
| Po zakończeniu obsługi incydentu poważnego, podmiot sporządza szczegółowy raport końcowy, który również przekazuje do CSIRT (art. 11 ust. 1 pkt 4b–4c). Raport ten powinien podsumowywać przebieg incydentu, zastosowane środki naprawcze, czas trwania zakłóceń, skalę strat lub szkód oraz wnioski na przyszłość. Ustawa nie wskazuje wprost terminu na sprawozdanie końcowe, ale zgodnie z dyrektywą NIS 2 należy to zrobić nie później niż miesiąc od zgłoszenia incydentu (lub na żądanie organu wcześniej). W naszym przykładzie uczelnia po opanowaniu skutków ataku ransomware (np. po 2 tygodniach) sporządza raport końcowy, w którym opisuje, że odtworzono dane z backupu, przywrócono działanie serwerów po 5 dniach, szkody finansowe były minimalne, natomiast podjęto decyzję o wdrożeniu dodatkowego szkolenia dla pracowników i segmentacji sieci na przyszłość. |

Należy zaznaczyć, że powyższe obowiązki dotyczą incydentów poważnych (spełniających określone kryteria istotności wpływu). Ustawa (dostosowując się do NIS 2) wprowadziła progi lub definicje pozwalające ocenić, czy dane zdarzenie jest incydentem poważnym[89]. Mniejsze incydenty (tzw. zwykłe) być może nie podlegają obowiązkowemu raportowaniu, ale praktyką dobrą jest rejestrowanie wszystkich incydentów wewnętrznie. Natomiast incydenty krytyczne – tj. takie, które mogą zagrozić bezpieczeństwu publicznemu lub porządkowi publicznemu – podlegają szczególnym procedurom[90]. W przypadku incydentu krytycznego Minister właściwy ds. informatyzacji może nawet wydać tzw. polecenie zabezpieczające nakazujące podjęcie określonych działań natychmiastowych przez zaatakowany podmiot[91]. Przykładem incydentu krytycznego mógłby być skoordynowany

[89] Zob. art. 11 ust. 1 pkt 3–4a; ust. 4–5 UKSC.

[90] Zob. art. 2 pkt 6–7 UKSC.

[91] Zob. art. 67g UKSC.

cyberatak, który unieruchamia kluczowe systemy wielu szpitali jednocześnie lub atak na infrastrukturę energetyczną o skutkach odczuwalnych społecznie – wówczas reakcja może być koordynowana na szczeblu centralnym.

Poza obowiązkiem notyfikacji na zewnątrz, podmioty kluczowe i ważne muszą obsługiwać incydenty wewnętrznie zgodnie z procedurami SZBI[92]. Oznacza to ustanowienie wewnętrznych struktur (np. wewnętrzny zespół reagowania lub wyznaczenie osoby kontaktowej ds. incydentów) oraz procesów (rejestrowanie incydentu, analiza przyczyn, eliminacja zagrożenia, odtworzenie systemów, informowanie kierownictwa i interesariuszy, wyciągnięcie wniosków). Ustawa z 2018 r. już wcześniej wymagała od podmiotów publicznych wyznaczenia *punktu kontaktowego ds. cyberbezpieczeństwa* – nowelizacja te kwestie uszczegóławia i rozszerza[93]. Teraz np. każda jednostka JST objęta ustawą musi mieć oficjalnie wyznaczony punkt kontaktowy do obsługi incydentów (może to być np. inspektor IT albo osoba pełniąca funkcję podobną do ABI/Inspektora Ochrony Danych, lecz ds. cyberbezpieczeństwa). Dane kontaktowe tej osoby są zgłaszane do krajowego systemu (do właściwego CSIRT), co zapewnia sprawną komunikację, np. gdy CSIRT wysyła ostrzeżenie o nowej podatności – trafi ono do odpowiedzialnego specjalisty w jednostce[94].

Podmioty kluczowe i ważne zobowiązane są do współdziałania z zespołami CSIRT w trakcie incydentów. W praktyce mogą korzystać z pomocy CSIRT sektorowego lub krajowego w analizie zdarzenia, usunięciu skutków ataku czy w identyfikacji sprawcy. Ustawa wzmacnia uprawnienia CSIRT – np. CSIRT NASK został wyznaczony krajowym koordynatorem ds. skoordynowanego ujawniania podatności (koordynuje proces informowania o lukach w oprogramowaniu). Z punktu widzenia jednostki publicznej (np. szpitala), ważne jest, by w razie wykrycia krytycznej podatności w używanym systemie (np. systemie radiologicznym) skontaktować się z CSIRT, który może pomóc ostrzec producenta lub inne placówki używające tego samego systemu.

---

[92] Zob. art. 11 ust. 1 pkt 1–2 i 4–5 UKSC, które nakazują zapewnić obsługę incydentu, udostępniać informacje CSIRT i współdziałać przy obsłudze, a także raportować incydenty poważne w określonych terminach.

[93] Zob. art. 9 ust. 2–4 UKSC, który przewiduje wyznaczanie co najmniej jednej osoby odpowiedzialnej za utrzymywanie kontaktów z innymi podmiotami, w szczególności dla podmiotów publicznych.

[94] Zob. art. 7 ust. 5 pkt 4–6 UKSC.

Podsumowując, niezastosowanie się do obowiązków zgłaszania incydentów może skutkować sankcjami finansowymi, a także osłabić zdolność reagowania na poziomie krajowym. Dla organizacji zamawiających (podmiotów publicznych) oznacza to konieczność posiadania sprawnego systemu detekcji i raportowania incydentów, co bywa wyzwaniem np. dla małych instytucji kultury czy gmin – dlatego nowelizacja przewiduje możliwość wsparcia tych zadań w modelu wspólnym.

### 2.3.6. Nadzór i kontrola przestrzegania przepisów

Ustawa w nowym brzmieniu określa mechanizmy nadzoru nad podmiotami objętymi KSC oraz procedury kontroli spełniania przez nie wymogów[95]. Organy właściwe do spraw cyberbezpieczeństwa (np. minister cyfryzacji dla administracji publicznej, właściwi ministrowie dla sektorów, sektorowe organy regulacyjne) otrzymują uprawnienia, aby weryfikować, czy podmioty kluczowe i ważne wykonują obowiązki nałożone ustawą. Z punktu widzenia podmiotów publicznych (zamawiających) oznacza to możliwość planowych lub doraźnych kontroli, żądania przedstawienia dokumentów, a w razie stwierdzenia uchybień – wydawania zaleceń i decyzji naprawczych, a nawet nakładania kar[96].

Dla podmiotów kluczowych ustawa przewiduje, że kontrola spełniania wymagań może mieć charakter uprzedni (proaktywny) – tzn. organ nadzorczy może z urzędu, bez czekania na incydent, skontrolować dany podmiot[97]. Może to przybrać formę audytu zgodności: np. Minister Cyfryzacji może zarządzić sprawdzenie wybranego urzędu marszałkowskiego pod kątem wdrożenia SZBI, nawet jeśli nie doszło tam do żadnego incydentu. Ponadto kontrola może być następcza – czyli wszczynana po wystąpieniu incydentu lub w związku z podejrzeniem naruszenia przepisów[98]. W przypadku podmiotów ważnych nowelizacja ogranicza uprawnienia organów nadzoru: kontrola w ich przypadku może mieć charakter wyłącznie następczy (po incydencie lub zgłoszeniu nieprawidłowości). Oznacza to, że np. gminna biblioteka jako podmiot ważny

[95] Zob. art. 53 ust. 2–3 UKSC: określa nadzór nad podmiotami kluczowymi/ważnymi, w tym kontrole (także doraźne), żądanie audytu, żądanie informacji i dowodów realizacji wymogów; zob. art. 42 ust. 1 UKSC: zadania organów właściwych, m.in. bieżąca analiza podmiotów, wpisy do wykazu, wydawanie decyzji, monitorowanie stosowania ustawy, kontrole.

[96] Zob. art. 53 ust. 2–5 UKSC.

[97] art. 53 ust. 3 pkt 1 UKSC, który wprost stanowi, że nadzór nad podmiotami kluczowymi ma charakter prewencyjny i następczy.

[98] Zob. art. 53 ust. 2 pkt 1–5 UKSC.

publiczny nie będzie raczej przedmiotem rutynowych audytów z ramienia państwa, lecz jeśli dojdzie tam do poważnego incydentu lub skargi, organ może przeprowadzić kontrolę post factum.

W toku kontroli organ ma prawo żądać od kontrolowanego podmiotu wszelkich informacji, dokumentów i danych niezbędnych do oceny zgodności z ustawą[99]. Może również dokonać oględzin systemów, zażądać dostępu do infrastruktury teleinformatycznej, przeprowadzić wywiady z personelem odpowiedzialnym za IT itp[100]. Ustawa przewiduje, że kontrola odbywa się na podstawie upoważnienia i powinna być wcześniej zapowiedziana, jednak w sytuacjach szczególnych (np. incydenty krytyczne) może następować tryb doraźny[101]. Dla podmiotów publicznych oznacza to konieczność prowadzenia dokumentacji potwierdzającej realizację obowiązków – np. raportów z analiz ryzyka, planów szkoleń, rejestrów incydentów, sprawozdań z audytów – aby móc je okazać kontrolerom.

Jeżeli w wyniku kontroli stwierdzone zostaną naruszenia ustawy, organ właściwy może wydać zalecenia pokontrolne[102], a w poważniejszych przypadkach – decyzje administracyjne nakazujące podjęcie określonych działań w celu usunięcia uchybień. Na przykład, jeśli kontrola wykaże, że powiat nie dokonał wymaganego wpisu do wykazu podmiotów kluczowych lub nie opracował analizy ryzyka, organ może nakazać uzupełnienie tych obowiązków w wyznaczonym terminie[103]. Niewykonanie zaleceń może skutkować nałożeniem kary pieniężnej. W skrajnych sytuacjach, gdy zaniedbania podmiotu stanowią bezpośrednie zagrożenie dla bezpieczeństwa państwa lub życia ludzi, organy nadzoru mają obowiązek zdecydowanie reagować – ustawa umożliwia nałożenie bardzo wysokich kar oraz zastosowanie innych środków nadzorczych (np. zawiadomienie organów ścigania, jeśli doszło do naruszenia prawa)[104].

Każdy podmiot kluczowy i ważny ma być ujęty w wykazie podmiotów prowadzonym przez właściwy organ. Nowelizacja określa procedurę wpisu do rejestru (art. 7) – w wielu przypadkach podmioty dokonują samoidentyfikacji i

[99] art. 53c ust. 1 oraz ust. 4 UKSC.

[100] Zob. art. 55 pkt 2, 5–6 UKSC.

[101] Zob. art. 58 ust. 2 pkt 3 oraz art. 59c ust. 1 oraz ust. 4–5 UKSC.

[102] art. 59 UKSC.

[103] art. 53e w zw. z art. 53 ust. 9 UKSC

[104] Zob. art. 73 – kary pieniężne za naruszenia, w tym progi dla podmiotów kluczowych i ważnych oraz do 100 000 000 zł przy najpoważniejszych zagrożeniach.

samodzielnego zgłoszenia do wykazu[105]. Dla podmiotów publicznych kluczowych (jak urzędy centralne, wojewódzkie, powiatowe) przewidziano tryb odgórny: minister ds. informatyzacji wpisuje je z urzędu do wykazu i zawiadamia o tym wpisie[106]. Wpis do rejestru formalnie oznacza objęcie danej jednostki reżimem KSC – od tego momentu staje się ona adresatem obowiązków i potencjalnym celem kontroli[107]. Organy nadzoru mogą zatem sprawdzać, czy wszystkie kwalifikujące się podmioty zostały ujęte w wykazie[108].

### 2.3.7. Odpowiedzialność i kary za naruszenia przepisów

Jednym z najbardziej dotkliwych dla podmiotów elementów nowelizacji jest zaostrzenie odpowiedzialności za nieprzestrzeganie ustawy – zarówno odpowiedzialności finansowej samych podmiotów, jak i osobistej kadry zarządzającej. Ustawodawca, implementując NIS 2, przewidział surowe kary administracyjne, które mają zdyscyplinować podmioty kluczowe i ważne oraz uczynić cyberbezpieczeństwo realnym priorytetem w ich działaniach. Poniżej przedstawiono najważniejsze rodzaje sankcji:

- **Kary pieniężne dla podmiotów (administracyjne)**
    - Zgodnie z projektem, podmiot kluczowy może zostać ukarany karą finansową do 10 000 000 euro lub 2% przychodu rocznego z poprzedniego roku obrotowego – w zależności, która kwota jest wyższa. Ustawodawca ustanawia przy tym minimalny poziom kary: nie może być ona niższa niż 20 tys. zł[109].
    - Sankcje tej rangi będą grozić za poważne naruszenia obowiązków z ustawy (np. brak wdrożenia środków bezpieczeństwa, niezgłoszenie incydentu, uporczywe ignorowanie zaleceń pokontrolnych).
    - Co istotne, nowelizacja przewiduje szczególne, jeszcze wyższe kary w sytuacjach zagrażających bezpieczeństwu państwa: jeśli podmiot (kluczowy lub ważny) naruszy przepisy w sposób powodujący bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla

[105] Zob. art. 7d ust. 1 [wpis z chwilą złożenia wniosku]; art. 7j ust. 1 [wpis z urzędu, gdy brak wniosku w terminie].

[106] Zob. art. 7a ust. 2 pkt 3 [minister informatyzacji wpisuje dane z urzędu]; art. 7b ust. 1–2 [zawiadomienie o wpisie, wezwanie do uzupełnienia danych].

[107] Zob. art. 4 pkt 1–2 [KSC obejmuje podmioty kluczowe i ważne]; art. 42 ust. 1 [monitorowanie stosowania ustawy, kontrole].

[108] Zob. art. 42 ust. 1 pkt 1–3.

[109] Zob. art. 73 ust. 3 [widełki dla podmiotu kluczowego; próg minimalny 20 000 zł].

obronności, bezpieczeństwa narodowego, porządku publicznego lub życia i zdrowia ludzi, organ obowiązkowo nałoży karę do 100 mln zł[110].

- Analogiczna maksymalna kara (do 100 mln zł) grozi podmiotowi kluczowemu, którego naruszenie wywołało ryzyko wyrządzenia poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług. W poprzednim brzmieniu ustawy takie kary (do 1 000 000 zł dla OUK) istniały, lecz wymierzane były za uporczywe naruszanie ustawy – nowelizacja usuwa wymóg uporczywości, co oznacza, że jednorazowe zaniedbanie o dużej szkodliwości może skutkować natychmiast bardzo wysoką karą[111].

- **Kary dla kadry kierowniczej (odpowiedzialność osobista)**
  - Nowelizacja wprowadza przełomową regulację nakładającą odpowiedzialność finansową na osoby zarządzające podmiotem kluczowym lub ważnym. Menedżerowie (np. dyrektor szpitala, wójt, burmistrz, prezes spółki komunalnej) mogą zostać ukarani grzywną administracyjną do 300% ich miesięcznego wynagrodzenia, niezależnie od kar nakładanych na sam podmiot. Kara dla osoby fizycznej ma być liczona wg zasad jak ekwiwalent za urlop (czyli od pełnego wynagrodzenia)[112].
  - Co ważne, w najnowszej wersji projektu złagodzono ten wymiar dla kierowników podmiotów publicznych – dla nich maksymalna kara ma wynosić 100% wynagrodzenia[113]. Jednak jeżeli dany podmiot publiczny jest jednocześnie objęty jako kluczowy w sektorze innym niż administracja (np. jest gminą ale też operatorem infrastruktury cyfrowej), to wobec jego kierownika stosuje się wyższy próg 300%. Ta personalna odpowiedzialność oznacza, że np. prezydent miasta, które nie dopełni obowiązków KSC, może z własnej kieszeni zapłacić karę do wysokości miesięcznej pensji. Ma to motywować najwyższe

[110] Zob. art. 73 ust. 5 pkt 1 [bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, porządku publicznego lub życia i zdrowia ludzi – kara do 100 mln zł].
[111] Zob. art. 73 ust. 5 pkt 2
[112] Zob. art. 73 ust. 1–3, ust. 4 [można ukarać kierownika niezależnie od kary dla podmiotu; maks. 300% wynagrodzenia liczonego jak ekwiwalent urlopowy].
[113] Zob. art. 73 ust. 5 [limit 100% dla kierownika podmiotu publicznego; wyjątek sektorowy odsyła do ust. 4 = 300%]

kierownictwo do nadania priorytetu sprawom cyberbezpieczeństwa w zarządzaniu jednostką.

- **Kary okresowe (za opóźnienia)**
  - Jeżeli podmiot opóźnia się z wykonaniem nałożonych nań obowiązków (np. nie wdrożył środka zarządzonego decyzją organu w wyznaczonym terminie), organ nadzoru może nakładać kary pieniężne za każdy dzień opóźnienia[114].
  - Według projektu kara taka może wynosić od 500 zł do 100 000 zł za każdy dzień zwłoki. Jest to instrument dyscyplinujący – ma zmusić do niezwłocznego usunięcia uchybień. Przykład: jeśli uczelnia (podmiot ważny) otrzyma decyzję nakazującą w ciągu 30 dni przeprowadzić audyt bezpieczeństwa, a po upływie terminu nie dostosuje się, organ może naliczać np. 1000 zł za każdy kolejny dzień braku audytu, aż do wykonania obowiązku.
- **Relacja do kar za naruszenie ochrony danych osobowych**
  - Nowelizacja zawiera klauzulę zapobiegającą podwójnemu karaniu za ten sam czyn w kontekście RODO. Gdyby naruszenie przepisów KSC jednocześnie stanowiło naruszenie ochrony danych osobowych (np. wyciek danych osobowych w wyniku cyberincydentu) i Prezes UODO nałożył za to karę, wówczas organ ds. cyberbezpieczeństwa nie nakłada już drugiej kary, poprzestając na pouczeniu[115].
  - Ma to zapewnić proporcjonalność i spójność egzekwowania prawa – podmiot nie będzie płacił dwa razy za jedno zdarzenie (choć oczywiście może odpowiadać na dwóch podstawach, ale kara administracyjna będzie jedna).

Wymienione wyżej sankcje sprawiają, że ryzyko finansowe dla podmiotów publicznych znacznie rośnie. Dotąd wiele jednostek samorządowych mogło uważać kwestie cyberbezpieczeństwa za drugorzędne z braku bezpośrednich konsekwencji. Po wejściu nowelizacji w życie, np. średniej wielkości miasto (podmiot kluczowy) w skrajnym przypadku może zostać ukarane nawet do równowartości 10% swojego rocznego budżetu, co byłoby ogromnym obciążeniem. Kierownicy instytucji publicznych również muszą liczyć się z osobistymi konsekwencjami, co zapewne wpłynie na ich podejście – np. burmistrz

[114] art. 76b ust. 1–2 UKSC.

[115] Zob. art. 76c ust. 1 UKSC.

będzie dbał, by wyznaczone osoby realizowały obowiązki KSC, wiedząc że zaniedbanie może skutkować dla niego karą.

Należy przy tym zaznaczyć, że celem ustawodawcy nie jest fiskalne karanie jednostek, lecz wymuszenie compliance – stąd też kary zapewne będą nakładane po uprzednim wezwaniu do usunięcia naruszeń, a nie automatycznie. Nowelizacja pozostawia organom nadzoru pewną swobodę co do wysokości kar, uzależniając ją od okoliczności (stopnia winy, skali naruszenia, współpracy podmiotu z organem itp.). Niemniej jednak, świadomość grożących sankcji ma mobilizować podmioty publiczne do priorytetowego traktowania zagadnień cyberbezpieczeństwa.

### 2.3.8. Dostawcy wysokiego ryzyka – ograniczenia dla zamawiających

Jedną z najbardziej dyskutowanych zmian w nowelizacji KSC jest wprowadzenie koncepcji Dostawcy Wysokiego Ryzyka (DWR), określanej czasem jako *high-risk vendor*. Dla podmiotów publicznych (realizujących zamówienia publiczne) oznacza to konieczność zwrócenia szczególnej uwagi na pochodzenie i wiarygodność technologii, które kupują, a w skrajnym przypadku – obowiązek wycofania już używanych produktów od zakazanego dostawcy.

Zgodnie z projektowanymi przepisami, Minister Cyfryzacji będzie mógł decyzją administracyjną uznać danego dostawcę produktów lub usług ICT za dostawcę wysokiego ryzyka[116]. Decyzja taka może być podjęta z urzędu lub na wniosek Przewodniczącego Kolegium ds. Cyberbezpieczeństwa (którym jest Premier), po zasięgnięciu opinii Kolegium ds. Cyberbezpieczeństwa. Kryteria uznania za DWR nie są czysto techniczne – mają charakter oceny ryzyka z punktu widzenia bezpieczeństwa narodowego[117]. Bierze się pod uwagę m.in.: prawdopodobieństwo, że dany dostawca podlega wpływom obcego państwa, brak zaufania do przestrzegania standardów bezpieczeństwa, wcześniejsze incydenty z udziałem produktów dostawcy, a także znaczenie produktów dostawcy dla funkcjonowania kluczowych systemów. W praktyce chodzi głównie o dostawców z krajów autorytarnych, którzy mogliby zostać zmuszeni do współpracy z obcym wywiadem (najczęściej wskazuje się tutaj firmy chińskie lub rosyjskie[118]).

Jeśli Minister Cyfryzacji wyda decyzję uznającą firmę X za dostawcę wysokiego ryzyka, jej produkty i usługi nie będą mogły być wykorzystywane w

[116] Zob. art. 67b ust. 1 i ust. 15–19 UKSC.

[117] Zob. art. 67f ust. 1–3 UKSC.

[118] Osobnym zagadnieniem pozostaje oczywiście kwestia list sankcyjnych.

kluczowych systemach teleinformatycznych podmiotów KSC. Ustawa nakłada obowiązek wycofania produktów lub oprogramowania pochodzącego od takiego dostawcy z użytkowania przez podmioty kluczowe[119]. Ma to zapobiec sytuacji, w której newralgiczne systemy (np. sieci 5G telekomów, systemy SCADA w energetyce, ale też serwery w urzędach) zawierają „konia trojańskiego" w postaci podatnych urządzeń od niepewnego producenta. Co istotne, regulacja DWR obejmie również jednostki samorządu terytorialnego i ich systemy – uznany DWR może zmusić np. miasto do wymiany posiadanych elementów infrastruktury IT.

W praktyce nowelizacja wymusza na podmiotach publicznych staranniejszą weryfikację dostawców IT już na etapie przetargu. Zamawiający przed zakupem powinni sprawdzić, czy potencjalny wykonawca lub producent sprzętu nie figuruje (bądź nie jest bliski wpisania) na liście DWR. Prawdopodobnie powstanie oficjalny rejestr dostawców wysokiego ryzyka, publikowany przez Ministerstwo, aby podmioty wiedziały, kogo unikać. Co więcej, jak wspomniano w pkt 4, ustawa nakazuje badanie bezpieczeństwa łańcucha dostaw przy zamówieniach IT. Można się spodziewać, że wymagane będzie w SWZ/OPZ stawianie warunków dotyczących bezpieczeństwa (np. certyfikat Common Criteria dla urządzeń, brak podzespołów od określonych producentów).

Dla przykładu: Jeżeli w przyszłości producent popularnych kamer monitoringu zostanie uznany za DWR, to urząd miasta planujący rozbudowę sieci kamer będzie musiał odrzucić ofertę tego producenta z postępowania o udzielenie zamówienia. Jeśli zaś taki sprzęt już zainstalowano, miasto będzie zmuszone w określonym terminie go usunąć lub wymienić na inny – co generuje dodatkowe koszty, jednak z punktu widzenia państwa jest konieczne dla eliminacji słabych punktów w infrastrukturze.

Wprowadzenie krajowej listy DWR jest krokiem dalej niż wymogi NIS 2 (żaden inny kraj UE dotąd takich przepisów nie wdrożył). Może budzić to kontrowersje, m.in. z uwagi na możliwe zarzuty protekcjonizmu lub napięcia dyplomatyczne. Jednak polski rząd argumentuje, że Unia wymaga analizy ryzyka dostawcy, a Toolbox 5G (unijne zalecenia) dopuszcza ograniczanie udziału dostawców wysokiego ryzyka. W polskim kontekście przepisy te pojawiały się już we wcześniejszych projektach nowelizacji KSC, głównie w związku z bezpieczeństwem sieci 5G. Teraz przyjęto je w szerszym zastosowaniu. Dla podmiotów publicznych kluczowe jest śledzenie komunikatów rządowych –

[119] Zob. art. 67c ust. 1 pkt 1–2 UKSC.

decyzja uznająca konkretnego dostawcę za DWR będzie ogłaszana w Dzienniku Urzędowym ministra ds. informatyzacji i podlega publikacji (także będzie możliwość odwołania się przez dostawcę do sądu administracyjnego[120]).

### 2.3.9. Polecenia zabezpieczające – nadzwyczajne środki reagowania

Nowelizacja przywraca do ustawy mechanizm tzw. poleceń zabezpieczających, który istniał w pierwotnej ustawie KSC (choć nie był dotąd stosowany) i budził duże emocje. Polecenie zabezpieczające to specjalne, nadzwyczajne zarządzenie wydawane przez władze, nakazujące podmiotowi KSC wykonanie określonych działań lub zaniechanie działań w celu natychmiastowego zabezpieczenia cyberbezpieczeństwa. Zgodnie z nowelizacją, minister właściwy do spraw informatyzacji (obecnie Minister Cyfryzacji) będzie mógł wydać polecenie zabezpieczające w przypadku wystąpienia incydentu krytycznego, który może zagrozić bezpieczeństwu lub porządkowi publicznemu. Innymi słowy, gdy dojdzie do bardzo poważnego cyberataku, rząd zyskuje prawo wydania wiążących dyspozycji dla zaatakowanej instytucji (lub innych instytucji) w trybie alarmowym.

Polecenie zabezpieczające ma formę decyzji administracyjnej wydanej z urzędu, z rygorem natychmiastowej wykonalności. Ustawa precyzuje, że może ono obejmować np. nakaz wyłączenia określonego systemu lub jego części, odłączenia go od sieci, wprowadzenia określonych konfiguracji bezpieczeństwa, dokonania aktualizacji, uruchomienia zapasowych procedur, a także zakaz wykonywania określonych czynności (np. powstrzymanie się od udostępniania usług do czasu zabezpieczenia systemu). Przykładowo, jeśli doszłoby do rozległego ataku na systemy energetyczne, Minister mógłby wydać polecenie wyłączenia pewnych systemów sterowania aż do ich sprawdzenia, choć normalnie takie wyłączenie mogłoby np. spowodować przerwę w usługach – tu jednak priorytetem jest powstrzymanie rozprzestrzeniania się ataku.

Polecenie może być skierowane do podmiotów kluczowych lub ważnych, ale potencjalnie także do innych uczestników KSC, np. do operatorów infrastruktury internetowej czy dostawców usług kluczowych spoza sektora publicznego. Dla sektora publicznego oznacza to podporządkowanie się centralnie zarządzanym akcjom w cyberkryzysie – np. jeśli atak dotknie wiele urzędów, mogą one zbiorczo

[120] Zob. art. 67i ust. 1 [skarga do sądu administracyjnego w terminie 2 miesięcy od ogłoszenia decyzji]; art. 67b ust. 19 [brak wniosku o ponowne rozpatrzenie].

otrzymać polecenie odcięcia się od Internetu na pewien czas lub zmiany haseł w określony sposób.

Decyzja o wydaniu polecenia zabezpieczającego musi być skonsultowana z Kolegium ds. Cyberbezpieczeństwa (jego przewodniczącym jest Premier). Z racji, że jest to instrument mogący mocno ingerować w działania podmiotu (np. nakazać wyłączenie usługi publicznej), ustawa prawdopodobnie przewiduje szybki tryb odwoławczy do sądu administracyjnego. Jednak odwołanie nie wstrzymuje wykonania – polecenie jest wykonywane od razu, bo liczy się efekt natychmiastowy. W poprzednich dyskusjach wskazywano, że polecenia zabezpieczające mogą budzić wątpliwości konstytucyjne (ograniczenie samodzielności samorządu), lecz w sytuacji zagrożenia krytycznego argumentem jest tu ochrona nadrzędnych dóbr (bezpieczeństwo państwa, życie ludzi).

Dla podmiotów publicznych implikacje są takie, że muszą być gotowe technicznie i organizacyjnie na wykonanie ewentualnych poleceń. To znaczy: urzędy powinny mieć procedury i możliwości awaryjnego odłączenia systemów, przestawienia się na tryb manualny obsługi usług czy uruchomienia zapasowych systemów, jeśli przyjdzie nakaz. Warto też przemyśleć kanały komunikacji – polecenie przyjdzie zapewne drogą pilną (np. szyfrowaną wiadomością z RCB/CSIRT), więc punkt kontaktowy ds. cyberbezpieczeństwa w jednostce musi być w stanie odebrać i rozpropagować taką dyspozycję natychmiast (również poza godzinami pracy). Na szczęście incydenty krytyczne to sytuacje rzadkie. Mimo to w dobie rosnących zagrożeń (np. w trakcie konfliktu hybrydowego) posiadanie takiego narzędzia może okazać się konieczne. Przykładowy scenariusz: fala cyberataków destabilizuje serwisy rządowe w całym kraju – rząd wydaje polecenie, by *wszystkie urzędy wojewódzkie* tymczasowo wyłączyły dostęp do swoich platform ePUAP i przeniosły obsługę newralgicznych spraw na tryb offline, dopóki incydent nie zostanie opanowany i systemy sprawdzone. Takie skoordynowane działanie może ograniczyć zasięg szkód.

Podsumowując, polecenie zabezpieczające jest narzędziem ostatecznym, z którego skorzysta się tylko w wyjątkowych sytuacjach zagrożenia. Jednostki sektora publicznego powinny jednak mieć świadomość jego istnienia i podporządkować się, gdy zostanie wydane – niewykonanie polecenia zapewne samo w sobie będzie poważnym naruszeniem ustawy, zagrożonym wysoką karą.

### 2.3.10. Zastosowanie przepisów w praktyce – przykłady dla JST, instytucji kultury, szkół, szpitali

Nowe przepisy KSC wpłyną bezpośrednio na codzienne funkcjonowanie rozmaitych instytucji publicznych. Poniżej przedstawiono kilka przykładów ilustrujących, jak w praktyce realizować obowiązki ustawy w różnych typach jednostek oraz jakie ryzyka i wyzwania mogą się pojawić:

- Urząd miasta (gmina > 50 pracowników) – podmiot kluczowy publiczny: Taki urząd będzie musiał gruntownie sformalizować swoje podejście do cyberbezpieczeństwa. Pierwszym krokiem będzie prawdopodobnie *wyznaczenie koordynatora ds. cyberbezpieczeństwa* (o ile dotąd nie było etatowego informatyka o takich kompetencjach). Następnie urząd musi opracować dokumentację SZBI: politykę bezpieczeństwa, procedury zarządzania dostępami do systemów (np. system meldunkowy, podatkowy), plan reagowania na incydenty (co zrobić, gdy system padnie ofiarą ataku). Konieczne stanie się przeprowadzenie analizy ryzyka – np. zidentyfikowanie, że jednym z największych zagrożeń jest phishing wymierzony w pracowników wydziału finansowego i ataki szyfrujące dokumenty. Urząd wdroży więc odpowiednie zabezpieczenia: przeszkolenie pracowników z rozpoznawania phishingu, wprowadzenie dwuskładnikowego uwierzytelniania do poczty służbowej, regularne backupy bazy dokumentów. W razie incydentu (np. zawirusowania stacji roboczej) urząd zgłosi to do CSIRT GOV. Dodatkowo, urząd przed zakupem nowego oprogramowania do obsługi mieszkańców przeprowadzi ocenę ryzyka dostawcy – czy firma ma certyfikaty, czy kod będzie audytowany, czy nie jest na liście DWR. Ryzykiem dla gminy jest tu głównie brak wyspecjalizowanego personelu i funduszy – dlatego może skorzystać z rozwiązania centrów usług wspólnych (patrz pkt 11), np. powierzyć obsługę bezpieczeństwa IT wspólnemu centrum na szczeblu powiatu. Niemniej odpowiedzialność za zgodność z ustawą spoczywa na burmistrzu i to on będzie musiał dopilnować, by wszystkie wymagania art. 8–11 zostały spełnione, inaczej grożą kary finansowe dla urzędu lub nawet dla niego samego.
- Samorządowa instytucja kultury (np. miejska biblioteka) – podmiot ważny publiczny: Biblioteka publiczna zatrudniająca 15 osób formalnie będzie podmiotem ważnym (bo instytucja kultury jest wymieniona w zał. 2). To oznacza, że *musi spełnić niemal te same wymagania co podmioty kluczowe*, choć jej nadzór będzie łagodniejszy (kontrola tylko następcza). W praktyce biblioteka pewnie nie ma dedykowanego specjalisty IT – więc dyrektor może wyznaczyć jednego z pracowników (lub siebie) jako osobę kontaktową ds.

KSC i zlecić firmie zewnętrznej przygotowanie dokumentacji SZBI. Biblioteka zinwentaryzuje swoje systemy (np. katalog książek online, komputery dla czytelników, monitoring CCTV budynku) i oceni zagrożenia (włamanie do sieci Wi-Fi, kradzież danych czytelników). Wdroży podstawowe środki: silne hasła na routerach, antywirus na komputerach, rozdzielenie sieci gościnnej od wewnętrznej. Jeśli zdarzy się incydent (np. atak ransomware szyfrujący komputery), biblioteka powiadomi CSIRT NASK i poprosi zapewne o pomoc miasto (właściciela). Wyzwanie dla instytucji kultury to brak kompetencji – stąd ustawa przewiduje, że np. gmina może pomóc swoim instytucjom wypełniać obowiązki (mechanizmy wspólnego wykonywania zadań opisane w pkt 11). Bez takiej pomocy ryzykiem jest, że mała instytucja nie poradzi sobie z formalnościami (co naraża ją i dyrektora na kary, choć pewnie organ nadzoru brałby pod uwagę skalę i mógłby poprzestać na zaleceniach przy pierwszych brakach).

- Szpital powiatowy – podmiot kluczowy (sektor zdrowia): Publiczne szpitale już od 2018 r. często były operatorami usług kluczowych, więc w pewnym stopniu są przygotowane do nowych wymogów. Jednak NIS 2 zaostrza wymagania – szpital będzie musiał np. zapewnić audyt zewnętrzny bezpieczeństwa co parę lat, poszerzyć polityki o nowe elementy (np. procedura ujawniania podatności). Szpital ma wiele systemów (HIS, RIS/PACS, e-recepta, serwer ERM) i jest narażony na ataki ransomware (przykłady z ostatnich lat w Polsce pokazały, że szpitale były celem ataków). Nowe przepisy wymuszą na szpitalu lepszą izolację sieci medycznej, szyfrowanie danych pacjentów, a także formalne przeszkolenie personelu medycznego z cyberhigieny (bo incydenty często zaczynają się od błędu człowieka). W razie poważnego incydentu (np. unieruchomienie systemu rejestracji pacjentów) szpital powiadomi CSIRT sektorowy (prawdopodobnie CSIRT CSIOZ/MZ, jeśli taki powstanie) w 24h i 72h. Będzie musiał też zapewnić ciągłość działania – np. przejść na tryb papierowy w izbie przyjęć, jeśli system padnie. Ryzyko dla szpitala – oprócz zagrożeń związanych z bezpieczeństwem – to możliwość wysokich kar finansowych w razie zaniedbań (dyrekcja szpitala odpowiada podobnie jak firma, do 10 mln euro lub 2% obrotu, co w praktyce może sięgnąć milionów złotych kary). To motywuje dyrekcję, by inwestować w IT (choć budżety publicznych placówek ochrony zdrowia są napięte). W razie ataku zagrażającego pacjentom możliwe byłoby też wydanie polecenia zabezpieczającego – np. Minister

mógłby nakazać wyłączenie szpitalnej sieci IT celem izolacji zagrożenia, co pokazuje jak poważnie traktuje się takie sytuacje.

- Uczelnia publiczna – podmiot ważny (sektor edukacja/badania): Większość szkół wyższych i instytutów badawczych wejdzie do kategorii podmiotów ważnych (zgodnie z art. 7 ust. 1 pkt 1–4, 6–7 ustawy Prawo o szkolnictwie wyższym i nauce wymienionymi w zał. 2). Dla dużych uniwersytetów przepisy KSC będą nowością – dotąd nie były one OUK, choć oczywiście chroniły swoje dane (np. systemy dziekanatowe czy bazy naukowe). Teraz uczelnia musi formalnie wdrożyć SZBI: np. Politechnika będzie musiała sporządzić politykę bezpieczeństwa i powołać zespół ds. cyberbezpieczeństwa (być może rozbudowując istniejące działy IT/certy akademickie). Wymagane będzie zabezpieczenie sieci uczelnianej, która bywa bardzo rozległa i otwarta (studenci, goście Wi-Fi) – może to oznaczać inwestycje w segmentację sieci, systemy NAC do kontrolowania urządzeń podłączanych przez studentów. Ponadto uczelnie prowadzą projekty badawcze o znaczeniu strategicznym – ustawa wymienia instytucje badawcze jako podmioty ważne, by zapewnić ochronę kluczowych badań (np. nad technologiami, które mogłyby być celem cyberszpiegostwa). Wyzwaniem dla uczelni będzie pogodzenie kultury otwartości akademickiej z koniecznością wprowadzenia restrykcyjnych zasad bezpieczeństwa (np. wymuszanie zmiany haseł, monitorowanie ruchu sieciowego – to może spotkać się z oporem użytkowników). Jednak w razie incydentu, np. wycieku danych studentów, rektorat musi działać zgodnie z ustawą: zgłosić incydent do CSIRT, powiadomić też zapewne UODO (jeśli dane osobowe wyciekły). Kary finansowe mogą dotknąć uczelnię podobnie jak firmy, co dla instytucji publicznej byłoby dotkliwe zarówno finansowo, jak i reputacyjnie.
- Jednostka administracji rządowej – podmiot kluczowy publiczny: Weźmy np. Urząd Wojewódzki. Jako organ administracji zespolonej w terenie, urząd wojewódzki stanie się podmiotem kluczowym publicznym (marszałkowski jest samorządowy, wojewódzki – rządowy). Taki urząd już teraz podlega różnym reżimom bezpieczeństwa (np. ma Pełnomocnika ds. Ochrony Informacji Niejawnych, stosuje KRI). Nowelizacja spowoduje, że urząd wojewódzki będzie musiał zaktualizować swoje procedury i dostosować do KSC. Ponieważ organem nadzoru będzie tu Minister Cyfryzacji, można spodziewać się centralnych wytycznych dla urzędów. Urząd będzie zobligowany m.in. prowadzić rejestr incydentów i raportować je do CSIRT GOV (który obsługuje administrację rządową). W przypadku incydentu

krytycznego (np. masowego ataku na infrastrukturę usług administracji), to właśnie wojewodowie mogą otrzymać od Premiera polecenie zabezpieczające, by skoordynować działania w terenie. Urząd wojewódzki też może pełnić rolę pomocniczą dla mniejszych jednostek – np. zapewniać wspólną obsługę bezpieczeństwa dla urzędów gmin w swoim województwie, jeśli takie rozwiązanie zostanie wprowadzone (o czym w pkt 11). Ryzyko dla urzędu wojewódzkiego jest stosunkowo niewielkie, bo to duża jednostka dysponująca zasobami – jednak ewentualne naruszenie (np. wyciek danych z rejestrów) mógłby mieć skutki polityczne i zostać ukarany przykładnie wysoką karą (w granicach 100 mln zł w skrajnych sytuacjach). Dlatego administracja rządowa już teraz przygotowuje się na te zmiany, organizując szkolenia i audyty (np. Ministerstwo Cyfryzacji testuje zdolności reagowania w różnych urzędach).

Jak widać, różnorodność podmiotów objętych ustawą jest ogromna – od małych gminnych bibliotek po duże ministerstwa. Ustawa stara się uwzględnić tę różnorodność, różnicując obowiązki i dopuszczając ich wspólne wykonywanie. Wspólnym mianownikiem jest jednak to, że każda instytucja publiczna powinna podnieść standardy swojego cyberbezpieczeństwa, formalizując procesy i inwestując w rozwiązania ochronne. W wielu przypadkach konieczna będzie zmiana dotychczasowego podejścia: z reaktywnego (działania po incydencie) na proaktywne i systemowe (zarządzanie ryzykiem przed incydentem). W praktyce sektor publiczny zapewne skorzysta z dostępnych wzorców – np. z normy PN-EN ISO/IEC 27001 jako bazy SZBI, z poradników CSIRT GOV czy z doświadczeń we wdrażaniu RODO (co często jest przywoływane jako analogia).

### 2.3.11. Współpraca i wspólne wykonywanie obowiązków przez podmioty publiczne

Nowelizacja dostrzega, że nie wszystkie podmioty publiczne – zwłaszcza na poziomie lokalnym – mają wystarczające zasoby, by samodzielnie sprostać nowym wymaganiom. Dlatego dodano do ustawy rozdział 3b pt. „Wspólne wykonywanie obowiązków z zakresu cyberbezpieczeństwa przez podmioty publiczne”. Celem tych przepisów jest umożliwienie jednostkom sektora finansów publicznych realizacji obowiązków ustawowych w modelu współpracy lub usług wspólnych, co ma podnieść efektywność i obniżyć koszty. Kluczowe rozwiązania to:

- **Centra Usług Wspólnych (CUW) ds. Cyberbezpieczeństwa**

- JST mogą tworzyć wyspecjalizowane jednostki organizacyjne (lub rozbudować istniejące centra usług wspólnych) zajmujące się obsługą cyberbezpieczeństwa dla wielu podmiotów jednocześnie.
- Przykładowo, powiat może powołać powiatowe centrum cyberbezpieczeństwa, które będzie prowadzić SZBI nie tylko dla starostwa, ale i dla gmin z terenu powiatu, ich szkół, bibliotek itp.
- Taki CUW zatrudniałby ekspertów i świadczył „usługę" zapewnienia zgodności z ustawą dla podmiotów, które do niego przystąpią. Ustawa odsyła tu do ogólnych przepisów samorządowych o CUW (możliwość wspólnej obsługi administracyjnej jednostek).

- **Porozumienia między JST**
  - Alternatywnie lub uzupełniająco, kilka jednostek samorządu może zawrzeć porozumienie, na mocy którego jedna z nich (np. większe miasto lub urząd marszałkowski) będzie wykonywać zadania z zakresu cyberbezpieczeństwa w imieniu pozostałych.
  - Takie porozumienia „z góry na dół" mogą pozwolić mniejszym gminom przekazać obowiązki np. powiatowi, który dysponuje lepszym zapleczem IT.
  - Warunkiem jest wskazanie w porozumieniu konkretnych zadań i jednostek odpowiedzialnych.
  - Dla przykładu: kilka sąsiednich gmin wiejskich może umówić się, że ich obowiązki KSC przejmie powiatowe centrum informatyczne, które będzie prowadzić wspólny SZBI i obsługiwać incydenty dla wszystkich. To przypomina model z niektórych rozwiązań RODO, gdzie np. jeden inspektor ochrony danych obsługuje wiele szkół.
- **Obowiązek współpracy podmiotów korzystających ze wspólnej obsługi:**
  - Ustawa podkreśla, że jeśli ustanowiono taką wspólną jednostkę lub porozumienie, to podmioty publiczne objęte wspólną obsługą muszą współpracować z tą jednostką.
  - Współpraca ta polega m.in. na: przekazywaniu wszelkich informacji o incydentach do wspólnej jednostki, wykonywaniu decyzji i zaleceń jej kierownika w zakresie SZBI, publikowaniu na swoich stronach internetowych linku do strony tej jednostki (co sugeruje, że tam będą komunikaty dot. cyberbezpieczeństwa), oraz obowiązkowym udziale kierowników jednostek w szkoleniach organizowanych przez wspólną jednostkę. Innymi słowy, jeśli np. gminy powierzą swoje

obowiązki powiatowi, to wójtowie tych gmin muszą stosować się do instrukcji wydawanych przez powiatowego koordynatora cyberbezpieczeństwa.
    - Zapewnia to spójność – bo trudno wspólnie prowadzić SZBI, jeśli poszczególne gminy robiłyby coś po swojemu.
- **Podział odpowiedzialności i ewentualnych kar**
    - Choć ustawa tego explicite nie rozstrzyga na poziomie ogólnym, logika wskazuje, że odpowiedzialność administracyjna za naruszenia będzie spoczywać nadal na poszczególnych podmiotach (one są adresatami obowiązków ustawowych).
    - W praktyce jednak, jeśli np. gmina przekaże swoje obowiązki centrum usług wspólnych, a centrum to czegoś zaniedba, trudno obwiniać samą gminę.
    - Można przewidywać, że organ nadzoru w razie stwierdzenia uchybienia będzie kierował swoje zalecenia do jednostki obsługującej lub do wszystkich uczestników porozumienia.
    - Ustawa dopuszcza pewną decentralizację wykonywania zadań, ale nie zwalnia żadnego podmiotu z ostatecznej odpowiedzialności za zgodność – stąd każdy kierownik jednostki powinien pilnować, by nawet przy obsłudze w CUW jego instytucja dostarczała wymagane informacje i stosowała się do zaleceń (inaczej ryzykuje karę, choćby niższą, np. do 100% pensji w przypadku kierownika podmiotu publicznego).

Dla wielu małych jednostek opcja wspólnego wykonywania zadań będzie zbawienna. Pozwoli na oszczędność skali – zamiast każda szkoła osobno zatrudniać specjalistę, powiat zatrudni jednego eksperta obsługującego wszystkie szkoły. Ujednolicone zostaną polityki bezpieczeństwa (co zresztą sprzyja standaryzacji i łatwiej spełnić wymogi). Wspólne centra mogą też zapewnić lepszą reakcję na incydenty – np. jeden zespół monitorujący sieć całego powiatu wykryje szybciej atak dotykający wielu urzędów jednocześnie.

**Przykład**

W jednym z województw tworzony jest regionalny ośrodek cyberbezpieczeństwa pod auspicjami urzędu marszałkowskiego. Ośrodek ten zawiera porozumienia z gminami i powiatami, że przejmie ich obowiązki SZBI. Następnie zatrudnia kilkunastu specjalistów, którzy opracowują jednolitą politykę bezpieczeństwa dla wszystkich samorządów w regionie, konfigurują wspólnie używane systemy

(np. system kopii zapasowych w chmurze dla urzędów), organizują szkolenia dla pracowników wszystkich urzędów, a także pełnią 24/7 dyżur jako lokalny CSIRT – przyjmują zgłoszenia incydentów od gmin i reagują. Każda gmina za taką usługę płaci składkę, ale jest to dużo tańsze niż budowanie wszystkiego samemu. W razie kontroli Minister Cyfryzacji widzi, że np. gminy powiatu X mają wspólną obsługę, więc kontroluje centrum – a tam jest pełna dokumentacja i kompetentni ludzie, więc kontrola przebiega pomyślnie.

Podsumowując, wspólne wykonywanie obowiązków to odpowiedź na ryzyka i wyzwania, jakie nowelizacja stawia przed małymi podmiotami publicznymi. Zmniejsza to ryzyko niezgodności (bo fachowcy w CUW dopilnują wymogów) oraz ryzyko finansowe (dzielenie kosztów). Jednak kluczem jest tutaj dobra koordynacja oraz zaufanie między jednostkami – a także formalne uregulowanie porozumień. Ustawa tworzy ramy, ale to do samorządów należy inicjatywa ich wykorzystania. Jeśli zostanie to zrobione umiejętnie, polskie JST mogą kolektywnie podnieść swój poziom cyberbezpieczeństwa bez nadmiernego obciążenia każdej gminy z osobna, co wpisuje się w zasadę solidarności i efektywności w administracji.

*Niniejszy materiał opracowano na podstawie znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa (wersja ujednolicona z projektem UC32, wrzesień 2025) oraz oficjalnych omówień i komentarzy do ustawy. W tekście przytoczono liczne fragmenty przepisów (oznaczone artykułem, ustępem, punktem) oraz komentarze ekspertów, co zostało odpowiednio opatrzone przypisami. Wszystkie cytowane artykuły (art.) odnoszą się do znowelizowanej ustawy o KSC, zaś numery linii w odnośnikach – do źródłowych dokumentów i publikacji wskazanych w bibliografii.*

## 3. Wymogi cyberbezpieczeństwa w dokumentacji zamówień publicznych

### 3.1. Wstęp, czyli od czego zacząć przygotowania do prawidłowego udzielania zamówień publicznych

Skuteczne zbudowanie cyberodporności podmiotu publicznego nie jest możliwe bez zaangażowania procesu udzielania zamówień i zakupów w zarządzanie ryzykiem w obszarze cyberbezpieczeństwa, w tym

cyberbezpieczeństwa łańcucha dostaw. Podobne wytyczne można znaleźć w opublikowanych przez Ministerstwo Cyfryzacji "Praktykach zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw dla systemów i organizacji NIST SP 800-161r1_PL wer. 1.0", gdzie w najważniejszych wnioskach wyraźnie wskazano:" Włączenie zagadnień dotyczących obszaru C-SCRM do działań związanych z zamówieniami i zakupami jest kluczem do zapewnienia skuteczności programu C-SCRM. Wymagania dotyczące obszaru C-SCRM powinny zostać uwzględnione w całym cyklu życia zamówień. Działania związane z obszarem C-SCRM obejmują przeprowadzanie oceny ryzyka usług, dostawców i produktów; określanie odpowiednich zabezpieczeń w zakresie C-SCRM; przeprowadzanie analiz due diligence, a także stałe monitorowanie dostawców.[121] Jak już wspomniano w Rozdziale II, podmioty uznane za ważne i kluczowe zostaną objęte przepisami UKSC, a co za tym idzie zobowiązane będą do wdrożenia adekwatnych i proporcjonalnych środków zapewniających bezpieczeństwo łańcucha dostaw. Zważywszy, że projektowane zmiany UKSC obejmują swym zakresem szerszy katalog podmiotów niż dotychczas, w tym liczne grono jednostek zobowiązanych do stosowania ustawy Pzp, zamówienia staną się istotnym narzędziem kreującym cyberbezpieczeństwo usług ICT, systemów ICT oraz procesów ICT. Wraz z implementacją przepisów dyrektywy NIS 2, czy CRA liczne instytucje wejdą w permanentny ciąg zmian w obszarze technologicznym, administracyjnym a także zakupowym. Raz przyjęte praktyki, strategie i regulacje, również te wewnętrzne, pozostaną w jednostkach już na stałe i będą nieustannie ewoluować, a także promieniować na współpracujące podmioty: nie tylko wykonawców i podwykonawców, ale również podmioty zależne i nadzorowane.

Praktyczną emanacją holistycznego podejścia zamawiającego do współpracy będzie tworzenie multidyscyplinarnych zespołów, w skład których wejdą specjaliści od zarządzania kluczowymi procesami w organizacji - takimi jak zarządzanie ryzykiem, bezpieczeństwo informacji, zarządzanie zasobami ludzkimi, wsparcie prawne, ale także proces zamówień. Im większa organizacja tym więcej poziomów zarządzania zostanie zaangażowanych we współpracę, w celu opracowania i wdrożenia polityki wewnętrznej zarządzania ryzykami w obszarze cyberbezpieczeństwa. Zmiany obejmą także politykę zakupową zamawiającego lub sprzedażową wykonawców. Dobrą praktyką przy tworzeniu dokumentacji na

[121] "Praktyki zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw dla systemów i organizacji NIST SP 800-161r1_PL wer. 1.0" [online] https://www.gov.pl/web/baza-wiedzy/nist-sp-800-161r1-wer-10-pl dostępne 12.11.205 r.

potrzeby udzielenia zamówienia uwzględniającej aspekty cyberbezpieczeństwa będzie udział w komisjach przetargowych ekspertów (wewnętrznych bądź zewnętrznych), w celu spełnienia wynikających z przepisów i potrzeb wymagań.

Należy podkreślić, że nigdy nie dojdzie do jakiejkolwiek poprawy zarządzania cyberbezpieczeństwem łańcucha dostaw u zamawiającego bez włączenia do kompleksowej analizy ryzyk każdego etapu nabywania usług, procesów, produktów ICT - w tym planowania postępowań, udzielania zamówień, a także wykonywania umowy.

Każdy etap postępowania, który tworzy swoisty cykl życia zamówienia, powinien uwzględniać potrzebę zapewnienia adekwatnego dla danego zakupu usługi ICT, systemu ICT czy procesu ICT poziomu bezpieczeństwa.

Wspomniany cykl życia rozpoczyna się od określenia przez zamawiającego swojej potrzeby - obejmuje procesy:

- planowania i określania wymagań,
- prowadzenia badań w celu zidentyfikowania i oceny możliwych źródeł dostaw, pozyskiwania ofert,
- oceny ofert w celu zapewnienia zgodności z wymogami w zakresie cyberbezpieczeństwa oraz oceny ryzyka związanego z wykonawcą, a także z oferowanymi produktami lub usługami.

Prawidłowo sformułowane dokumenty zamówienia powinny odzwierciedlać działania zamawiającego zgodne z wymogami przepisów prawa oraz wewnętrznymi procedurami tak, aby dla wykonawców i organów nadzorujących było jasne, jak realizowana jest polityka zakupowa uwzględniająca bezpieczeństwo łańcucha dostaw. Dlatego też monitorowanie zmian, które mogą mieć wpływ na ryzyko związane z cyberbezpieczeństwem w łańcuchu dostaw, powinno odbywać się przez cały cykl życia zamówienia i może wymagać ponawiania oceny zdiagnozowanych ryzyk.

Umowy również powinny zostać skonstruowane w taki sposób, aby organy kontrolujące mogły uznać, że umożliwiają stałą weryfikację zarządzania ryzykiem zarówno poprzez monitorowanie, czy dostarczane produkty i usługi spełniają postawione przed nimi wymogi z zakresu cyberbezpieczeństwa, jak również czy sam wykonawca dochowuje należytej staranności w zakresie zarządzania wewnętrznymi ryzykami związanymi z cyberbezpieczeństwem łańcucha dostaw, chroniąc tym samym zamawiającego.

## 3.2. Planowanie, analiza potrzeb i wymagań oraz raporty do Prezesa Urzędu zamówień publicznych

### 3.2.1. Należyte planowanie jako źródło informacji odnośnie realizacji obowiązków wynikających z dyrektywy NIS 2 i CRA

Ustawodawca przewidział w art. 23 ust. 1 ustawy Pzp obowiązek opracowania przez zamawiających publicznych wskazanych w art. 4 pkt 1 i 2 ustawy Pzp oraz ich związki corocznego planu postępowań o udzielenie zamówień publicznych. Wartość takiego dokumentu dla efektywnego zarządzania zamówieniami w jednostkach publicznych jest niezaprzeczalna, gdyż daje kierownikowi jednostki całościową wiedzę o liczbie i wartości planowanych zamówień, terminach oraz trybach ich udzielania. Pozyskane w ten sposób informacje są niezbędne dla skutecznej kontroli zarządczej organizacją.

**Przydatne użycie planu:**

- Analizując historycznie swoje plany zamówień jednostki mogą nie tylko uzyskać niezbędne dane do realizacji zasady efektywności zamówień publicznych, ale również usystematyzować rodzaje i skalę swoich zamówień na usługi ICT, produkty ICT i systemy ICT. Dane zawarte w planach zamówień mogą pomóc zespołom odpowiedzialnym w danej instytucji za zarządzanie ryzykiem w obszarze cyberbezpieczeństwa w oszacowaniu, które z ryzyk mogą wystąpić i jaki jest wskaźnik prawdopodobieństwa zmaterializowania się określonego zagrożenia.
- Na podstawie historycznych informacji o potrzebach zakupowych organizacji możliwa jest ocena, choćby jakim oprogramowaniem posługuje się dana jednostka oraz czy sukcesywnie je aktualizuje i wspiera, jaki kupuje sprzęt i w jakiej ilości, a także czy występuje ryzyko uzależnienia od konkretnych dostawców. Kompleksowa analiza planów daje możliwość ustalenia, czy istnieje konieczność realizacji obowiązków wynikających z CRA i w jakiej skali.

W świetle nowych wymagań przewidzianych nowelizowaną ustawą KSC oraz CRA warto wykorzystywać rubrykę (6) przewidzianą we wzorze planu „Informacje na gromadzenie danych w obszarze możliwych ryzyk pojawiających się przy

danym zamówieniu [122]. Jednakże należy pamiętać, że plan zamówień jest dokumentem jawnym i zgromadzone dane będą powszechnie dostępne, dlatego też ważne jest, aby zawarte w nim informacje, zostały przedstawione w taki sposób, aby nie mogły zostać wykorzystane przez podmioty zamierzające negatywnie oddziaływać na infrastrukturę krytyczną.

### 3.2.2. Analiza potrzeb i wymagań

Kolejnym przydatnym źródłem informacji, którym w zestawieniu z planami może posłużyć zamawiającemu do przeglądu swojego procesu zakupowego jest analiza potrzeb i wymagań. Rzeczony dokument został wprowadzony do systemu zamówień publicznych jako sposób na realizację nowej zasady - efektywności. Jak wskazuje UZP w swoim komentarzu analiza potrzeb i wymagań: „Na etapie przygotowania postępowania stanowi zebranie informacji na temat potrzeb i wymagań zamawiającego, jakie mają być zaspokojone, i zarazem próbę odpowiedzi, jak te potrzeby i wymagania najlepiej, najskuteczniej i najefektywniej zaspokoić. Ponadto na etapie ewaluacji zamówienia lub na etapie przygotowania do kolejnego podobnego zamówienia wespół z raportem z realizacji zamówienia (art. 446 Pzp) stanowią cenne dokumenty pomocne przy planowaniu i realizacji kolejnych zamówień.“[123]

Zarówno plan zamówień jak i analiza potrzeb sporządzane są w celach analitycznych, aby umożliwić zamawiającym dokonywanie racjonalnych decyzji gospodarczych. Podobne twierdzenie znalazło się we “Wskazówkach dla zamawiających publicznych do opracowania analizy potrzeb i wymagań w świetle nowego prawa zamówień publicznych”[124], gdzie stwierdzono, że “W każdym przypadku zamawiający powinien również ocenić, jakie korzyści, koszty i ryzyka będą wiązać się ze stosowaniem wybranych metod zaspokojenia potrzeby bądź z nich wynikać”.

---

[122] Wzory planów postępowań o udzielnie zamówienia publicznego zostały określone w rozporządzeniu Ministra Rozwoju, Pracy i Technologii z 8 grudnia 2020 r. w sprawie wzorów planu postępowań (Dz. U. 2020.2362)

[123] Prawo zamówień publicznych, komentarz wyd. II. pod. red. Huberta Nowaka str. 83, https://www.gov.pl/web/uzp/komentarz-do-prawa-zamowien-publicznych [dostęp on line 12.11.2025]

[124] Wskazówki w przedmiocie analizy potrzeb i wymagan https://www.gov.pl/web/uzp/wskazowki-dla-zamawiajacych-publicznych-do-opracowania-analizy-potrzeb-i-wymagan [dostęp on line 12.11.2025]

**Ryzyko –** pomijanie w APW konieczności wypełniania wymogów dotyczących cyberbezpieczeństwa przewidzianych w dyrektywie NIS 2 lub CRA może prowadzić do zarzutów nienależytej realizacji obowiązków w obszarze zapewniania bezpieczeństwa łańcucha dostaw. Negatywny skutek wspomnianego powyżej zaniechania to np. możliwość uzależnienia się od jednego dostawy/producenta, zakup sprzętu niespełniającego wymagań CRA.
W trakcie APW ocenie ryzyka będzie podlegał zarówno wybór:

- technologii, jakimi posługiwać będą się zamawiający realizujący swoje zadania publiczne, jak również
- wykonawców/podwykonawców, którzy będą im partnerować w wykonywaniu dostaw ICT, usług ICT lub procesów ICT w celu realizacji zadań publicznych.

Z dyrektywy NIS 2 jasno przebija zamiar unijnego prawodawcy, aby zasada proporcjonalności zawsze przyświecała prowadzeniu postępowań o udzielenie zamówienia publicznego, co zostało wprost wyartykułowane w art. 21 ust. 1 dyrektywy klasycznej. Dlatego też projektując politykę zarządzania ryzykiem w obszarze cyberbezpieczeństwa warto w ramach holistycznego podejścia do zagadnienia wymagać, aby pracownicy przygotowujący wspomnianą analizę uwzględniali aspekty wpływające na zidentyfikowane w organizacji ryzyka w obszarze cyberbezpieczeństwa łańcucha dostaw już na najwcześniejszych etapach procesu związanego z udzieleniem zamówienia publicznego. W trakcie APW dokonywać się będzie analiza, czy obowiązki wynikające z NIS 2 bądź CRA muszą znaleźć odzwierciedlenie w opisie przedmiotu zamówienia, kryteriach wyboru. Dlatego też prawidłowo przygotowany dokument będący wynikiem APW powinien zawierać odzwierciedlenie oceny zamawiającego w obszarze zdiagnozowanych ryzyk.

Taka inicjatywa wymaga współdziałania osób o różnych specjalizacjach oraz na różnych poziomach zarządzania. Począwszy od kadry zarządzającej, która odpowiada za strategię cyberbezpieczeństwa i czuwa nad bezpieczeństwem infrastruktury, przez pracowników badających rynek, którzy posiadają odpowiednią wiedzę merytoryczną dotyczącą konkretnego zakupu i realizacji umowy, wydziały zamówień publicznych uwzględniające w procedurze niezbędne elementy wskazanych polityk po działy prawne, czuwające nad zabezpieczającymi realizację umowy odpowiednimi postanowieniami umownymi. Ustawodawca w art. 83 ust. 3 pkt 5 ustawy Pzp wprowadził wprost zalecenie, aby analiza potrzeb i wymagań wskazywała na ryzyka związane z postępowaniem o udzielenie i

realizację zamówienia. Nie będzie stanowić nadinterpretacji intencji twórców tego przepisu, jeżeli zamawiający na jego podstawie oprócz ryzyk związanych z terminowością czy zasobami finansowymi zweryfikują przyszły zakup pod kątem także zdiagnozowanych ryzyk w ramach cyberbezpieczeństwa łańcucha dostaw.

Ustawodawca nie sprecyzował dokładnej treści czy obszerności analizy pozostawiając te kwestie zamawiającym. W niektórych wypadkach wystarczająca będzie krótka notatka, jednakże w sytuacji, gdy przed zamawiającym zostanie postawione skomplikowane zadanie - choćby stworzenia zawansowanego projektu dotyczącego infrastruktury krytycznej - analiza przybierze formę wielowątkowego studium. W ramach takiego dokumentu nie może zabraknąć wykazu ryzyk związanych także z cyberbezpieczeństwem, jeżeli opis przedmiotu zamówienia lub infrastruktura, której dotyczy, znajduje się w obszarze wskazanym w strategii cyberbezpieczeństwa. Prezes UZP w opublikowanym na swojej stronie poradniku Wskazówki dla zamawiających publicznych do opracowania analizy potrzeb i wymagań w świetle nowego Prawa zamówień publicznych[125] wskazał: ”Pojęcie „ryzyka” nie jest zdefiniowane normatywnie na gruncie prawa zamówień publicznych. W rozumieniu powszechnym ryzyko oznacza miarę, ocenę zagrożenia czy niebezpieczeństwa wynikającego albo z prawdopodobnych zdarzeń od nas niezależnych, albo z możliwych konsekwencji podjęcia decyzji.” Zatem pojęcie zarządzenia ryzkiem związanym z bezpieczeństwem łańcucha dostaw mieści się także w obszarze zarządzania ryzykiem w ramach konkretnego zamówienia.

**Przykładowe zagadnienia, których rozpoznanie może wpłynąć na prawidłowe przygotowanie APW**

Przygotowując analizę warto zastanowić się w zależności od stojącego przed zamawiającym wyzwaniem:

- Czy na potrzeby jednostki bezpieczne będzie nabycie rozwiązania opartego na oprogramowaniu zamkniętym, czy też otwartym (Open Source)? - przy jednoczesnym wskazaniu występujących ryzyk typu – oprogramowanie zamknięte może prowadzić do uzależnienia instytucji od jednego producenta oprogramowania, oprogramowanie otwarte może być bardziej podatne na umieszczanie w nim złośliwego kodu, jeżeli jego producent nie będzie poddawał kontroli procesu wytwórczego swojego kodu.

[125] Ibid.

- Czy urządzenia, które zostaną nabyte mogą zawierać komponenty niebezpieczne np. oprogramowanie z back door'em, czy mogą posiadać elementy nieautoryzowane, których pochodzenie lub funkcje będą zamawiającemu nieznane?
- Czy konieczna będzie ochrona informacji zawartych w dokumentach postępowania, jeżeli tak, to jakich informacji i w jaki sposób?
- Czy planując zakup usługi chmurowej organizacja potrzebuje dokonać jakiś działań wynikających z przepisów dotyczących tego typu usług np. ze względu na przetwarzane informacje zamówienie powinno dotyczyć modelu chmury prywatnej, hybrydowej, czy też bezpiecznie można będzie przechowywać informacje w chmurze publicznej?
- Czy zamówienie jest realizowane pierwszy raz, czy też jest powtórzeniem poprzedniego i trzeba przemodelować opis przedmiotu zamówienia lub warunki udziału w postępowaniu ze względu na nowe przepisy zmieniające UKSC lub CRA lub inne przepisu regulujące wymogi dotyczące cyberbezpieczeństwa?
- Czy należy zdywersyfikować rodzaj nabywanych dóbr, aby stworzyć infrastrukturę odporną na przerwanie łańcucha dostaw?
- Czy planowane rozwiązanie w zakresie cyberbezpieczeństwa nie generują nadmiernych kosztów albo czy dotychczasowe rozwiązanie były niewystarczające i należy zmienić producenta/wykonawcę lub przemodelować infrastrukturę?
- Czy w postępowaniu należy postawić na sprawdzonych, doświadczonych wykonawców czy też można się zdecydować na swobodne dopuszczenie szerokiej gamy wykonawców, jeżeli nabywane rozwiązanie jest dla zamawiającego newralgiczne, jaki wykonawca daje najlepsze gwarancje? (Uwaga: taka analiza nie powinna wskazywać na konkretnego wykonawcę, a zdiagnozować jakimi cechami winien się legitymować potencjalny wykonawca, aby zapewnił nam możliwie najlepsze gwarancje realizacji umowy.)
- Czy projektowane rozwiązanie wiąże się ze zdiagnozowanymi w matrycy ryzyk danej jednostki zagrożeniami?
- Czy projektowane rozwiązanie będzie wiązało się w jakikolwiek sposób z innymi jednostkami i musi spełniać jakieś dodatkowe wymagania w obszarze cyberbezpieczeństwa wynikające z takiego powiązania lub współpracy?

- Czy zamawiający potrzebuje jakiś szczególnych zabezpieczeń fizycznych, technologicznych lub prawnych, wynikających z mapy ryzyk w obszarze cyberbezpieczeństwa, jeżeli tak, to jaki jest wpływ takich wymagań na terminy realizacji zamówienia i jego wartość?
- Czy podzielenie zamówienia na części wpłynie na cyberbezpieczeństwo np. posiadanego Systemu IT?

**Uwaga:** Powyższe pytania stanowią jedynie przykładowe zagadnienia, które mogą się pojawiać w obszarze cyberbezpieczeństwa łańcucha dostaw. Zamawiający powinien podchodzić do każdego zamówienia indywidualnie, gdyż jak już wspomniano polityka zarządzaniem ryzkiem w organizacji jest zmienna i wymaga ciągłego reagowania na nowe zagrożenia pojawiające się w cyberprzestrzeni.

W przypadku, gdy analiza potrzeb wykaże ryzyko w obszarze cyberbezpieczeństwa następnym krokiem, do którego zamawiający jest zobowiązany przy dokładaniu należytej staranności, jest ocena prawdopodobieństwa zmaterializowania się ryzyka i jego wpływ na realizację potrzeby.
Innymi słowy w wyniku analizy potrzeb i wymagań zamawiający musi zdiagnozować swój apetyt na ryzyko i przeanalizować najbardziej efektywne rozwiązanie, wybierając czasami pomiędzy rozwiązaniami droższymi, bardziej skomplikowanymi, ale bezpieczniejszymi albo tańszymi, gdyż ryzyko zostanie uznane za akceptowalne. Scenariusz, na który zdecyduje się zamawiający powinien być obiektywnie uzasadniony i odzwierciedlony w treści APW.

## 3.3. Wstępne konsultacje rynkowe

### 3.3.1. Rola instrumentu w procesie uwzględniania cyberbezpieczeństwa łańcucha dostaw w dokumentacji przetargowej

W wyniku analizy potrzeb i wymagań u zamawiającego może pojawić się potrzeba przeprowadzenia wstępnych konsultacji rynkowych. Instytucja ta zastępująca dialog techniczny przewidziany ustawą - Prawo zamówień publicznych z 2004 r. daje większe możliwości niż poprzednie rozwiązania legislacyjne do uzupełnienia częstych u zamawiającego luk kompetencyjnych. W art. 40 dyrektywy klasycznej i art. 58 dyrektywy sektorowej unijny prawodawca przewidział

możliwość wejścia w sposób jawny i legalny w swoistą dyskusję bez narzucania zamawiającym sztywnych form takiego kontaktu. Oczywiście pozostały obowiązki zapewnienia równego traktowania wykonawców oraz przestrzegania zasady uczciwej konkurencji, jednak sposób rozmów z rynkiem pozostał jedynie ramowo naszkicowany, co należy uznać za plus zwłaszcza w sytuacji dynamicznie rozwijających się technologii, które trudno jest zamawiającym na bieżąco monitorować. Narzędziem, które umożliwia w sposób legalny na pozyskanie potrzebnej wiedzy z rynku jest jak już wspomniano instytucja przewidziana w art. 84 ustawy Pzp. Rozwiązanie to nie jest idealne i nie zawsze pozwoli uniknąć wszystkich "pułapek", gdyż wykonawcy zazwyczaj nie chcą się dzielić swoim know – how, jeśli nie mają z tego tytułu zagwarantowanych korzyści, a uczestnictwo w konsultacjach generuje koszty. Potencjalny wykonawca dysponujący skuteczniejszym zespołem potrafi lepiej przekonać do swoich rozwiązań, które w istocie rzeczy nie zawsze muszą być najlepsze, lecz zostaną najlepiej zaprezentowane.

Zapewnienie cyberbezpieczeństwa łańcucha dostaw ze względu na funkcjonowanie w wielowymiarowym ekosystemie nastręczy licznych trudności zarówno na polu organizacyjnym, technologicznych jak i prawnym z powodu funkcjonującej luki kompetencyjnej wynikającej z braku dostępnych na rynku specjalistów, którzy pomogliby zamawiającym przy podejmowaniu decyzji w zakresie zdiagnozowanych potrzeb. Jednakże wydaje się, że konsultacje pozostają najlepszym prawnym mechanizmem nawiązania kontaktu z rynkiem przed wszczęciem postępowania o udzielenie zamówienia i dają także doskonałą możliwość przekazania potencjalnym wykonawcom, jakie wymagania w zakresie cyberbezpieczeństwa mogą być im postawione. Właśnie wstępne konsultacje rynkowe czy nawet zwykłe szacowanie są w stanie pomóc zamawiającym ustalić, czy przewidywane potrzeby i wymagania odzwierciedlają realną ocenę ryzyka w ich organizacji oraz zderzyć tę ocenę z dojrzałością rozwiązań stosowanych przez wykonawców oraz ich faktycznych możliwości do spełnienia postawionych wymagań.

Zatem przed wszczęciem postępowania o udzielenie zamówienia instytucje planujące nabyć usługi ICT, procesy ICT czy dostawy ICT mogą powiadomić wykonawców o swoich potrzebach oraz wymaganiach, również tych w obszarze cyberbezpieczeństwa.

Na konsultacje rynkowe można spojrzeć także z odwrotnej strony. Zamawiający posługując się tą instytucją mają sposobność sprawdzenia wykonawców, na ile są oni przygotowani w zakresie zapewnienia cyberbezpieczeństwa sobie i swoim klientom. W ten sposób w formie pytań i odpowiedzi zamawiający mogą dopasować swoje wymagania w obszarze cyberbezpieczeństwa łańcucha dostaw do możliwości rynku, aby warunki postawione w omawianym obszarze pozostawały uzasadnione, proporcjonalne, realne i umożliwiały wykonawcom złożenie oferty. Natomiast zaadresowanie tematu zabezpieczenia łańcucha dostaw usług ICT, procesów ICT czy dostaw ICT w trakcie wstępnych konsultacji rynkowych będzie dla wykonawców czytelnym sygnałem, że obszar ten należy taktować poważnie, jeżeli planuje się aktywny udział w postępowaniach o udzielenie zamówień publicznych.

### 3.3.2. Przykładowe zagadnienia do omówienia z wykonawcami podczas wstępnych konsultacji rynkowych dające obraz cyberbezpieczeństwa łańcucha dostaw

W przypadku, gdy Zamawiający zdiagnozował potrzebę zakupu usługi, procesu, produktu ICT (np. sprzętu komputerowego, urządzeń sieciowych) zespół zajmujący się realizacją zamówień razem z osobami odpowiedzialnymi za stroną techniczną posiadanego lub planowanego rozwiązania może w trakcie wstępnych konsultacji zadbać o ochronę łańcucha dostaw ustalając przykładowo:

- Czy planowany do wykorzystania oferowany sprzęt będzie spełniał wymagania dotyczące certyfikatów potwierdzających ich bezpieczeństwo (np. Common Criteria, raporty SBOM/VEX, certyfikaty w schematach UE (EUCC)?
- Czy wykonawcy posiadają certyfikaty np. ISO/IEC 2700-1, ISO/IEC 27017 lub inne w dopasowane do rodzaju i skali zamówienia? (Uzyskanie z rynku informacje od potencjalnych wykonawcach oraz o postrzeganiu przez nich ryzyka w obszarze cyberbezpieczeństwa może pomóc w przygotowaniu adekwatnych i proporcjonalnych warunków w postępowaniu o udzielenie zamówienia lub kryteriów oceny ofert)
- Czy wykonawcy posiadają poświadczenia bezpieczeństwa przemysłowego i jakiego stopnia – czy posiadanie takiego poświadczenia wiąże się z przedmiotem zamówienia?

- Czy wykonawcy zatrudniają osoby posiadające dostępy do informacji objętych ochroną na podstawie klauzul określonych w ustawie o dostępie do informacji niejawnych?
- Czy pracownicy przechodzą regularne szkolenia z cyberhigieny i jak te szkolenia wyglądają, jak są częste, ile trwają, jakie tematy są poruszane?
- Czy wykonawca wdraża i utrzymuje u siebie zasady cyberhigieny oraz czy podwykonawcy są weryfikowani w zakresie przestrzegania analogicznych wymogów?
- Czy pentesty są regularnie wykonywane?
- Czy wykonawca poddaje się zewnętrznym audytom w obszarze cyberbezpieczeństwa, jak często, czy ma na to dowody i jakie?
- Jakie dowody może przedstawić wykonawca na potwierdzenie wdrożonych u siebie procedur w obszarze cyberbezpieczeństwa - takie pytania pozwolą ustalić, jakich aktualnych dowodów może wymagać zamawiający.
- Czy wykonawca dba o ciągłość i stałą gotowość do świadczenia usług np. wykonywanie kopii zapasowych danych, odtwarzanie po awarii?

- Czy w przypadku konieczności powierzenia przetwarzania danych osobowych wykonawca wie, gdzie dokładnie zostaną przekazane (w UE czy też poza terytorium UE)?
- Czy wykonawca ma wdrożoną procedurę na wypadek wystąpienia incydentu i jak planuje pomagać zamawiającemu w przypadku wystąpienia takiego zdarzenia, czy w organizacji została ustanowiona polityka zarządzania podatnościami?
- Jakie wykonawca ma przewidywane czasy reakcji na incydenty cyberbezpieczeństwa?
- Czy wykonawca redukuje ekspozycje na Internet, czy dba o dostęp wyłącznie z zaufanych adresów, czy dba o segmentację środowisk?
- Czy szyfruje transmisję danych?
- Czy kontroluje dostępy i tożsamość przy usługach chmurowych?
- Czy chroni przetwarzane dane przed ich nieuprawnioną modyfikacją i jak?
- Czy korzysta z narzędzi SI i w jaki sposób, czy ma procedurę korzystania z takich narzędzi?

- Jakie są modele licencjonowania proponowanych produktów?
- Jakie parametry SLA mogą zaproponować poszczególny wykonawcy?
- Czy istnieje możliwość analizy próbek i na jakich warunkach?

**Ważne:** Zamawiający powinni się dobrze przygotowywać do spotkań z wykonawcami, wcześniej opracowywać listę zagadnień do omówienia i w sposób przejrzysty komunikować rozmówcom swoje potrzeby. Przygotowanie listy pytań oraz prezentacji zarówno przez wykonawców jak i zamawiającego wydaje się być dobrą praktyką w tego typu spotkaniach.

Ze wstępnych konsultacji rynkowych korzystali zamawiający realizujący najbardziej skomplikowane inwestycje w kraju, aby uzyskać dostęp do najnowszych rozwiązań technicznych i technologicznych czy organizacyjnych funkcjonujących na rynku. Dlatego też jest to doskonałe narzędzie zarówno do:

- pozyskiwania skutecznie i efektywnie wiedzy w obszarach powszechnych jak i niestandardowych rozwiązań telekomunikacyjnych, czy teleinformatycznych, których ewolucja przebiega w wyjątkowo szybkim tempie, jak również
- zaprezentowania swych potrzeb związanych z cyberbezpieczeństwem dostawcom rozwiązań ICT.

W ten bezpieczny sposób zamawiający, którzy w wyniku luki kompetencyjnej nie potrafią samodzielnie poradzić sobie z opisem swoich potrzeb, mogą uzyskać wiedzę umożliwiającą adekwatne umiejscowienie w opisie przedmiotu zamówienia stosownych wymagań łagodzących ryzyka dla cyberbezpieczeństwa łańcucha dostaw np.:

- dobór właściwego certyfikatu do nabywanego produktu,
- określenie proporcjonalnych do możliwości rynku warunków udziału w postępowaniu (np. zakres doświadczenia wykonawców umożliwiający przygotowanie wymogów uznawanych w postępowaniu, referencji),
- znalezienie rozwiązań wariantowych dla dotychczas planowanych.

Wszystkie narzędzia komunikacji z rynkiem np.:

- szacowanie wartości zamówienia,
- wstępne konsultacje rynkowe,
- pytania RFI czy RFP,

powinny być wykorzystywane przez zamawiających zamierzających zapewnić bezpieczeństwo swojemu łańcuchowi dostaw, gdyż ono nie zaistnieje, jeżeli potencjalni wykonawcy nie będą mieli wiedzy o niezbędnych, minimalnych wymaganiach w tym zakresie.

**Przykład**: W wyniku analizy informacji uzyskanych z rynku zamawiający mogą dojść do wniosku, że nawet minimalne wymagania wobec wykonawców, które zamierzał postawić zamawiający są nadmiarowe i naruszają zasadę proporcjonalności choćby w sytuacji, gdy wykonawcy realizując zamówienie uzyskają jedynie sporadyczny i mocno ograniczony dostęp do limitowanych i konkretnych danych lub miejsc. Może się okazać także odwrotnie, że realizacja zamówienia wiąże się z głębokim dostępem do infrastruktury krytycznej i zaspokojenie potrzeby zamawiającego w bezpieczny sposób możliwe będzie wyłącznie poprzez jego samodzielne działania bez dopuszczania kogokolwiek z zewnątrz.

Ponadto uzyskanie niezbędnej wiedzy od rynku może skutkować także doborem odpowiedniej procedury postępowania lub zmiany kwalifikacji zamówienia z klasycznego na zamówienie z dziedziny obronności i bezpieczeństwa.

Nie tylko wstępne konsultacje rynkowe mogą pomóc określić wymagania w obszarze cyberbezpieczeństwa łańcucha dostaw, gdyż już na etapie szacowania wartości zamówienia zamawiający mogą zbierać informacje odnośnie przedmiotu zamówienia i warunków świadczenia. W przypadku gdy zdiagnozowana zostanie potrzeba zarządzania ryzykami w obszarze cyberbezpieczeństwa łańcucha dostaw, przekazanie informacji o obowiązku zapewnienia odpowiedniej ochrony informacjom objętym umową oraz konsekwencje naruszenia tych obowiązków mają charakter istotnych, cenotwórczych warunków stawianych wykonawcom. Kolejną ważną informację stanowi kwestia możliwości korzystania z podwykonawców, którzy bez wątpienia pozostają ogniwami łańcucha. Zwłaszcza w obszarze zamówień dotyczących obronności i bezpieczeństwa, ograniczenia w doborze podwykonawców znajdują szczególne uzasadnienie i zapewne w wyniku dynamicznie zmieniającej się sytuacji geopolitycznej pojawią się wkrótce szerzej w dokumentacji na potrzeby udzielania zamówień dotyczących także systemów IT/OT. Stąd do istotnych zobowiązań umownych publikowanych lub w inny sposób udostępnianych przez zamawiających nawet na wczesnych etapach

przygotowania postępowania o udzielenie zamówienia zaliczyć należy wytyczne, na jakie rodzaje umów z podwykonawcami zamawiający powinien zwrócić szczególną uwagę. Świadczenia podwykonawców istotne z punktu widzenia bezpieczeństwa łańcucha dostaw nie powinny pozostać poza regulacjami kontaktowymi pomiędzy zamawiającym a wykonawcą. W tym wypadku standardowe postanowienie umowne odnośnie odpowiedzialności wykonawcy za działania swojego podwykonawcy regulują zapisy art. 409 ustawy Pzp, które umożliwiają ustanowienie szczególnych wymogów dotyczących podwykonawstwa. Należyte zabezpieczenie łańcucha dostaw powinno obejmować zarówno kwestie odpowiedzialności za podwykonawcę, ale także obowiązki w zakresie zmiany takiego podwykonawcy (art. 409 ust. 1 pkt 2 ustawy Pzp), zmiany technologii lub usług, jeżeli zostaną uznane za cyberzagrożenie.

Analizowanie wniosków wynikających z dokumentów opisujących poszczególne wymagania wobec procesów, usług i dostaw ICT może przyczynić się do optymalizacji wewnętrznych potrzeb organizacji, jak również poprawy efektywności dokonywanych zakupów, co powinno skutkować zmniejszeniem nakładu pracy i uniknięciem generowania nadmiarowych, zbędnych zadań. Informacje zdobyte w trakcie prowadzonych konsultacji, prac nad planem, szacowania wartości zamówienia czy pytań RFP i RFI pozwolą w skali organizacji przygotować możliwie najefektywniejszą politykę zarządzania zobowiązaniami zamawiających i wykonawców w obszarze cyberbezpieczeństwa łańcucha dostaw.

### 3.3.3 Korzyści wynikające z konsultacji z rynkiem

Przypomnieć należy, że projektowane przepisy ustawy o KSC przewidują możliwość kontroli w podmiotach objętym jej regulacjami przez organy właściwe także w zakresie środków stosowanych w celu zapewnienia bezpieczeństwa łańcucha dostaw. Tym samym prowadzenie wstępnych konsultacji rynkowych, w których podjęte zostaną tematy dotyczące zarządzania ryzykami związanymi z cyberbezpieczeństwem:

- doskonale wpisze się w realizację ustawowych obowiązków, w tym realizację wewnętrznej polityki tworzenie cyberodporności organizacji,
- pozwoli na zbudowanie argumentacji pozwalającej uzasadnić dobór rozwiązań uzasadnionych i proporcjonalnych do zamierzonych celów,

- przybliży do dobrej praktyki polegającej na ustanowieniu indywidualnych wymagań w obszarze danego zamówienia, dostosowanych do zdiagnozowanych ryzyk i pomoże uniknąć zagrożenia, jakim jest naturalna skłonność organizacji, do ustanawiania wzorów postanowień umownych, zapisów SWZ poprzez określanie tego samego pakietu wymagań wobec wszystkich wykonawców w obszarze określonego przedmiotu zamówienia. Obowiązek proporcjonalnego i uzasadnionego określania wymagań wobec wykonawców był wielokrotnie wyartykułowanym przez TSUE, KIO, czy UZP, jednak każda organizacja cechuje się chęcią optymalizacji procesu także zakupowego poprzez stosowania ujednoliconych wzorów. Praktyka ta w żaden sposób nie jest naganna, a wręcz przyspiesza realizację zamówień publicznych, jednak w dłuższej perspektywie potrafi ujawnić tendencję do bezrefleksyjnego kopiowania wymagań, które nie pasują do przedmiotu zamówienia albo już się zdezaktualizowały.

Jak już to było wspominane, aby skutecznie zarządzać ryzykiem w obszarze cyberbezpieczenstwa danej organizacji niezbędne jest przygotowanie i wdrożenie strategii oraz opracowanie matrycy ryzyk w tym tych pojawiających się w trakcie procesu udzielania zamówień publicznych. Omówionej powyżej dokumenty takie jak plany postępowań, protokoły z wstępnych konsultacji rynkowych, dane zgromadzone w ramach RFI czy RFP służą generowaniu wiedzy mającej wspomóc zamawiającego w określeniu minimalnych wymogów stawianych wykonawcom w celu zapewnienia stabilności i ochrony łańcucha dostaw. Kolejnym dokumentem umożliwiającym efektywne wykorzystanie posiadanej przez zamawiającego wiedzy do tworzenia matrycy ryzyk jest raport z realizacji umowy, o którym mowa w art. 446 ustawy Pzp.

### 3.4. Raport z realizacji umowy

Postanowienia umowne w obszarze ochrony informacji pojawiających się w ramach realizacji zamówienia publicznego bez wątpienia są jednym z istotniejszych aspektów oceny cyberbezpieczeństwa łańcucha dostaw. Jak słusznie wskazuje się w Komentarzu do Prawa zamówień publicznych – II wydanie ”Z analizy treści umowy oraz sposobu jej realizacji zamawiający może wywieść wnioski pozwalające mu na wprowadzenie zmian mających na celu poprawę procesu

zakupowego w odniesieniu do podobnych zamówień w przyszłości.[126]" Obowiązek sporządzenia raportu jest elementem praktycznego zastosowania zasady efektywności mającej na celu wzmocnienie regulacji dotyczących fazy wykonania zamówienia i jego ewaluacji. Ustawodawca przewidział sytuacje, gdy taki raport musi zostać przygotowany. Raport przygotowuje się, gdy pojawiły się trudności w realizacji umowy takie jak: nieterminowa realizacja, realizacja z zastrzeżeniami generującymi obowiązek naliczenia kary umownej itp. Jednakże w art. 446 ust. 2 dopuszczono sporządzenie raportu z innych przyczyn niż wymienione w przepisach, przy czym ustawodawca katalog okoliczności, w których sporządza się raport pozostawił jako katalog otwarty. Tym samym zamawiający dysponują w tym obszarze swobodą. Dlatego też raport zawierać może również inne informacje odpowiadające dodatkowym potrzebom zamawiającego (np. w obszarze cyberbezpieczeństwa).

Obowiązek sporządzania raportu obejmuje jedynie umowy realizowane w wyniku postępowań wszczętych po 1 stycznia 2021 r. - zatem zakres danych nie jest jeszcze zbyt szeroki. Przygotowując informacje do raportu zamawiający powinni mieć jednak na względzie, że mimo, iż ustawodawca nie wskazuje wprost obowiązku jego publikacji, to dokument ten jest co do zasady jawny i jego upublicznienie nastąpić może w ramach dostępu do informacji publicznej. Dlatego też z jednej strony raport pozostaje cennym źródłem informacji, czy cyberbezpieczeństwo wpływa na sposób wykonywania zobowiązań, z drugiej jednak strony warto mieć na uwadze, że istnieją informacje, których ujawnienie może stanowić cenną wiedzę dla wrogich podmiotów planujących zaatakować infrastrukturę zamawiającego. Tym samym wypełniając raport warto się zastanowić, czy publikowanie informacji w obszarze posiadanych technologii, konfiguracji sprzętu, dat wygaśnięcia wsparcia oprogramowania jest niezbędnym elementem takiego dokumentu. Z drugiej strony jawność w pewnym aspektach jest przydatna, gdyż stanowi jasny przekaz dla wykonawców, że zamawiający stawia wymagania w obszarze cyberbezpieczeństwa i skutecznie je egzekwuje od swoich wykonawców.

Podsumowując powyższe dokumenty powinny wpisywać się w ogólną politykę zarządzania bezpieczeństwem łańcucha dostaw, w ramach której organizacja opracuje swoją własną matrycę ryzyk także w obszarze cyberbezpieczenstwa

[126] Prawo zamówień publicznych, komentarz wyd. II. pod. red. Huberta Nowaka str. 1114, https://www.gov.pl/web/uzp/komentarz-do-prawa-zamowien-publicznych [dostęp on line 12.11.2025]

łańcucha dostaw, następnie dopasuje potencjalne ryzyka do nabywanych rodzajów produktów, usług i procesów ICT, by w końcu przygotować dla nich minimalne wymogi, które zostaną zakomunikowane wykonawcom mającym zamiar realizować poszczególne zamówienia.

**Jak prawidłowo formułować wymagania wobec wykonawców**

### 3.5. Opis Przedmiotu Zamówienia

Wybór odpowiedniego produktu ICT, usługi ICT czy procesu ICT, czy też produktu z elementami cyfrowymi zależy od celu jaki przyświeca zamawiającemu, specyfiki projektu w jakim realizowany jest zakup, wymagań sprzętowych, dostępności zasobów specjalistów, czy choćby oczekiwań co do wydajności nabywanych technologii (np. Budowa systemu newralgicznego z punktu widzenia obronności i bezpieczeństwa wykreuje inne wymagania niż zamówienie obejmujące nabycie standardowego "pudełkowego" oprogramowania). Dlatego też kwestii dotyczących cyberbezpieczeństwa może być tyle, ile zamówień i niewykonalne będzie uszeregowanie oraz całkowite ujednolicenie wymogów, które będą musiały spełniać komponent ICT/ produkt z elementem cyfrowym (urządzenie, oprogramowanie, komponent). Jednakże bardzo pomocne w tym zadaniu stają się przywołane i omówione w Rozdziale II akty prawne.

Zgodnie z rekomendacjami Prezesa Urzędu Zamówień dotyczącymi zamówień publicznych na systemy informatyczne[127]:

- Rekomendacja ogólna nr 18: zamawiający powinien określić w OPZ wymagania dotyczące cyberbezpieczeństwa, jakie powinien spełniać system informatyczny.
- Rekomendacja szczegółowa nr 18.1: uwzględniając wnioski z analizy ryzyka, zamawiający powinien określić wymagania cyberbezpieczeństwa oraz określić środki konieczne do zastosowania
- Rekomendacja szczegółowa nr 18.2: zamawiający powinien określić wymagania systemu informatycznego w zakresie cyberbezpieczeństwa w sposób, który pozwoli reagować na dynamicznie zmieniające się uwarunkowania, w szczególności pojawiające się nowe, nieznane wcześniej zagrożenia

[127] Postępowanie o udzielenie zamówienia publicznego na system informatyczny Tom II, Urząd Zamówień Publicznych, grudzień 2021 r. [online] https://www.gov.pl/web/uzp/rekomendacje-dotyczace-zamowien-publicznych-na-systemy-informatyczne [dostęp 12.11.2025 r.]

- Rekomendacja szczegółowa nr 18.3: zamawiający powinien określić odpowiednie procedury na wypadek zaistnienia incydentów bezpieczeństwa.

Sformułowane powyżej zalecenia dotyczą wyłącznie systemów informatycznych, jednakże zawarte w nich wytyczne zawierają aktualne wskazówki jak formułować opis przedmiotu zamówienia, aby wpisać się w obowiązki wynikające z różnych przepisów prawnych oddziaływujących na dokumenty tworzone w trakcie udzielania zamówień publicznych.

Obowiązkiem każdej komórki organizacyjnej zamawiającego opracowującej OPZ jest uwzględnienie aspektów obejmujących cyberbezpieczeństwo w trakcie procesu udzielania zamówień publicznych. Naturalnym i niekwestionowany działaniem towarzyszącym formułowaniu opisu przedmiotu zamówienia będzie analiza:

- Czy istnieją regulacje prawne, które zobowiązują zamawiającego do stawiania szczególnych wymagań w zakresie cyberbezpieczeństwa (NIS 2, CRA, RODO),
- Czy planowane zamówienie wiąże się z zarządzaniem ryzkiem w obszarze łańcucha dostaw, (określenie jakie ryzyka mogą się zmaterialiować i jak wpłynąć na organizację)?
- Jak może wpłynąć na bezpieczeństwo organizacji zmaterializowanie się zdiagnozowanego ryzyka)?
- Jaki apetyt na ryzyko akceptuje organizacja w przypadku konkretnego zamówienia,
- Jak wskazać potencjalnym dostawcom właściwości lub niezbędne wymagania bezpieczeństwa produktu lub usługi w sposób nie naruszający zasady uczciwej konkurencji i równego traktowania wykonawców?
- Wymaganie jakich praktyk/standardów/certyfikatów w obszarze cyberbezpieczeństwa będzie z punktu widzenia opisu przedmiotu zamówienia niezbędne dla spełnienia wymagań przewidzianych w wewnętrznych politykach zarządzania cyberbezpieczeństwem?
- Jakie wymagania postawić w zakresie cyberbezpieczeństwa w obszarze przedmiotowym a jakie w obszarze podmiotowym?
- Czy należy ograniczyć ryzyko geopolityczne np. poprzez wprowadzenie preferencji dla produktów, usług, procesów ICT

świadczonych na terytorium UE czy też otworzyć się na produkty i usługi pochodzące z państw trzecich[128]?
- Jakie podzielić ryzyka w kontrakcie pomiędzy zamawiającego a wykonawcę?

Powyższe zagadnienia są jedynie przykładowymi tematami, których zbadania wymaga należyte przygotowanie opisu przedmiotu zamówienia i bardziej szczegółowo zostały rozpisane w rozdziale 4 i 5.

Jeżeli z wyników przeprowadzonej analizy wyniknie konieczność zarządzenia ryzykiem w obszarze cyberbezpieczeństwa łańcucha dostaw, kolejnym krokiem wspólnym dla każdego rodzaju zamówienia jest ustanowienie minimalnych niezbędnych wymogów, które są konieczne i stanowią nieodzowny element przedmiotu zamówienia. Zatem następnym wyzwaniem przy konstruowaniu opisu przedmiotu zamówienia z uwzględnieniem aspektów cyberbezpieczeństwa będzie ustalenie odpowiednich kryteriów wyboru i zabezpieczenie ich również odpowiednimi klauzulami umownymi np. dotyczącymi obowiązków regularnego audytowania, poddaniu się kontroli zamawiającego w obszarze spełniania obowiązku audytowego czy wprowadzenia procedury zarządzaniem incydentem (patrz Rozdział 2 OPZ/SWZ 2.1.7.1. i nast. (wymogi techniczne, funkcjonalne i bezpieczeństwa).

Wskazówki, co należy mieć na względzie formułując OPZ znaleźć można w orzecznictwie TSUE.

Trybunał w wyroku z dnia 25 października 2018 r. w sprawie C- 413/17 Roche Lietuva, ECLI:EU:C:2018:865 przypomniał, że zgodnie z art. 42 ust. 1 akapit pierwszy dyrektywy 2014/24/UE specyfikacje techniczne zdefiniowane w pkt 1 załącznika VII do tej dyrektywy, zamieszcza się w dokumentach zamówienia i określają one wymagane cechy robót budowlanych, usług lub dostaw. Natomiast w myśl art. 42 ust. 3 tej dyrektywy, specyfikacje techniczne można sformułować na kilka sposobów, bądź to w kategoriach wymagań wydajnościowych lub funkcjonalnych, bądź poprzez odniesienie do specyfikacji technicznych oraz w kolejności, co do: norm krajowych przenoszących normy europejskie, europejskich ocen technicznych, wspólnych specyfikacji technicznych, norm

[128] art. 16b ustawy Pzp

międzynarodowych, innych systemów referencji technicznych ustanowionych przez europejskie organy normalizacyjne lub – w przypadku ich braku – do norm krajowych, krajowych aprobat technicznych lub krajowych specyfikacji technicznych dotyczących projektowania, wyliczeń i realizacji robót budowlanych oraz wykorzystania dostaw, bądź też jako kombinację tych dwóch sposobów.

Tymczasem z art. 44 ust. 1 dyrektywy klasycznej wynika uprawnienie dla zamawiających do wymagania od wykonawców przedstawienia raportu z testów opracowanego przez jednostkę oceniającą zgodność lub zaświadczenia wystawionego przez taką jednostkę jako środka dowodowego potwierdzającego zgodność z wymaganiami lub kryteriami określonymi w specyfikacjach technicznych, kryteriach udzielenia zamówienia lub warunkach realizacji zamówienia. Powyższe normy europejskie znajdują odzwierciedlenie chociażby w art. 101 ustawy Pzp.

Zastosowanie efektywnych wymagań w celu zabezpieczenia łańcucha dostaw wydaje się być niezwykle skomplikowany procesem, dlatego też naprzeciw wyzwaniom, jakie napotykają zamawiający zamierzający uwzględnić aspekty cyberbezpieczeństwa w swojej polityce zakupowej wychodzi legislacja unijna i krajowa oraz cały szereg standardów szczegółowo omówionych w Rozdziale 4 i 5.

## 3.6. Kryteria oceny ofert

### 3.6.1. Rodzaje kryteriów ofert

Zgodnie z art. 239 ust. 1 ustawy Pzp Zamawiający wybiera najkorzystniejszą ofertę na podstawie kryteriów oceny ofert określonych w dokumentach zamówienia. Kryteria obok warunków udziału są podstawowymi narzędziami zamawiającego, którymi może kształtować krąg uczestników postępowania jak i przedmiot zamówienia. Przy czym oba te narzędzia wzajemnie ze sobą korespondują pozwalając zamawiającemu, ograniczyć krąg wykonawców do podmiotów, które spełniają niezbędne wymogi w pożądanym obszarze, którym w naszym wypadku będzie cyberbezpieczeństwo łańcucha dostaw. Natomiast uzupełniając warunki udziału poprzez korespondujące z nim kryteria oceny ofert zamawiający jest w stanie osiągnąć efekt kompleksowego zarządzenia ryzykami związanymi bezpieczeństwem łańcucha dostaw.

Ustawodawca nie wprowadził żadnego katalogu zamkniętego kryteriów, jakimi powinien kierować się zamawiający, wręcz odwrotnie dozwolone jest swobodne

tworzenie kryteriów oraz określanie ich wagi (znaczenia). Jednakże kryteria oceny ofert nie mogą być dowolne i uznaniowe, ich skutkiem nie może być pełna arbitralność zamawiającego w wyborze oferty. ~~Opis przedmiotu zamówienia musi być konkretny, jasny, czytelny uwzględniający zasadę równego traktowania wykonawców, zasadę proporcjonalności oraz efektywności.~~ Dopuszczalne jest jednak premiowanie preferowanych przez siebie rozwiązań, o ile jest to uzasadnione zobiektywizowanymi potrzebami, a nie chęcią wyboru konkretnego wykonawcy.
UZP wyróżniło następujące rodzaje kryteriów:

- cena i inne kryteria kosztowe;
- **kryteria jakościowe odnoszące się do jakości przedmiotu zamówienia;**
- kryteria odpowiedzialnego rozwoju obejmujące kwestie społeczne, środowiskowe oraz innowacyjność;
- kryteria kontraktowe odnoszące się do sposobu realizacji zamówienia;
- kryteria odnoszące się do personelu przewidzianego do realizacji zamówienia.

W przypadku gdy z analizy przedmiotu zamówienia, w kontekście zastosowania właściwych przepisów prawa wyznaczającego obowiązki w obszarze cyberbezpieczeństwa, wyniknie potrzeba wprowadzenia do dokumentacji postępowania rozwiązań związanych z bezpieczeństwem łańcucha dostaw, materializuje się przesłanka do zastosowania kryteriów oceny ofert preferujących bezpieczne technologie/zarządzanie/sprzęt/usługi itp., czyli kryteria powiązane z jakością przedmiotu zamówienia.

Co do zasady kryteria oceny ofert muszą być związane z przedmiotem zamówienia, przy czym związek ten nie musi być istotną cechą przedmiotu zamówienia. Kryteria mogą dotyczyć usług, dostaw lub robót budowlanych w odniesieniu do dowolnych aspektów także tych związanych z bezpieczeństwem łańcucha dostaw. Mogą też być tworzone w odniesieniu do dowolnych etapów cyklu życia, zatem także do elementów składających się na proces produkcji, dostarczania lub wprowadzania na rynek np. Oprogramowania. Zatem za pomocą jakościowych kryteriów oceny ofert można promować wgląd w proces wytwarzania oprogramowania (Secure Software Development Life Cycle (SSDLC).

W praktyce nabywanie w drodze zamówień publicznych produktów z elementem cyfrowym, czy komponentów ICT determinować będzie wprowadzenie kryteriów jakościowych związanych z cyberbezpieczeństwem. Premiować za ich pomocą można produkty, które zapewniają wymagany poziom cyberbezpieczeństwa i posiadają odpowiednią dokumentację mogącą posłużyć za dowód w postępowaniu.

Uwaga: W kontekście zamówień obejmujących aspekty cyberbezpieczeństwa na uwagę zasługuje dyspozycja art. 241 ust. 3 ustawy Pzp, zgodnie z którym kryteria oceny ofert nie mogą dotyczyć właściwości wykonawcy. Wątpliwości interpretacyjne pojawiają się w kontekście wymogu wdrożenia i utrzymania normy ISO/IEC 27001 u wykonawcy i jej interpretacji. Można spotkać się na rynku z kryteriami oceny ofert odnoszących się do tej normy. Jednakże zważywszy na jej cel oraz sposób wprowadzenia wydaje się bardziej związana z cechą właściwą wykonawcy jako podmiotu, który poprzez jej wdrożenie daje zamawiającemu swoistą gwarancję określonej kultury wewnętrznej w podejściu do zarządzania bezpieczeństwem informacji.

Podobny problem zapewne pojawi się w przypadku formułowania kryteriów wyboru dla dostaw produktów zawierających elementy cyfrowe. Wymogi CRA przewidują określone obowiązki komunikacyjne w obszarze cyberbezpieczeństwa oferowanych produktów. Tym samym wykonawcy, którym udzielono zamówienia na dostawy sprzętu bądź oprogramowania objętego CRA, będą prawnie zobowiązani wykazać się posiadaniem odpowiedniego, dedykowanego kanału kontaktu do obsługi zgłoszeń lub podatności (patrz Rozdział 2.1.7.1). Wydaje się, że tak ukształtowany obowiązek ściśle związany jest z podmiotem dostarczającym urządzenia, bądź oprogramowanie niż z samym przedmiotem zamówienia. Realizacja powyższego zobowiązania zostanie bezsprzecznie elementem opisu przedmiotu zamówienia (bez którego nie będzie możliwe należyte wykonanie np. dostaw, do których zastosowanie znajdzie w przyszłości CRA) i może zostać uzupełnione przez postawienie odpowiedniego warunku udziału w postępowaniu o udzielenie zamówienia.

Podsumowując zamawiający, który zdecyduje się posłużyć się w dokumentach zamówienia określoną normą ISO powinien dokonać dokładnej analizy, czy określa ona cechy, bez których wykonawca nie będzie dawał wystarczającej gwarancji spełnienia należycie swojego zobowiązania. Odpowiedź twierdząca

pozwala na sformułowanie w oparciu o taką normę warunku udziału w postępowaniu o udzielenie zamówienia. Jeżeli wybrany standard/norma/wytyczna dotyczy dostawy, usługi lub roboty budowlanej lub ich elementów – może stanowić jakościowe kryterium oceny ofert.

Zgodnie z poglądem panującym w doktrynie certyfikatowi ISO dotyczącemu zarządzania jakością produktu/usługi przypisuje się charakter przedmiotowych środków dowodowych, na co wskazuje choćby komentarz cytowany poniżej:
"*Przykładowo zatem dokument w formie certyfikatu (np. ISO), potwierdzający, że wykonawca wdrożył odpowiednie normy produkcyjne, co do zasady będzie podmiotowym środkiem dowodowym weryfikującym zdolność techniczną wykonawcy. Natomiast certyfikat wystawiany na konkretny produkt oferowany przez wykonawcę w konkretnym postępowaniu będzie już przedmiotowym środkiem dowodowym, służącym potwierdzeniu zgodności oferowanych dostaw, usług lub robót budowlanych z wymaganiami zamawiającego*"[129]

**Kiedy wprowadzić jakościowe kryteria oceny ofert?**
W przypadku, gdy nie jest możliwe przygotowanie szczegółowego opisu przedmiotu zamówienia za pomocą dostępnych parametrów technicznych, funkcjonalnych bądź użytkowych.

W przypadku dostaw najbardziej zalecanym kryterium oceny ofert będą parametry techniczne i jakościowe określone w postaci warunków minimalnych.

**Jak określać parametry jakościowe dostaw?** (opis oparty na zaleceniach UZP zob. Pozacenowe kryteria oceny ofert. Poradnik z katalogiem dobrych praktyk. Ver. 2.0 dostęp 12.11.2025, UZP, Warszawa https://www.gov.pl/web/uzp/pozacenowe-kryteria-oceny-ofert). )

- należy wybrać do oceny te funkcje i parametry, które są związane z bezpieczeństwem łańcucha dostaw np. zarządzanie tożsamością i dostępem, posiadanie kryteriów doboru dostawców – można rozbić na podkryteria oparte na konkretnych wymogach;
- należy wskazać, czy zamawiającemu zależy na maksymalnej wartości wybranego parametru czy też na minimalnej, jeżeli parametry mogą być

[129] A. Gawrońska-Baran [w:] E. Wiktorowska, A. Wiktorowski, P. Wójcik, A. Gawrońska-Baran, Prawo zamówień publicznych. Komentarz aktualizowany, LEX/el. 2024, art. 116.

stopniowalne np. minimalny czas zapewniania aktualizacji bezpieczeństwa (np. x lat);

- w przypadku parametrów ciągłych należy podać zakres wielkości parametru, który będzie oceniany: dolnym progiem jest wielkość postawiona w postaci warunku, natomiast górnym – wielkość optymalna, której przekroczenie staje się dla zamawiającego obojętne i nie skutkuje zwiększeniem liczby punktów przy ocenie;
- w przypadku parametrów lub funkcji ocenianych zero-jedynkowo np. posiadanie certyfikatu produktu w ramach normy CC i należy przyjąć dwuwartościową ocenę: w przypadku gdy funkcja jest oferowana – ofercie przyznawana jest określona liczba punktów, gdy nie – oferta otrzymuje zero punktów za ten parametr;
- przedmiotem oceny może być również sposób osiągania jakiejś funkcji: np. wymagane standardy konfiguracji, wprowadzenie szczególnych, związanych z przedmiotem zamówienia procedur bezpieczeństwa - każdy ze sposobów może wiązać się z inną punktacją;
- w ramach danego kryterium można uzyskać określoną liczbę punktów, należy rozdzielić pulę możliwych do uzyskania punktów między poszczególne parametry poddane ocenie;
- na koniec należy przyjąć sposób punktacji, zakładając, że zaoferowanie parametru na poziomie minimalnym skutkuje przyznaniem 0 punktów, natomiast na poziomie optymalnym – maksymalnej liczby punktów, jakie za ten parametr można uzyskać.

W przypadku usług najczęściej spotykanym kryterium oceny ofert jest doświadczenie wykonawcy zebrane w ramach jego dotychczasowej działalności. Takie kryteria nazywane są koncepcją realizacji zamówienia.
Zamawiający opisuje w SWZ niezbędny zakres informacji, który musi przedstawiać związek z cyberbezpieczeństwem łańcucha dostaw np. powiązania mogą wynikać ze standardów przejętych dla danego rodzaju usług i procesów ICT albo z norm prawnych np. NIS 2 lub rozporządzenia 2024/2847.

**Przykład:** w postępowaniu na usługi audytu zgodności z wymogami NIS 2 można przyznawać punkty za koncepcję realizacji takiego audytu. Wykonawca opisuje sposób podejścia do takiego audytu w zakresie określonym przez zamawiającego, który podaje w dokumentacji zamówienia, jakich informacji wymaga oraz sposoby oceny podejścia wykonawcy do zadania. W takim wypadku ocenie może podlegać

metoda przeprowadzenia audytu (audyt zdalny 0 pkt., audyt przeprowadzony bezpośrednio u zamawiającego x pkt. – można przy złożonych usługach tworzyć podkryteria i subkryteria), środki dojścia do celu (testy penetracyjne, analiza procedur zarządzania ryzykiem), rozplanowanie zadań w harmonogramie realizacji audytu, raportowanie zagrożeń, skład oraz kompetencje zespołu (certyfikowani audytorzy, pentesterzy z odpowiednimi kwalifikacjami.

Kolejnym kryterium oceny ofert, którym posługują się zamawiający przy kupowaniu usług i może ono znaleźć zastosowanie do zamówień z komponentami ICT, są kompetencje osób realizujących zamówienie tj. wykształcenie, szkolenia potwierdzone dyplomem ukończenia, certyfikaty, potwierdzone doświadczenie w realizacji zamówień podobnych. Zgodnie z art. 242 ust. 2 pkt 5 ustawy Pzp kryterium jakościowe może się odnosić do organizacji, kwalifikacji zawodowych i doświadczenia osób wyznaczonych do realizacji zamówienia, jeżeli mogą one mieć znaczący wpływ na jakość wykonania zamówienia. Na zamawiającym leży obowiązek precyzyjnego sfomułowania swoich wymagań i dowodów na potwierdzenie ich spełnienia, aby nie ograniczyć konkurencyjności np. poprzez wykluczenie z punktacji doświadczonego personelu ze względu na niewłaściwe określenie paramentów projektu wymaganych do wykazania doświadczenia lub błędnego opisu (zawyżonego/nieadekwatnego) stanowiska. W przypadku tego typu kryterium zamawiający mają czasami wątpliwości, czy określenie kompetencji personelu mieści się w instytucji warunku, czy też kryterium oceny ofert. Jeżeli przyjmiemy zasadę, że oba narzędzia powinny się uzupełniać z OPZ dopuszczalne jest premiowanie kompetencji zespołu przeznaczonego do realizacji zamówienia, przy czym potrzebna jest analiza, czy istnieje próg kompetencji, który jest tak istotny, że bez niego wykonawca nie będzie zdolny do należytego świadczenia usługi np. pentestów. W takim wypadku kompetencje wykonawcy będą wynikać z kompetencji zespołu.

**Kryteria kontraktowe**

Kryteria kontraktowe premiują sposób realizacji zamówienia. Najczęściej spotykanym kryterium kontraktowym jest określenie terminu. Jednakże aspekty cyberbezpieczeństwa łańcucha dostaw także winny znajdować się w umowach,

aby zapewnić ciągłość stosowania wymaganych w OPZ standardów. Dlatego też można punktować np. określone w kontrakcie i OPZ wymagania:

Deklaracja zgodności komponentów z CRA - wartość minimalna X% - wartość optymalna Y% - max. X pkt.

Proces oceny ryzyka łańcucha dostaw zgodny z ISO/IEC 27036 / ENISA - wartość minimalna 1 x na dwa lata, wartość optymalna 1 x na rok – maks. x pkt.

Udokumentowania polityka zarządzania podatnościami w łańcuchu dostaw - wartość minimalna - częściowa, wartość optymalna - pełna wraz z SLA – max. X pkt.

Podobnym mechanizmem można kształtować parametry dotyczące serwisu, pomocy technicznej, czy warunków dostaw.

Uwaga: Przy konstruowaniu warunku określającego czasy lub terminy należy przeanalizować jego adekwatność do realiów świadczenia usługi. Zbyt wyśrubowane wartości mogą spowodować problemy w realizacji umowy, gdyż będą niemożliwe do dotrzymania, wszyscy wykonawcy wpiszą maksymalne wartości i kryterium będzie pozorne lub wygrać może oferta znacznie droższa, podczas gdy różnica wartości nie będzie mieć większego znaczenia dla samej usługi.

Jakościowe kryterium oceny ofert może dotyczyć także cyklu życia produktu. Zgodnie z art. 7 pkt 2 Pzp przez cykl życia należy rozumieć wszelkie możliwe kolejne lub powiązane fazy istnienia przedmiotu dostawy, usługi lub roboty budowlanej, w szczególności badanie, rozwój, projektowanie przemysłowe, testowanie, produkcję, transport, używanie, naprawę, modernizację, zmianę, utrzymanie przez okres istnienia, logistykę, szkolenie, zużycie, wyburzenie, wycofanie i usuwanie. Zatem zamawiający, jak już wspomniano, ma możliwość premiować w postaci kryterium także wykonawców/producentów/dostawców, którzy zapewnią mu wgląd w etap projektowania oprogramowania, tworzenia technologii, koncepcji świadczenia danej usługi lub projektowania procesu ICT.

Mając na uwadze różnorodny charakter opisanych w niniejszej publikacji zamówień przytoczyć można wskazany przez UZP podział na kryteria wymierne i niewymierne.

Kryteria wymierne powinny być stosowane w przypadku, gdy dane mające być przedmiotem oceny mają postać liczbową, gdy nie może być wątpliwości czy rozbieżności w ich ocenie.

### 3.6.2. Ocena spełnienia kryteriów

Zamawiający ma prawo ocenić spełnienie kryterium jakościowego poprzez przyjęcie od wykonawców oświadczenia. Takie podejście jest przyjmowane za właściwe, jeżeli z treści oferty zamawiający jest w stanie wywnioskować wszystkie niezbędne informacje dla ustalenia sposobu realizacji zamówienia. Formularz oferty może całkowicie i kompletnie wypełniać wszelkie wymogi, gdy całe zamówienie dotyczy obszaru cyberbezpieczeństwa. Jednakże w przypadku gdy zamówienie obejmuje elementy związane z cyberbezpieczeństwem, samo oświadczenie może okazać się nieidentyfikowalnym kryterium i spowodować wybór nierzetelnego wykonawcy.

W przypadku zamówień na komponenty ICT podstawą oceny mogą być dane techniczne potwierdzające spełnianie postawionych wymagań poprzez opis parametrów technicznych bądź funkcjonalnych np. sprzętu komputerowego, oprogramowania, usługi hostingu, usługi chmurowej. Za dowody bezstronne i obiektywne przyjmuje się dokumenty zewnętrzne, wytworzone bez jakiegokolwiek udziału stron postępowania jak np. dokumentacja techniczna producenta, karty katalogowe (choć w tym wypadku zdarzają się różnice w tego typu dokumentach, które następnie są podstawą sporów sądowych między konkurującymi wykonawcami), deklaracje zgodności, przeglądy, wyniki audytów, raporty. Rozwój certyfikacji zapewne ułatwi ocenę kryteriów pozacenowych, gdy powszechnie dostępne będą specyfikacje techniczne opisane w art. 2 pkt 20 Rozporządzenia 2019/881 - dokumenty określające wymogi techniczne, które mają być spełnione przez produkt ICT, usługę ICT, proces ICT lub usługę zarządzaną w zakresie bezpieczeństwa lub procedury oceny zgodności w odniesieniu do produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa.

Uwaga: Należy zwrócić uwagę, aby przygotowując dokumentację przetargową nie posługiwać się linkami, a w przypadku zmieniających się w okresie czasu wartości

określić dzień, z którego informacje o danym parametrze, będą właściwe przy ocenie ofert.

Podstawą oceny oferty może zostać ocena próbki. Do dokumentacji postępowania można wprowadzić kryterium jakościowe polegające na prezentacji wymaganego przez zamawiającego np. sprzętu, ale także prezentacji oprogramowania/prezentacji systemu komputerowego. Jednakże zamawiający jest zobowiązany do jasnego wskazania sposobu oceny takiej próbki w duchu zasad równego traktowania wykonawców i zachowania uczciwej konkurencji. Precyzyjna procedura przyjęcia i oceny próbki jest niestety często bardzo czasochłonna dla zamawiających, którzy koncentrują się, aby w roku budżetowym prowadzić przede wszystkim sprawnie postępowania i zdążyć odebrać sprzęt/system. Powyższe stanowi czynnik zniechęcający zamawiających do konstruowania dodatkowych dokumentów postępowania tj. zasady oceniania próbek, mimo że żądanie próbek należy uznać za praktykę pozwalającą na rzetelną ocenę oferowanego przedmiotu zamówienia.

Personel proponowany w ofercie, którym wykonawca zamierza posłużyć się przy realizacji zamówienia można poddać próbie wiedzy w zakresie cyberbezpieczeństwa. Zazwyczaj odbywa się ona w siedzibie zamawiającego, jednakże w zależności od rodzaju świadczenia w dobie cyfryzacji wydaje się możliwe korzystanie z kanałów komunikacji elektronicznej oraz aplikacji umożliwiającej prowadzenie zdalnych testów. Taka próba wiedzy może polegać na rozwiązaniu testu, w przypadku gdy zamawiana jest usługa, która wiąże się z przekazywaniem wykonawcy wrażliwych informacji. Można przetestować wiedzę personelu w zakresie higieny cyfrowej. W rozmowie kwalifikacyjnej można przetestować wiedzę audytora. Pentesterzy mogą rozwiązywać przygotowane dla nich zadania specjalne.

Ważne jest, aby zapewnić wszystkim uczestnikom takie same warunki uczestnictwa, gdyż tylko w ten sposób zachowana zostanie zasada bezstronności i obiektywizmu oceny.

Kolejnym elementem prawidłowo przygotowanej dokumentacji postępowania o zamówienie publiczne jest wskazanie minimalnego poziomu jakościowego,

poniżej którego dojdzie do odrzucenia oferty. Powyższe zastrzeżenie pozwala wyeliminować z postępowania oferty tych wykonawców, którzy w żadnej mierze nie są w stanie zagwarantować wymaganego poziomu realizacji zamówienia.

### 3.7. Warunki udziału w postępowaniu

Kwestie bezpieczeństwa muszą stać się integralną częścią procesu zamówieniowego i uzyskać wpływ na wybór odpowiedniego wykonawcy. W celu zapewnienia minimalnych standardów w obszarze bezpieczeństwa łańcucha dostaw należy przyglądać się standardom cyberbezpieczeństwa spełnianym przez wykonawców i podwykonawców. W świetle przedstawionych we wcześniejszych rozdziałach zagrożeń, które czyhają w obszarze łańcucha dostaw, tylko świadomy i przygotowany wykonawca jest w stanie wykonać świadczenia bez narażania zamawiającego na zbędne ryzyka (nigdy nie będzie to całkowite bezpieczeństwo).

W celu udzielenia zamówienia publicznego podmiotom, które dają najlepszą rękojmię należytej staranności w zabezpieczeniu łańcucha dostaw przed incydentami, warto w każdym zamówieniu, zwłaszcza dotyczącym produktów ICT, zdefiniować krąg wykonawców, którzy mogą ubiegać się o zamówienie poprzez sformułowanie kryteriów kwalifikacji potwierdzających stosowanie najlepszych praktyk zarządzania ryzkiem w obszarze cyberbezpieczeństwa. Powyższe działania wpisują się w wynikający z dyrektywy NIS 2 obowiązek, zgodnie z którymi podmioty kluczowe oraz ważne będą zobowiązane do wprowadzenia adekwatnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, wykorzystywanych przez nie do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu. Postawienie potencjalnym wykonawcom warunków udziału w postępowaniu odnoszących się do ich cyberbezpieczeństwa pozostaje doskonałym instrumentem realizującym ten wymóg, jednak musi pozostawać w zgodzie z wytycznymi zawartymi w art. 112 ust. 1 ustawy Pzp, według których zamawiający określa warunki udziału w postępowaniu w sposób proporcjonalny do przedmiotu zamówienia oraz umożliwiający ocenę zdolności wykonawcy do należytego wykonania zamówienia, w szczególności wyrażając je jako minimalne poziomy zdolności. Wskazane minimalne poziomy zgodności mają zapewnić wybór wykonawcy zdolnego do realizacji zamówienia i jednocześnie

zagwarantować dochowanie zasady uczciwej konkurencji i równego traktowania wykonawców. Innymi słowy kreując warunki w postępowaniu o udzielenie zamówienia publicznego zamawiający musi kierować się jedną z fundamentalnych zasad systemu zamówień publicznych – zasadą proporcjonalności.

W dyrektywie NIS 2 unijny ustawodawca nieprzypadkowo podkreślił w motywie 16, że "środki bezpieczeństwa powinny być proporcjonalne do zagrożeń, na jakie narażone są sieci i systemy informatyczne, oraz do znaczenia tych systemów dla społeczeństwa." Powyższe regulacje jednoznacznie wskazują na nakaz podejścia do udzielania zamówienia w sposób elastyczny i adekwatny do jego rodzaju i skali.
*Przykład:*
*Inne warunki muszą zostać postawione małej firmie, która nie będzie miała szerokich dostępów do infrastruktury zamawiającego, będzie realizowała zamówienia generujące minimalne lub nawet żadne ryzyko w obszarze zarządzania cyberbezpieczeństwem, a inne dostawcy oprogramowania do zarządzania infrastrukturą krytyczną zamawiającego.*
Nieprzypadkowe posługiwanie się w dyrektywie NIS 2 i dyrektywie klasycznej zasadą proporcjonalności jest wskazówką, że dotychczasowy dorobek orzecznictwa oraz doktryny znajdzie zastosowanie przy formułowaniu prawidłowych warunków udziału w postępowaniu o udzielenie zamówienia na usługi, dostawy, czy systemy ICT. Oba akty prawne należy traktować jako jeden spójny system.

Przenosząc zasadę proporcjonalności na obszar zamówień komponentów ICT, należy podkreślić obowiązek powiązania przedmiotu zamówienia ze stawianym warunkiem w postępowaniu oraz jego zakresem. Przy czym adekwatność tego powiązania powinna odzwierciedlać się zarówno w charakterze warunku, czyli jego treści, jak również w jego proporcji w sensie matematycznym. Jak wskazano w Procesie udzielania zamówień publicznych na podstawie nowego Prawa zamówień publicznych pod red. Małgorzaty Śledziewskiej: "Sama wartość wykonywanych przez wykonawców zamówień może nieść informacje na temat doświadczenia i zdolności wykonawców[130].

[130] Śledziewska, M. (red.), Adamiec, K., Jędrzejczyk, A., Matuszewska, A., Tarnowska, B. „Proces udzielania zamówień publicznych na podstawie nowego Prawa zamówień publicznych. Komentarz praktyczny z orzecznictwem", Wydawnictwo C.H. Beck, Warszawa, s. 289.

Warunek postawiony w zakresie wymogów cyberbezpieczeństwa nie może prowadzić do wyeliminowania wykonawców zdolnych wykonać zamówienie w sposób należyty poprzez np. określenie zbyt wysokiego wymagania wobec zamierzonego efektu.
*Przykład - wymóg wobec wykonawcy w postępowaniu o udzielenie zamówienia na dostawę pucharów na lokalne zawody sportowe, wdrożenia w swojej organizacji normy ISO 2700-1*.
Podany przykład jest oczywiście jaskrawym naruszeniem i pozostaje oczywiście nieadekwatny zarówno ze względu na brak powiązania przedmiotu zamówienia z obszarem cyberbezpieczeństwa, jak również skalę zamówienia, jego charakter i sposób realizacji, jednak daje pewien pogląd na relacje pomiędzy zakresem zbudowania cyberodporności zamawiającego a realiami rynku. Natomiast podany powyżej warunek nie wydawałby się już nadmiarowy wobec wykonawcy, który miałby świadczyć na rzecz zamawiającego usługi ICT, które pozwalałyby wykonywać pentesty oprogramowania należącego do infrastruktury krytycznej państwa, czy na dostęp i poznanie budowy architektury IT newralgicznych systemów zamawiającego.

Przy wyznaczaniu warunków udziału w postępowaniu o udzielenie zamówienia, które dotyczą co do zasady właściwości wykonawcy w obszarze cyberbezpieczeństwa uwzględniane mogą być np. elementy dotyczące potencjału technicznego, wykształcenia kadry zarządzającej, personelu realizującego zamówienie, całości personelu wykonawcy, kwalifikacji zawodowych itp. Wszystkie powyższe właściwości mieszczą się w pojęciu „zdolności technicznych lub zawodowych”. Jednak jak podkreślił TSUE w wyroku z dnia 1 marca 2018 r. w sprawie C-9/17 Maria Tirkkonen przeciwko Maaseutuvirasto, ECLI:EU:C:2018:142 za ,,kryteria udzielenia zamówienia” nie można uznać kryteriów, które nie prowadzą do wyboru najkorzystniejszej ekonomicznie oferty, lecz służą jedynie ocenie zdolności oferentów do realizacji zamówienia. Tym samym warunki w obszarze cyberbezpieczeństwa łańcucha dostaw muszą zezwolić z jednej strony na selekcję w celu zawarcia kontraktu z wykonawcą zarządzającym swoim cyberbezpieczeństwem w sposób należyty i jednocześnie umożliwić wybór oferty racjonalnej ekonomicznie.

Tym samym można się zastanawiać, jak rozpoznać takiego wykonawcę i jak skutecznie go wybrać. Najogólniej rzecz ujmując bezpieczny wykonawca:

- nie figuruje na liście podmiotów wysokiego ryzyka, ani żadnej liście dostawców objętych ustawowym zakazem lub podobnym ograniczeniem w działalności,
- dokłada należytej staranności przy weryfikacji podmiotów, z którymi współpracuje, audytuje siebie i wymaga też audytów od swoich podwykonawców,
- monitoruje w sposób nieprzerwany dostęp do posiadanych informacji, aby zapobiegać nieuprawnionemu dostępowi do danych i procedur,
- kładzie duży nacisk u siebie i swoich podwykonawców na edukacje i regularne szkolenia z higieny cyfrowej, zarządzania ryzykiem, ochrony informacji,
- potrafi właściwie działać w trakcie incydentu zarówno u siebie jak i zamawiającego, jak również posiada procedury i wiedzę, jak poradzić sobie ze skutkami incydentu.

Jedną z przykładowych praktyk, które świadczą o dojrzałym i odpowiedzialnym podejściu wykonawców do kwestii cyberbezpieczeństwa będzie:

- wdrożenie w organizacji polityki bezpieczeństwa zarządzaniem informacjami,
- prowadzenie przez wykonawcę i wymaganie od swoich podwykonawców regularnych audytów bezpieczeństwa IT,
- zawieranie z podwykonawcami umowy o zachowaniu w poufności (NDA-Non disclosure agreement),
- Wymagania, aby audyty u siebie i podwykonawców były prowadzone przez osoby posiadające stosowne kwalifikacje i doświadczenie (np. poprzez posiadanie certyfikatu audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 lub w zależności od potrzeb innych certyfikatów tj. Certified Internal Auditor (CIA), Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified in the Governance of Enterprise IT (CGEIT), Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP), Certified Reliability Professional, Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert, lub równoważny, w obszarze pentestów natomiast to OSCP (Offensive Security Certified Professional),OSCE (Offensive Security Certified Expert), GXPN (GIAC Exploit Researcher and Advanced Penetration Tester), CEH (EC-Council Certified Ethical Hacker), eLearnSecurity Web application Penetration Tester (eWPT). Przy czym należy zwrócić uwagę także na jakość audytu. Jak pokazuje doświadczenie na rynku przybywa podmiotów świadczących usługi audytorskie, jednak ich doświadczenie w tym zakresie nie zawsze jest weryfikowane przez zamawiających (uwagę zamawiającego

powinno przykuć stosowanie przy nabywaniu powyższych usług jedynie kryterium ceny lub wymaganie zbyt małej liczby certyfikowanego personelu w odniesieniu do wielkości badanego podmiotu).

- Przeprowadzanie audytów regularnie min. co 12 miesięcy,
- Audyty dostosowane do rodzaju i skali działalności (**Uwaga:** audyty zdalne nie będą wystarczające dla każdego rodzaju prowadzonego przedsiębiorstwa, raczej dopuszczalne są w mniejszych podmiotach),
- Prowadzenie testów penetracyjnych w obecności pracownika,
- Wdrożenie polityki zarządzania cyberincydentami,
- Posiadanie planu zarządzenia organizacją w przypadku udanego cyberataku uszkadzającego infrastrukturę, wykradającego dane itp.,
- Posiadanie w pełni dostępnej, pierwszej linii wsparcia o wysokiej responsywności,
- Posiadanie procedur dotyczących wykrywania i utraty lub modyfikacji danych.

**Uwaga**: Powyższe wymagania są przykładowe i znajdują swoje rozszerzenie w Rozdziele 4 i 5.

Wyzwaniem po stronie zamawiających będzie takie sformułowanie warunków udziału w postępowaniu i sprzężonych z nimi postanowień umownych, aby dopuścić do postępowania jedynie odpowiedzialnych wykonawców. Zadanie to wydaje się być pracochłonne zarówno w wymiarze kontroli podmiotowych środków dowodowych, jak i późniejszemu weryfikowaniu u wykonawcy postawionych wymogów w trakcie trwania umowy, dlatego też może rodzić pokusę rezygnowania ze stawiania warunków udziału w postępowaniu i oparciu swoich wyborów wyłącznie o kryterium ceny. Takie podejście owszem skraca procedurę udzielenia zamówienia i gwarantuje wybór najtańszej oferty, ale wprowadza ryzyko prawne zaniedbywania obowiązków wynikających z przepisów NIS 2 i rozporządzenia 2024/2690. Należy mieć na względzie, że w przypadku skutecznego cyberataku, gdy dojdzie do zniszczenia infrastruktury zamawiającego w wyniku zaniedbań wykonawcy w obszarze cyberbezpieczeństwa, odpowiedź na pytanie “za jaką cenę zamawiający zakupił dany proces ICT” będzie “za zbyt wysoką”, gdyż straty zapewne wielokrotnie przewyższą oszczędności wynikające z wyboru najtańszej oferty.

Warunki, które pomogą w sposób realny wpływać na wybór wykonawców starannie zarządzających ryzykiem w obszarze cyberbezpieczeństwa dotyczyć

będą najczęściej zdolności technicznych lub zawodowych wykonawców (art. 112 ust. 2 pkt 4 ustawy Pzp). Polski ustawodawca zezwolił zamawiającym w myśl § 9 pkt 5 - 7 rozporządzenia w sprawie podmiotowych środków dowodowych na żądanie w celu potwierdzenia spełniania przez wykonawcę warunków udziału w postępowaniu lub kryteriów selekcji dotyczących zdolności technicznej lub zawodowej:

- wykazu systemów zarządzania łańcuchem dostaw i śledzenia łańcucha dostaw, które wykonawca będzie mógł zastosować w celu wykonania zamówienia publicznego;
- oświadczenia o wyrażeniu zgody na przeprowadzenie kontroli zdolności produkcyjnych lub zdolności technicznych wykonawcy, a w razie konieczności także dostępnych mu środków naukowych i badawczych, jak również środków kontroli jakości, z których wykonawca będzie korzystać - w przypadku gdy przedmiot zamówienia obejmuje produkty lub usługi o złożonym charakterze lub w szczególnie uzasadnionych przypadkach w odniesieniu do produktów lub usług o szczególnym przeznaczeniu;
- oświadczenia na temat wykształcenia i kwalifikacji zawodowych wykonawcy lub kadry kierowniczej wykonawcy.

Tym samym zamawiający mają już teraz podstawy prawne do realizacji swoich obowiązków w obszarze cyberbezpieczeństwa łańcucha dostaw poprzez ustalenie adekwatnych i proporcjonalnych warunków, których weryfikacja może nastąpić poprzez przedłożenie określonych powyżej podmiotowych środków dowodowych. Katalog podmiotowych środków dowodowych obejmuje ponadto również certyfikaty, raporty, procedury, protokoły, na podstawie których jest zdolny do ukształtowania kręgu wykonawców uwzględniając ich poziom bezpieczeństwa, co zostało już omówione w Rozdziale 2.

**Przykład I**

Wyzwaniem po stronie zamawiających będzie takie sformułowanie warunków udziału w postępowaniu i sprzężonych z nimi postanowień umownych, aby dopuścić do postępowania jedynie odpowiedzialnych wykonawców. Zadanie to wydaje się być pracochłonne zarówno w wymiarze kontroli podmiotowych środków dowodowych, jak i późniejszemu weryfikowaniu u wykonawcy postawionych wymogów w trakcie trwania umowy, dlatego też może rodzić pokusę rezygnowania ze stawiania warunków udziału w postępowaniu i oparciu swoich wyborów wyłącznie o kryterium ceny lub kryterium ceny w połączeniu z

kryterium prostym, znanym zamawiającemu (np. termin dostawy), ale niepowiązanym z żadnym aspektem ochrony cyberbezpieczeństwa łańcucha dostaw. Takie podejście owszem skraca procedurę udzielenia zamówienia i gwarantuje wybór tańszej oferty, ale wprowadza ryzyko prawne zaniedbywania obowiązków wynikających z przepisów NIS 2 i rozporządzenia 2024/2690. Należy mieć na względzie, że w przypadku skutecznego cyberataku, gdy dojdzie do zniszczenia infrastruktury zamawiającego w wyniku zaniedbań wykonawcy w obszarze cyberbezpieczeństwa, odpowiedzią na pytanie "za jaką cenę zamawiający zakupił dany produkt ICT" będzie "za zbyt wysoką". Poniesione straty mogą wielokrotnie przewyższyć oszczędności wynikające z wyboru oferty, dokonanego z pominięciem kryteriów jakościowych dotyczących bezpieczeństwa.

Warunki, które pomogą w sposób realny wpływać na wybór wykonawców starannie zarządzających ryzykiem w obszarze cyberbezpieczeństwa dotyczyć będą najczęściej zdolności technicznych lub zawodowych wykonawców (art. 112 ust. 2 pkt 4 ustawy Pzp). Polski ustawodawca zezwolił zamawiającym w myśl § 9 ust. 1 rozporządzenia w sprawie podmiotowych środków dowodowych zażądać dowodów, którzy pozwolą ograniczyć ryzyko współpracy z wykonawcą nie dającym wystarczającej rękojmi w obszarze cyberbezpieczeństwa łańcucha dostaw. W celu potwierdzenia spełniania przez wykonawcę warunków udziału w postępowaniu lub kryteriów selekcji dotyczących zdolności technicznej lub zawodowej, które mogą znaleźć skuteczne zastosowanie w omawianej materii jest m in.:

- wykaz osób, skierowanych przez wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za świadczenie usług, kontrolę jakości lub kierowanie robotami budowlanymi, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami - § 9 ust. 1 pkt 3 – w przypadku zamówień, gdy personel wyznaczony do realizacji umowy będzie miał dostęp do systemów ICT w sposób mogący mieć realny wpływ na jego funkcjonowanie, będzie świadczył usługę pentestów, będzie miał wpływ na jakość i bezpieczeństwo świadczonych przez zamawiającego usług publicznych – przykładowo certyfikaty posiadane przez pentesterów, audytorów, kierowników projektów,
- opis urządzeń technicznych oraz środków organizacyjno-technicznych stosowanych przez wykonawcę w celu zapewnienia jakości oraz opisu

zaplecza naukowo-badawczego wykonawcy (§ 9 ust. 1 pkt 4), w sytuacji gdy urządzenia, środki lub zaplecze mogą np. stanowić potencjalny wektor ataku na świadczone przez zamawiającego usługi publiczne np. raporty, procedury;

- wykaz systemów zarządzania łańcuchem dostaw i śledzenia łańcucha dostaw, które wykonawca będzie mógł zastosować w celu wykonania zamówienia publicznego (§ 9 ust. 1 pkt 5);
- oświadczenie o wyrażeniu zgody na przeprowadzenie kontroli zdolności produkcyjnych lub zdolności technicznych wykonawcy, a w razie konieczności także dostępnych mu środków naukowych i badawczych, jak również środków kontroli jakości, z których wykonawca będzie korzystać - w przypadku gdy przedmiot zamówienia obejmuje produkty lub usługi o złożonym charakterze lub w szczególnie uzasadnionych przypadkach w odniesieniu do produktów lub usług o szczególnym przeznaczeniu;
- w przypadku dostarczania produktów:
    a) próbki, opisy lub fotografie dostarczanych produktów, których autentyczność musi zostać poświadczona przez wykonawcę na żądanie zamawiającego,
    b) zaświadczenie niezależnego podmiotu uprawnionego do kontroli jakości potwierdzającego, że dostarczane produkty odpowiadają określonym normom lub specyfikacjom technicznym.

Tym samym zamawiający mają już teraz podstawy prawne do realizacji swoich obowiązków w obszarze cyberbezpieczeństwa łańcucha dostaw poprzez ustalenie adekwatnych i proporcjonalnych warunków, których weryfikacja może nastąpić poprzez przedłożenie określonych podmiotowych środków dowodowych~~. Katalog podmiotowych środków dowodowych obejmuje ponadto również certyfikaty, raporty, procedury, protokoły, na podstawie których jest zdolny do ukształtowania kręgu wykonawców uwzględniając ich poziom bezpieczeństwa, co zostało już omówione w Rozdziale 2.~~

Przykładowe oświadczenie

**OŚWIADCZENIE WYKONAWCY**

(dotyczące systemu zarządzania bezpieczeństwem informacji)

Ja, niżej podpisany/a, działając w imieniu i na rzecz:

**Nazwa Wykonawcy:** .....

**Adres siedziby:** .....

**NIP:** ..... **REGON:** .....

oświadczam, że:

☐ Posiadam wdrożony system zarządzania bezpieczeństwem informacji zgodny z normą ISO/IEC 27001, potwierdzony aktualnym certyfikatem wydanym przez akredytowaną jednostkę certyfikującą.

**Lub**

☐ Posiadam równoważny system zarządzania bezpieczeństwem informacji, który spełnia następujące cechy:

1. Formalnie przyjęta polityka bezpieczeństwa informacji.
2. System identyfikacji i oceny ryzyk związanych z przetwarzaniem informacji.
3. Procedury zarządzania dostępem do informacji.
4. Środki ochrony fizycznej i technicznej infrastruktury.
5. Procedury reagowania na incydenty bezpieczeństwa.
6. Szkolenia pracowników w zakresie bezpieczeństwa informacji.
7. Audyty wewnętrzne lub zewnętrzne weryfikujące skuteczność systemu.
8. Mechanizmy ciągłego doskonalenia systemu ochrony informacji.

Zobowiązuję się do przedstawienia na żądanie Zamawiającego dokumentacji potwierdzającej spełnienie powyższych wymagań.

..... **(miejscowość, data)**

..... **(podpis Wykonawcy)**

W zależności od przedmiotu zamówienia i wymagań niezbędnych dla zachowania zasady proporcjonalności i efektywności, zamawiający jako podmiotowych środków dowodowych może wymagać opisów procedur lub polityk przyjętych i utrzymywanych przez wykonawców w zakresie bezpieczeństwa łańcucha dostaw dotyczących np.:

- Zarządzania aktualizacjami - § 9 ust. 1 pkt 4 – rozporządzenia w sprawie podmiotowych środków dowodowych,
- Weryfikacji podwykonawców - § 9 ust. 1 pkt 5 - rozporządzenia w sprawie podmiotowych środków dowodowych,

- Reagowania na incydenty § 9 ust. 1 pkt 4 - rozporządzenia w sprawie podmiotowych środków dowodowych,

**Uwaga**: Powyższy projekt ma charakter ogólny i przykładowy, nie uwzględnia w swojej treści wykonawców wspólnie ubiegających się o udzielenie zamówienia, ani podwykonawstwa, a w przypadku usługi kolokacji kwestia ta może mieć istotny wpływ na dodatkowe wymogi w dokumentacji zamówienia. W przypadku gdy wykonawca właśnie w tym obszarze powołuje się na zasoby podmiotu trzeciego, może powstać wątpliwość, jaką część zamówienia realnie wykonuje, gdyż w przypadku usługi kolokacji cechy realnie i bezpośrednio wykonującego świadczenie są istotą gwarancji bezpieczeństwa. Dlatego też w warunkach udziału w postępowaniu warto wskazywać, że warunek posiadania ważnego certyfikatu ISO 27001 lub równoważnego dotyczy podmiotu, który będzie odpowiedzialny za zapewnienie budynku dla usług kolokacji.

**Przykład II**

Kolejnym warunkiem, który można postawić w postępowaniu o udzielenie zamówienia publicznego, związanym z zapewnieniem cyberbezpieczeństwa jest w przypadku zamówień z dziedziny obronności i bezpieczeństwa żądanie posiadania i przedłożenia odpowiedniego poświadczenia bezpieczeństwa przemysłowego.

Zamawiający uzna warunek za spełniony, jeżeli wykonawca wykaże, że posiada świadectwo bezpieczeństwa przemysłowego co najmniej III stopnia i przekaże zamawiającemu następujące dokumenty według listy poniżej:

1. Poświadczona za zgodność z oryginałem kopia świadectwa bezpieczeństwa przemysłowego co najmniej trzeciego stopnia, potwierdzająca zdolność wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia oraz znanych na tym etapie podwykonawców (przez które Zamawiający rozumie również podmioty udostępniające zasoby) do ochrony informacji niejawnych o klauzuli co najmniej „poufne”, wydanego przez Agencję Bezpieczeństwa Wewnętrznego (ABW) lub Służbę Kontrwywiadu Wojskowego (SKW). Kopia świadectwa powinna być poświadczona za zgodność z oryginałem przez osobę uprawnioną do reprezentowania wykonawcy lub podwykonawcy, w sposób umożliwiający identyfikację podpisu.

2. Wykaz pracowników wyznaczonych do realizacji umowy, którzy w trakcie jej wykonywania mogą mieć dostęp do informacji niejawnych, w tym także:

- osoby uprawnionej do podpisania umowy,

- oraz Pełnomocnika ds. Ochrony Informacji Niejawnych (Pełnomocnika OIN) wykonawcy.

3. Poświadczone za zgodność z oryginałem przez osobę uprawnioną do reprezentowania wykonawcy, w sposób umożliwiający identyfikację podpisu, kopie poświadczeń bezpieczeństwa oraz aktualnych zaświadczeń o odbytym szkoleniu w zakresie ochrony informacji niejawnych.

4. Oświadczenie wykonawcy o zobowiązaniu wszystkich pracowników oraz podwykonawców do zachowania poufności i ochrony informacji niejawnych, które zostaną im udostępnione lub które mogą pozyskać w trakcie postępowania albo realizacji zamówienia.

**Przykład III**

Szczególnie podatne na ryzyka związane z bezpieczeństwem łańcucha dostaw są usługi MSP (Managed Service Provider) i MSSP (Managed Security Service Provider). Przykładami takich usług są:

MSP

- Zarządzanie siecią i serwerami – konfiguracja, monitoring, aktualizacje
- Helpdesk i wsparcie użytkowników – zdalna pomoc techniczna
- Zarządzanie urządzeniami końcowymi – komputery, laptopy, drukarki
- Backup i odzyskiwanie danych – automatyczne kopie zapasowe
- Zarządzanie chmurą – np. Microsoft 365, Azure, AWS

MSSP

- Monitoring bezpieczeństwa (SOC) – wykrywanie i reagowanie na zagrożenia
- Zarządzanie zaporami sieciowymi (firewall) – konfiguracja i kontrola dostępu
- Systemy antywirusowe i EDR/XDR – ochrona punktów końcowych
- Testy penetracyjne i audyty – sprawdzanie podatności systemów
- Zgodność z regulacjami – RODO, ISO 27001, NIS2;

Zamawiający, którzy chcą zapewnić sobie sprawne działanie IT, a nie mają do tego wystarczających zasobów i nabywają od zewnętrznych dostawców tego typu usługi, muszą zwrócić szczególną uwagę na zarządzenie ryzykami w obszarze łańcucha dostaw, gdyż najpoważniejsze incydenty związane są przede wszystkim z tymi usługami.

**Przykładowe ogólne brzmienie warunku dla MSP (zarządzanie siecią i serwerami):**

"Zamawiający uzna, że warunek został spełniony, jeżeli wykonawca wykaże, że:

W ciągu ostatnich 3 lat przed upływem terminu składania ofert / wniosków o dopuszczenie do udziału w postępowaniu (a jeżeli okres prowadzenia działalności jest krótszy — w tym okresie) należycie wykonał co najmniej:

a. jedną usługę zarządzania infrastrukturą IT (sieciową lub serwerową), obejmującą elementy konfiguracji, monitoringu i aktualizacji systemów,
b. w której wdrożono lub utrzymywano mechanizmy zapewnienia bezpieczeństwa łańcucha dostaw, takie jak:
    i. weryfikacja źródeł pochodzenia komponentów oprogramowania,
    ii. stosowanie repozytoriów kontrolowanych lub podpisów cyfrowych przy aktualizacjach,
    iii. audyt bezpieczeństwa dostawców lub podwykonawców IT. (...)."

Oczywiście zarówno okres świadczenia usług, jak również liczba wykonanych usług powinny być proporcjonalne wobec przedmiotu zamówienia. Na zamawiającym ciąży zawsze obowiązek konkretyzacji warunku udziału poprzez opis sposobu oceny warunku, czyli wskazanie kryteriów, jakimi będzie się kierował zamawiający przy ocenie spełniania warunku.

Przykładowe podmiotowe środki dowodowe, których Zamawiający mogą wymagać dla spełnienia warunku zgodnie z § 9 ust. 1 pkt 2 rozporządzenia w sprawie podmiotowych środków dowodowych to:

- Wykaz usług - potwierdzający wykonanie co najmniej x usług/i zarządzania infrastrukturą IT (sieciową lub serwerową) obejmującej konfigurację, monitoring, aktualizacje i elementy bezpieczeństwa łańcucha dostaw,
- Referencje - potwierdzające należyte wykonanie usług,

- Protokoły odbioru - wskazujące, że doszło do odbioru świadczenia bez uwag i bez kar umownych,
- Inne dokumenty, wystawione przez podmiot, na rzecz którego usługa była świadczona.

**Przykładowe ogólne brzmienie warunku dla MSSP (testy penetracyjne i audyty):**

Zamawiający uzna warunek za spełniony, jeżeli wykonawca wykaże, że dysponuje lub będzie dysponować osobami skierowanymi przez wykonawcę do realizacji umowy, o odpowiednich kwalifikacjach zawodowych, uprawieniach, doświadczeniu i wykształceniu, odpowiednimi do funkcji, jakie zostaną im powierzone, tj.:

1) minimum x osobami do pełnienia funkcji testerów bezpieczeństwa, które powinny się cechować następującymi kompetencjami:

2) w ciągu ostatnich x miesięcy przed dniem składania ofert/wniosków o dopuszczenie do udziału w postępowaniu, tworzyły plany testów i scenariuszy testowych oraz przeprowadzała testy poniższymi metodykami:

- Blackbox,
- Whitebox,
- Greybox

3) posiadają co najmniej jeden z niżej wymienionych certyfikatów:

- Offensive Security Wireless Professional (OSWP)

- Offensive Security Certified Expert (OSCE),

- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN),

- eLearnSecurity Web application Penetration Tester (eWPT),

- eLearnSecurity Web application Penetration Tester eXtreme (eWPTX),

- eLearnSecurity Mobile Application Penetration Tester (eMAPT),

- OSCP (Offensive Security Certified Professional

lub równoważny certyfikat wystawiony przez niezależny od wykonawcy podmiot.

Na potwierdzenie spełnienia powyższego warunku wykonawca przedstawi wykaz osób wyznaczonych do pełnienia funkcji testerów bezpieczeństwa wraz z wykazem posiadanych certyfikatów i poświadczonych za zgodność z oryginałem kopii certyfikatów.

## 3.8. Inne instrumenty prawne, którymi może posługiwać się zamawiający formułując dokumenty zamówienia w celu mitygacji zdiagnozowanego ryzyka

### 3.8.1 Ograniczenie udziału podmiotów spoza UE

Skomplikowana sytuacja geopolityczna może mieć wpływ na cyberbezpieczeństwo łańcucha dostaw ze względu na kraj pochodzenia procesu ICT, usługi ICT, produktu ICT. Dlatego też warto w trakcie analizy zdiagnozowanych ryzyk uwzględnić najnowsze możliwości, jakie daje nowelizacja ustawy Pzp wprowadzająca do polskiego porządku prawnego linię orzeczniczą TSUE opartą o wyroki w sprawach o sygnaturach C-652/22 i C-266/22. Na podstawie ustawy z dnia 9 lipca 2025 r. (Dz.U.2025.1165) zmieniającej ustawę Pzp z dniem 9 września 2025 r., przyznano wykonawcom pochodzącym z państw trzecich będących stronami Porozumienia Światowej Organizacji Handlu w sprawie zamówień rządowych lub innych umów międzynarodowych gwarantujących na zasadzie wzajemności i równości dostęp do rynku zamówień publicznych, których stroną jest Unia Europejska równe prawa w dostępie do unijnego rynku w zakresie objętym tym porozumieniem. Oczywiście głównym celem zmiany jest możliwość ograniczenia dostępu o polskiego rynku zamówień publicznych wykonawcom z państw trzecich, które nie są stroną Porozumienia Światowej Organizacji Handlu i nie zawarły z Unią Europejską porozumień o wzajemnej liberalizacji dostępu do rynku zamówień publicznych, lub robót budowlanych, dostaw i usług pochodzących z tych państw trzecich, jednakże nie można nie zauważyć, że zamawiający ma także możliwość ograniczania dostępu do zamówienia podmiotom generującym ryzyko geopolityczne np. wynikające ze znalezienia podejrzanych komponentów w sprzęcie/oprogramowaniu a nieujawnionych w dokumentacji technicznej lub eliminowaniu podmiotów, które nie poddają weryfikacji procesu wytwarzania swojego oprogramowania. Kompleksowa ochrona łańcucha dostaw winna uwzględniać różne ryzyka, przy czym często te geopolityczne potrafią iść w parze z protekcjonistyczną polityką poszczególnych państw względem swojego rynku i rodzimych produktów.

Podobne podejście w zakresie ograniczania dostępu do rynku UE znajdziemy w przypadku zamówień realizowanych w ramach programu „Cyfrowa Europa". W przypadku konieczności ochrony informacji newralgicznych, podmioty prawne mające siedzibę w państwach stowarzyszonych i podmioty prawne, które mają siedzibę w Unii Europejskiej, lecz są kontrolowane z państwa trzeciego, nie kwalifikują się do uczestnictwa we wszystkich lub niektórych działaniach w ramach celu szczegółowego nr 3, jeśli istnieją należycie uzasadnione względy bezpieczeństwa. W takich przypadkach zaproszenia do składania wniosków i zaproszenia do składania ofert ogranicza się do grona podmiotów prawnych mających siedzibę lub uznanych za mające siedzibę w państwach członkowskich i kontrolowanych przez państwa członkowskie lub obywateli państw członkowskich[131].

Jeszcze innym instrumentem prawnym pozwalającym zamawiającemu na zarządzeniem ryzykiem związanym z podwykonawcami, jest możliwość zastrzeżenia określonych części zamówienia do realizacji wyłącznie przez wykonawcę bez udziału podwykonawców (art. 121 ustawy Pzp).

Zwłaszcza w obszarze zamówień dotyczących obronności i bezpieczeństwa, ograniczenia w doborze podwykonawców znajdują szczególne uzasadnienie. Zapewne w wyniku dynamicznie zmieniającej się sytuacji geopolitycznej powyższe ograniczenia wkrótce pojawią się szerzej w dokumentacji postępowania o udzielnie zamówienia publicznego zamówień dotyczących także systemów IT/OT. Stąd do istotnych zobowiązań umownych publikowanych lub w inny sposób udostępnianych przez zamawiających, nawet na wczesnych etapach przygotowania postępowania o udzielenie zamówienia, zaliczyć należy wytyczne, na jakie rodzaje umów z podwykonawcami zamawiający powinien zwrócić szczególną uwagę. Świadczenia podwykonawców istotne z punktu widzenia bezpieczeństwa łańcucha dostaw nie powinny pozostać poza regulacjami kontaktowymi pomiędzy zamawiającym a wykonawcą. W tym wypadku standardowe postanowienie umowne odnośnie odpowiedzialności wykonawcy za działania swojego podwykonawcy wydaje się zbyt ogólne. Należyte zabezpieczenie łańcucha dostaw powinno obejmować zarówno kwestie odpowiedzialności za podwykonawcę, ale także obowiązki w zakresie zmiany takiego podwykonawcy, zmiany technologii lub usług, jeżeli zostaną uznane za cyberzagrożenie.

[131] art. 12(5) rozporządzenie ustanawiające program "Cyfrowa Europa"

Dlatego też zastosowanie możliwości, jakie dają przepisy z art. 409 ustawy Pzp odnośnie szczegółowych wymagań związanych z realizacją zamówienia w zakresie podwykonawstwa wydają się racjonalnym krokiem ku właściwemu zarządzaniu ryzykiem w obszarze bezpieczeństwa łańcucha dostaw. Znajomość kręgu podwykonawców realizujących newralgiczne usługi, dostawy lub roboty budowlane i możliwość wpływania na szeroko pojęte otoczenie podmiotowe realizujące zamówienie wpisuje się w zalecaną praktykę, aby kontrolować nie tylko samego wykonawcę, ale również podmioty z nim współpracujące, gdyż mogą być źródłem zagrożenia.

### 3.8.2 Ochrona informacji w zabezpieczeniu łańcucha dostaw

Wobec dynamicznie przyrastającej liczby ataków w polskiej cyberprzestrzeni pojawiło się pytanie, czy w celu utrudnienia wrogim podmiotom ich działań, nie powinno się zmienić dotychczasowego podejścia do zasady jawności. Nie chodzi oczywiście o jej wyłączenie, jednak mając na uwadze skalę i rodzaj zagrożeń, wydaje się zasadne, aby przygotowując dokumenty zamówienia dokonać także analizy, które informacje mogą być użyteczne dla wrogich podmiotów. Czasami może się okazać, że zwyczajne dane w OPZ o wygasającym w określonym dniu wsparciu oprogramowania mogą być cenną wskazówką i wskazywać potencjalny wektor ataku.

#### 3.8.2.1 Informacje chronione w zamówieniach klasycznych

Ochrona istotnych informacji może znaleźć zastosowanie w przetargu nieograniczonym poprzez zastosowanie dyspozycji art. 133 ust. 3 ustawy Pzp, zgodnie z którym, jeżeli zamawiający nie może udostępnić części SWZ na stronie, internetowej prowadzonego postępowania z powodu ochrony poufnego charakteru informacji zawartych w SWZ, określa w ogłoszeniu o zamówieniu sposób dostępu do tych informacji oraz wymagania związane z ochroną ich poufnego charakteru.

**Przykłady braku należytego zabezpieczenia informacji przez zamawiających**

A) Jako negatywną należy ocenić praktykę zamawiających publikujących w ramach SWZ dokumentację techniczną, budowlaną, która wrogim podmiotom umożliwia zapoznanie się z budową newralgicznych systemów, sieci, czy budynków. Zważywszy, że często wybór przez wrogie podmioty celów swoich operacji odbywa się zdalnie, przy pomocy powszechnie dostępnych narzędzi OSINT, wprowadzenie ograniczenia w

dostępie do poszczególnych części SWZ poprzez udostępnianie informacji po zawarciu umowy o poufności i ograniczeniu dostępu do informacji na podstawie art. 133 ust. 3 ustawy Pzp wyłącznie w siedzibie zamawiającego może już stanowić barierę, która odstraszy potencjalnych cyberprzestępców. Oczywiście takie restrykcje w dostępie do dokumentacji postępowania będą się wiązały z mniejszym lub większym ograniczeniem dostępności informacji i być może część wykonawców nie zdecyduje się nawet na zapoznanie z dokumentacją postępowania. Jest to ryzyko, które należy uwzględniać przy stosowaniu środków adekwatnych do zamierzonych celów. Jak każde ograniczenie tak i to, zwiększa bezpieczeństwo zamawiającego stanowiąc jednocześnie barierę dla niektórych wykonawców, dlatego też należy je stosować po uprzedniej analizie proporcjonalności takiego rozwiązania. Odnośnie obowiązków leżących po stronie jednostki stosującej dyspozycję art. 133 ust. 3 ustawy Pzp wypowiedział się Prezes UZP swoim komentarzu wskazując: "Wówczas zamawiający musi określić w ogłoszeniu o zamówieniu nie tylko sposób dostępu do tych informacji, ale również wymagania związane z ochroną ich poufnego charakteru. W takim przypadku może się zdarzyć, że zamawiający zdecyduje się na ograniczenie grona osób ze strony potencjalnego wykonawcy, którzy będą mogli zapoznać się z poufną częścią SWZ[132],

**Uwaga:** Jeżeli w trakcie APW lub tworzenia OPZ pojawi się potrzeba ochrony informacji na podstawie art. 133 ust. 3 ustawy Pzp należy ustalić, czy zamówienie nie powinno zmienić kwalifikacji z klasycznego na zamówienie w dziedzinie obronności i bezpieczeństwa".

B) Kolejnym przykładem ryzykownej praktyki w obszarze stosowania zasady jawności w postępowaniu o udzielenie zamówienia publicznego jest zamawianie kompleksowego audytu bezpieczeństwa IT bez wprowadzania jakichkolwiek wymogów ochrony raportu powstającego w wyniku takiego audytu.

- Po pierwsze taki raport bez zastrzeżenia ochrony informacji o zdiagnozowanych lukach w zabezpieczeniach czy podatnościach jest

[132] Prawo zamówień publicznych, komentarz wydanie II, pod redakcją Huberta Nowaka i Mateusza Winiarza [on - line] https://www.gov.pl/web/uzp/komentarz-do-prawa-zamowien-publicznych, dostępny 12.11.2025 str. 490.

narażony na ujawnienie choćby w wyniku pozytywnego rozpatrzenia wniosku o udostępnienie informacji publicznej.

- Po drugie stwierdzono zintensyfikowaną działalność wrogich podmiotów celowaną w organy administracji publicznej zwłaszcza samorządowej oraz pracowników zajmujących się cyberbezpieczeństwem, zatem wydaje się, że dotychczasowe podejście do zasady jawności musi zostać zweryfikowane, wymóg usunięcia przez wykonawcę ze swoich systemów wrażliwych danych w odpowiednim terminie i zwrot wszystkich dokumentów udostępnionych wykonawcy powinien być standardowym obowiązkiem.

#### 3.8.2.2. Informacje chronione w zamówieniach z dziedziny obronności i bezpieczeństwa

W świetle zamówień w dziedzinie obronności i bezpieczeństwa, którym poświęcono Dział VI ustawy Pzp, pojawia się wiele wątpliwości co do:

- posługiwania się informacjami objętymi klauzulami przewidzianymi w UOIN,
- zastosowania przepisów z tego działu wobec zamówień dotyczących infrastruktury krytycznej.

Trudności interpretacyjne wynikają przede wszystkim z treści dyrektywy obronnej, która nie została zaktualizowana niemal od początku swojego istnienia, podczas gdy rozwój technologii wywarł ogromny wpływ na modernizację sił zbrojnych czy infrastruktury krytycznej.

Pomimo braku jasnego i precyzyjnego odniesienia pojęć i uregulowań dyrektywy obronnej do cyberprzestrzeni wydaje się racjonalnym założeniem, że jej normy należy interpretować w sposób pozwalający przyjąć, iż mogą dotyczyć nie tylko kwestii ściśle wojskowych, ale także odnosić się w określonych przypadkach do infrastruktury krytycznej i zagrożeń płynących z cyberprzestrzeni. Tym samym przepisy działu VI, czy przepisy wyłączające stosowanie ustawy Pzp, nawet jeżeli nie dotyczą wyłącznie sprzętu/usług/robót budowlanych zamawianych do celów stricte wojskowych, mogą w określonych wypadkach znaleźć zastosowanie, gdyż aktualnie pojęcie „w dziedzinie obronności i bezpieczeństwa" trzeba interpretować uwzględniając realny wpływ realizowanych zamówień na infrastrukturę państwową i samorządową. Przykładem ostatnich działań potwierdzających, że

wrogie podmioty upatrują możliwość naruszenia bezpieczeństwa państwa poprzez cyberataki są ataki na polskie wodociągi.[133]

Jak pokazuje wojna w Ukrainie, coraz trudniej jest postawić jasną granicę, co może być sprzętem wojskowym, a co sprzętem podwójnego zastosowania albo co uznać za cel wojskowy. Pojawia się pytanie odnośnie celów strategicznych jak energetyka, transport, ochrona zdrowia, czy łączność, których bezpieczeństwo okazuje się być częścią składową, istotną z punktu widzenia prawidłowego funkcjonowania państwa. Infrastruktura ta znajduje się pod ciągłą presją intensywnych, wrogich działań w cyberprzestrzeni. Dlatego zamawiający coraz częściej będą stawiać pytanie, jak zakwalifikować dane zamówienie i jak chronić informacje, aby zapewnić infrastrukturze newralgicznej ciągłość i bezpieczeństwo łańcucha dostaw.

Zamówienia z dziedziny obronności i bezpieczeństwa odnoszą się w swojej definicji do pojęcia newralgicznego sprzętu lub usług oraz robót budowlanych. Natomiast pojęcie „newralgiczności" jest definicyjnie powiązane z korzystaniem z informacji niejawnych lub informacji podlegających ochronie ze względów bezpieczeństwa, wymagają ich wykorzystania lub je zawierają. Zatem czym różnią się informacje podlegające ochronie ze względów bezpieczeństwa od informacji niejawnych. Wydaje się, że rozbieżności interpretacyjne wynikają z samej konstrukcji prawa unijnego, tworzonego na takim stopniu ogólności, aby mogło zostać zaimplementowane w różnych europejskich systemach prawnych. Tym samym ich wprowadzenie do polskiego porządku prawnego w obecnej formie nie do końca odzwierciedla wyzwania, przed którymi muszą stawać zamawiający.

Zgodnie z dyrektywą obronną art. 1 pkt 8) "informacje niejawne" oznaczają wszelkie informacje lub materiały, niezależnie od ich formy, charakteru lub sposobu ich przekazania, którym przyznano określony poziom niejawności lub ochrony ze względów bezpieczeństwa i które - w interesie bezpieczeństwa narodowego i zgodnie z przepisami ustawowymi, wykonawczymi i administracyjnymi obowiązującymi w danym państwie członkowskim - wymagają ochrony przed wszelkim sprzeniewierzeniem, zniszczeniem, usunięciem, ujawnieniem, utratą lub dostępem ze strony osób nieupoważnionych lub wszelkim innym zagrożeniem.

W polskim porządku prawnym aktem rangi ustawowej regulującym ochronę informacji ze względu na jej znaczenie dla bezpieczeństwa narodowego jest UOIN

[133] Oskar Klimczuk „Ataki na wodociągi. Szef CERT Polska o realnych skutkach" https://cyberdefence24.pl/cyberbezpieczenstwo/ataki-na-wodociagi-szef-cert-polska-o-realnych-skutkach [on line] dostępny 18.12.2025

i ustawa ta nie przewiduje ochrony informacji inaczej niż przez uczynienie ich formalnie niejawnymi poprzez nadanie odpowiedniej klauzuli. Tak sztywne ujęcie formalne jest wyjątkowo niepraktyczne, gdyż informacje objęte klauzulami mają ściśle określony sposób przetwarzania.

Przykład:

*Dokumentacja dotycząca systemu IT, który zamawiający chciałby chronić przed ujawnieniem, musiałaby być przechowywana w kancelarii tajnej, co w przypadku awarii systemu znacznie utrudniałoby prace nad jej usunięciem.*

Sytuacji nie poprawia definicja zamówienia w dziedzinach obronności i bezpieczeństwa (art. 7 pkt 36 c), który referuje do robót budowlanych, dostaw i usług związanych z zabezpieczeniem obiektów będących w dyspozycji podmiotów realizujących zamówienia w dziedzinach obronności i bezpieczeństwa lub związane ze sprzętem, o którym mowa w lit. a i b, i wszystkich jego części, komponentów i podzespołów związanych z cyklem życia tego produktu lub usługi. Ustawodawca przewidział w tym przepisie odniesienie do materialnych przedmiotów - obiekty - pomijając istnienie cyberprzestrzeni.

Powyższa niejednolitość terminologii wywołuje wątpliwości:

- czy w przypadku każdego zamówienia, w którego dokumentacji pojawią się informacje objęte klauzulami przewidzianymi w UOIN mamy do czynienia z zamówieniami określonymi w Dziale VI,
- czy zamówienie, w którym nie znalazły się żadne dokumenty objęte wskazanymi klauzulami można zakwalifikować jako zamówienie w dziedzinach obronności i bezpieczeństwa ze względu na ochronę infrastruktury krytycznej także tej związanej z cyberprzestrzenią.

Z pomocą skonfundowanym zamawiającym stara się przyjść orzecznictwo i doktryna. W wyroku z 18 lipca 2024 r. sygn akt II SA/Wa 307/24 Wojewódzki Sąd Administracyjny w Warszawie, stwierdził, że “W świetle ugruntowanych już poglądów orzecznictwa, dla zakwalifikowania danej informacji do informacji niejawnej wystarczy element materialny. Informacja niejawna chroniona jest zatem bez względu na to, czy osoba uprawniona uznała za stosowne oznaczyć ją odpowiednią klauzulą. Jest ona bowiem niejawna z uwagi na zagrożenia wynikające z jej treści, lub sposobu jej uzyskania, a nie w następstwie klasyfikacji.” Zgodnie z powyższym istnieje możliwość powiązania skutkowo-przyczynowego kwestii bezpieczeństwa państwa i obronności z informacjami chronionymi bez

nadania im takiego charakteru w sposób formalny. Jednak takiego działania nie można uznać za wynikającego wprost z treści obowiązujących przepisów UOIN.

Treść art. 13 ust. 1 pkt 3 ustawy Pzp, zezwala na odejście od stosowania przepisów ustawy Pzp wobec zamówień w dziedzinach obronności i bezpieczeństwa, jeżeli stosowanie przepisów ustawy zobowiązywałoby zamawiającego do przekazania informacji, których ujawnienie jest sprzeczne **z podstawowymi interesami bezpieczeństwa państwa.** Wydaje się, że formalna ochrona informacji jest niezbędnym elementem takiego postępowania. Pojęcie podstawowego interesu państwa znajduje swoje źródło w art. 346 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) „postanowienia Traktatów nie stanowią przeszkody w stosowaniu następujących reguł: a) żadne Państwo Członkowskie nie ma obowiązku udzielania informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami jego bezpieczeństwa; b) każde Państwo Członkowskie może podejmować środki, jakie uważa za konieczne w celu ochrony podstawowych interesów jego bezpieczeństwa, a które odnoszą się do produkcji lub handlu bronią, amunicją lub materiałami wojennymi; środki takie nie mogą negatywnie wpływać na warunki konkurencji na rynku wewnętrznym w odniesieniu do produktów, które nie są przeznaczone wyłącznie do celów wojskowych". Pomocny w jego wyjaśnieniu jest motyw 20 preambuły dyrektywy obronnej, zgodnie z którym „zamówienia w dziedzinach obronności i bezpieczeństwa zawierają często poufne informacje, które na mocy przepisów ustawowych, wykonawczych i administracyjnych obowiązujących w danym państwie członkowskim muszą być ze względów bezpieczeństwa chronione przed dostępem ze strony osób nieupoważnionych. W dziedzinie wojskowej istnieją w państwach członkowskich systemy opatrywania takich informacji klauzulą tajności w celach wojskowych. W zakresie bezpieczeństwa niewojskowego nie wszystkie państwa członkowskie posiadają system opatrywania takich informacji klauzulą tajności. W związku z tym właściwe jest zastosowanie koncepcji, która wzięłaby pod uwagę różnorodność praktyk w państwach członkowskich i która pozwoliłaby objąć zarówno aspekty wojskowe, jak i niewojskowe. (...) Ponadto art. 296 ust. 1 lit. a) Traktatu oferuje państwom członkowskim możliwość zwolnienia zamówień w dziedzinie obronności i bezpieczeństwa z obowiązku stosowania przepisów niniejszej dyrektywy, jeżeli jej zastosowanie zobligowałoby je do dostarczenia informacji, których ujawnienie uznałyby za sprzeczne z istotnymi interesami ich bezpieczeństwa. Taka sytuacja może zaistnieć zwłaszcza w przypadkach, gdy zamówienie jest tak newralgiczne, że nawet sam fakt jego

istnienia powinien zostać objęty tajemnicą.” Z powyższego można wysnuć wniosek, że zamówienie w dziedzinie obronności i bezpieczeństwa może mieć charakter niewojskowy, jednakże sugeruje też, aby zastosować art. 13 ust. 1 pkt 3 ustawy Pzp, konieczna jest ochrona informacji w sposób formalny, co w polskich warunkach oznacza stosowanie klauzul ochrony informacji niejawnych przewidzianych UOIN. Za pozytywny kierunek wykładni należy uznać utożsamienie pojęć podstawowego i istotnego interesu bezpieczeństwa państwa, którego dokonał UZP w swojej opinii „Istotny interes bezpieczeństwa państwa, o którym mowa w art. 12 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, w kontekście zamówień w dziedzinach obronności i bezpieczeństwa”[134], gdyż przecina dotychczasowe spekulacje, czy zróżnicowanie pojęciowe powinno odbijać się w analizach prawnych i powodować gradację kwestii bezpieczeństwa państwa.
Powyższe rozważania mają znaczenie w kontekście bezpieczeństwa łańcucha dostaw, gdyż ochrona wrażliwych informacji wymienianych pomiędzy zamawiającym a wykonawcami może istotnie wpływać na zarządzanie ryzykiem w łańcuchu dostaw.

## 4. Zarządzanie ryzykiem w łańcuchu dostaw

### 4.1. Rola zarządzania ryzykiem w kontekście zamówień publicznych

Zarządzanie ryzykiem w łańcuchu dostaw stanowi obecnie jeden z najważniejszych elementów zapewnienia cyberbezpieczeństwa w sektorze publicznym. W epoce cyfryzacji usług publicznych i rosnącej zależności instytucji administracji od technologii informacyjno-komunikacyjnych, każdy proces zakupowy może być potencjalnym punktem wejścia dla ryzyk technicznych, organizacyjnych lub prawnych.

Ryzyko w łańcuchu dostaw nie jest zjawiskiem nowym — zawsze towarzyszyło procesom zakupowym. Jednak jego charakter ewoluował: dawniej dotyczyło głównie jakości i terminowości dostaw, dziś obejmuje także sferę bezpieczeństwa informacji, integralności systemów oraz wiarygodności dostawców technologicznych. Oznacza to, że klasyczne modele oceny ryzyka (finansowego,

[134] Istotny interes bezpieczeństwa państwa, o którym mowa w art. 12 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, w kontekście zamówień w dziedzinach obronności i bezpieczeństwa [on line] https://www.gov.pl dostępny 18.12.2025 r.

operacyjnego, jakościowego) muszą być uzupełnione o perspektywę cyberbezpieczeństwa, w której kluczową rolę odgrywa ochrona danych, niezawodność systemów teleinformatycznych oraz zgodność z wymogami prawnymi i normatywnymi.

W kontekście zamówień publicznych zarządzanie ryzykiem nabiera szczególnego znaczenia z trzech powodów:

1. **Skala wpływu** – decyzje zakupowe sektora publicznego często dotyczą infrastruktury krytycznej (energetyka, transport, zdrowie, administracja). Błąd w ocenie ryzyka może doprowadzić do zakłóceń o charakterze ogólnokrajowym.
2. **Odpowiedzialność prawna i finansowa** – instytucje publiczne odpowiadają za wydatkowanie środków publicznych i muszą wykazać należytą staranność w ocenie ryzyk.
3. **Powiązanie z regulacjami UE** – dyrektywa NIS2, rozporządzenie CRA oraz nowelizacja KSC nakładają na podmioty publiczne obowiązek wdrażania mechanizmów zarządzania ryzykiem w całym łańcuchu dostaw, obejmującym także podmioty prywatne świadczące usługi ICT.

Właśnie dlatego zarządzanie ryzykiem w zamówieniach publicznych nie może być postrzegane jako jednorazowy element formalny, ale jako proces systemowy, powiązany z polityką bezpieczeństwa informacji oraz planowaniem strategicznym organizacji. Takie podejście jest zgodne z zasadami norm ISO/IEC 27001 (system zarządzania bezpieczeństwem informacji), ISO/IEC 27005 (zarządzanie ryzykiem) i ISO/IEC 27036 (bezpieczeństwo w relacjach z dostawcami).

Wspólnym mianownikiem tych dokumentów jest założenie, że bezpieczeństwo informacji jest wartością współdzieloną przez wszystkie podmioty uczestniczące w procesie świadczenia usług. Oznacza to, że odpowiedzialność za ryzyko rozkłada się na zamawiającego, wykonawcę i jego poddostawców.

### 4.1.1. Powiązanie zarządzania ryzykiem z cyklem życia zamówienia publicznego

Efektywne zarządzanie ryzykiem w zamówieniach publicznych wymaga zrozumienia, że jest to proces ciągły, który towarzyszy każdemu etapowi cyklu życia zamówienia. Nie można go ograniczyć do momentu wyboru oferty czy podpisania umowy – musi być zintegrowany z całym procesem zakupowym: od planowania po zakończenie współpracy.

Zgodnie z zasadą „security by design", bezpieczeństwo nie może być „doklejane" do projektu po fakcie, lecz musi być elementem jego projektowania i realizacji. Dlatego zarządzanie ryzykiem należy rozpocząć już na etapie definiowania potrzeb i opisu przedmiotu zamówienia.

**Etap 1. Planowanie zamówienia – analiza ryzyk strategicznych**

W tej fazie kluczowe jest określenie kontekstu organizacyjnego i otoczenia regulacyjnego. Zamawiający powinien zidentyfikować:

- **krytyczność systemu lub usługi**, która ma zostać nabyta,
- **zależności** od istniejących systemów i infrastruktury,
- **skutki utraty dostępności lub poufności danych**,
- **ograniczenia prawne** (np. lokalizacja danych, transfer do państw trzecich).

Następnie dokonuje się **oceny ryzyka strategicznego**, czyli takiego, które może mieć wpływ na funkcjonowanie całej instytucji lub sektora.

Przykład*:*
*Podmiot publiczny odpowiedzialny za administrację elektroniczną planując zakup platformy do e-usług, powinien w analizie ryzyka uwzględnić nie tylko kwestie techniczne (np. bezpieczeństwo serwerów), ale także ryzyka polityczne (np. dostawcy z państw o ograniczonym zaufaniu), prawne (np. zgodność z RODO) i operacyjne (np. ryzyko przerwy w świadczeniu usług).*

**Etap 2. Postępowanie o udzielenie zamówienia publicznego – zarządzanie ryzykiem wykonawców**

To etap, na którym ryzyko przenosi się z poziomu strategii na poziom operacyjny. W praktyce sprowadza się do określenia takich warunków udziału w postępowaniu, które pozwolą wyłonić dostawców zdolnych do zapewnienia bezpieczeństwa informacji.

Kluczowe działania zamawiającego:

- określenie **wymagań bezpieczeństwa** w opisie przedmiotu zamówienia (np. zgodność z ISO 27001, posiadanie certyfikatu bezpieczeństwa sprzętu),
- żądanie od wykonawców **dowodów zgodności** (raportów, certyfikatów, oświadczeń),
- stosowanie **kryteriów jakościowych** premiujących wyższy poziom bezpieczeństwa (np. posiadanie własnego CSIRT, testy penetracyjne).

***Przykład:***

*W jednym z postępowań dotyczących systemu finansowego dla administracji centralnej zamawiający wprowadził kryterium „poziomu dojrzałości bezpieczeństwa dostawcy" oparte na modelu CMMI. W efekcie wybrano wykonawcę, który posiadał dojrzałe procesy reagowania na incydenty, mimo że jego oferta była nieco droższa.*

**Etap 3. Realizacja umowy – monitorowanie i kontrola ryzyka**

Podpisanie umowy nie kończy procesu zarządzania ryzykiem. W rzeczywistości to dopiero początek jego praktycznego stosowania. W trakcie realizacji zamówienia ryzyka mogą się materializować — zwłaszcza te związane z integracją systemów, zmianą konfiguracji czy udziałem podwykonawców.

Zamawiający powinien wdrożyć:

- mechanizmy monitorowania zgodności wykonawcy z wymaganiami umownymi,
- procedury raportowania incydentów,
- możliwość audytu (zarówno planowego, jak i incydentalnego),
- system wskaźników KRI (Key Risk Indicators).

*Przykład:*

*Podczas realizacji projektu wdrożenia oprogramowania klasy ERP w jednej z agencji rządowych wykryto, że podwykonawca korzystał z chmury publicznej spoza EOG. Na podstawie klauzuli audytowej zamawiający zażądał weryfikacji zgodności i wymusił przeniesienie środowiska do dostawcy europejskiego.*

**Etap 4. Zakończenie umowy – zarządzanie ryzykiem resztkowym**

Końcowa faza cyklu życia zamówienia obejmuje zabezpieczenie danych i systemów po zakończeniu współpracy.

Zamawiający powinien zadbać o:

- usunięcie lub zwrot danych,
- unieważnienie dostępów i certyfikatów,
- archiwizację dokumentacji bezpieczeństwa,
- ocenę postprojektową (tzw. *lessons learned*).

Przykład*:*

*W urzędzie, który zakończył współpracę z dostawcą usług chmurowych, przeprowadzono audyt powykonawczy. Okazało się, że konta administratorów nadal miały dostęp do danych po rozwiązaniu umowy. W wyniku wniosków z tego incydentu*

*opracowano nową procedurę „deprovisioningu" – obowiązkowego odłączania dostawców po zakończeniu kontraktu.*

### 4.1.2. Zarządzanie ryzykiem jako obowiązek organizacyjny wynikający z NIS2, UKSC

Zarządzanie ryzykiem w obszarze bezpieczeństwa informacji przestało być elementem fakultatywnym polityki organizacyjnej, a stało się obowiązkiem prawnym i regulacyjnym, który instytucje publiczne muszą nie tylko realizować, ale i potrafić wykazać w sposób udokumentowany. To jedna z najistotniejszych zmian, jakie przyniosła nowa generacja przepisów unijnych — w szczególności dyrektywa NIS2 (UE) 2022/2555, rozporządzenie CRA (Cyber Resilience Act) oraz reforma ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Dyrektywa NIS2, w art. 21, wyraźnie stwierdza, że każdy podmiot uznany za kluczowy lub ważny — a więc m.in. jednostki administracji publicznej, podmioty infrastruktury krytycznej, operatorzy usług publicznych i dostawcy ICT — musi wdrożyć proporcjonalne środki techniczne, operacyjne i organizacyjne służące zarządzaniu ryzykiem bezpieczeństwa sieci i informacji. Co istotne, środki te mają obejmować również bezpieczeństwo łańcucha dostaw i relacje z podmiotami trzecimi.

Oznacza to, że obowiązek zarządzania ryzykiem nie ogranicza się do samego zamawiającego – rozciąga się na cały ekosystem dostawców, integratorów i usługodawców, którzy mają wpływ na funkcjonowanie jego systemów informacyjnych. W praktyce instytucja publiczna musi więc rozumieć, jakie ryzyka występują w otoczeniu, nad którym nie ma bezpośredniej kontroli – i w jaki sposób może je zminimalizować poprzez wymagania kontraktowe, audyty, procedury i monitoring.

Z kolei projekt nowelizacji ustawy UKSC (UC32) wprowadza wprost obowiązek prowadzenia analizy ryzyka obejmującej nie tylko własne zasoby, lecz także podmioty zewnętrzne realizujące zadania na rzecz podmiotu kluczowego lub ważnego. Co więcej, nowelizacja wprowadza wymóg oceny ryzyka dla łańcucha dostaw jako elementu planu zarządzania bezpieczeństwem. W praktyce instytucje publiczne będą musiały posiadać formalnie zatwierdzone dokumenty potwierdzające realizację procesu:

- rejestr zidentyfikowanych ryzyk,
- raporty z analiz zgodności,

- procedury monitorowania i przeglądu ryzyka,
- oraz dowody reagowania i aktualizacji działań korygujących.

Norma ISO/IEC 27005:2022 dostarcza tu pełnej metodologii – jest więc narzędziem do praktycznej implementacji wymogów NIS2 i KSC. Wyróżnia pięć głównych etapów zarządzania ryzykiem:

1. **Ustanowienie kontekstu organizacyjnego i regulacyjnego** – rozumienie celów, misji, zobowiązań prawnych, środowiska i interesariuszy.
2. **Identyfikacja ryzyka** – określenie zasobów, zagrożeń, podatności i skutków potencjalnych incydentów.
3. **Analiza ryzyka** – ocena prawdopodobieństwa i skutków, uwzględniająca środki kontrolne już istniejące.
4. **Ewaluacja ryzyka** – porównanie wyników analizy z kryteriami akceptowalności i ustalenie priorytetów działań.
5. **Traktowanie ryzyka** – wybór strategii postępowania: unikanie, ograniczenie, przeniesienie (np. ubezpieczenie, outsourcing) lub akceptacja.

Szczególnie istotny dla sektora publicznego jest etap ustalenia kontekstu, w którym należy uwzględnić uwarunkowania prawne – m.in. ustawę Pzp, ustawę o ochronie informacji niejawnych, RODO oraz krajowe strategie cyberbezpieczeństwa. Dzięki temu proces zarządzania ryzykiem nie jest oderwany od obowiązujących przepisów, lecz staje się spójną częścią systemu zarządzania zgodnością (*compliance*).

Co ważne, ISO/IEC 27005 zakłada ciągłość procesu – ryzyko musi być przeglądane i aktualizowane w odpowiedzi na zmiany w systemach, relacjach z dostawcami i otoczeniu. Oznacza to, że zarządzanie ryzykiem jest żywym procesem, nie raportem „do szuflady".

Przykład:
*Podczas postępowania na modernizację systemu rejestrów publicznych jeden z podmiotów publicznych wdrożył procedurę zgodną z ISO 27005, w której analizowano również ryzyka związane z outsourcowaniem utrzymania systemu. W wyniku tej analizy wykluczono model usługowy oparty na dostawcy spoza UE, uznając, że ryzyko niezgodności z wymogami ochrony danych i ciągłości działania jest zbyt wysokie.*

W praktyce wdrożenie zarządzania ryzykiem wymaga zbudowania kompetencji organizacyjnych – przeszkolonych zespołów, systemów raportowania i narzędzi wspierających (np. platform do rejestracji i analizy ryzyk). Instytucje publiczne coraz częściej korzystają tu z rozwiązań klasy GRC (Governance, Risk &

Compliance), które pozwalają łączyć zarządzanie ryzykiem, audyt i zgodność regulacyjną w jednym środowisku.

W ten sposób zarządzanie ryzykiem przestaje być zadaniem technicznym, a staje się funkcją strategiczną, która wspiera zarząd i najwyższe kierownictwo instytucji publicznej w podejmowaniu decyzji dotyczących zamówień, kontraktów i współpracy z podmiotami zewnętrznymi.

### 4.1.3. Współzależność między ryzykiem dostawcy a ryzykiem zamawiającego (model wspólnej odpowiedzialności)

Jedną z najważniejszych zasad zarządzania bezpieczeństwem w łańcuchu dostaw jest uznanie, że ryzyko jest współdzielone. W praktyce oznacza to, że ani zamawiający, ani dostawca nie mogą uznać, że odpowiedzialność za bezpieczeństwo spoczywa wyłącznie na drugiej stronie. Współczesne systemy informatyczne są tak zintegrowane i współzależne, że nawet drobne uchybienie w jednym z ogniw – np. u zewnętrznego operatora serwisu utrzymaniowego – może mieć konsekwencje dla całego systemu.

Zasada shared risk ownership (wspólnego zarządzania ryzykiem) została szczegółowo rozwinięta w normie ISO/IEC 27036-3, dotyczącej bezpieczeństwa informacji w relacjach z dostawcami usług ICT. Zakłada ona, że relacja między zamawiającym a dostawcą nie powinna opierać się wyłącznie na wymogach formalnych, lecz na wzajemnym zrozumieniu ryzyk, transparentności i zaufaniu operacyjnym.

W praktyce oznacza to trzy podstawowe obszary współdziałania:

1. Wspólne planowanie bezpieczeństwa – zamawiający i wykonawca powinni uzgodnić, jakie dane, systemy i procesy będą objęte ochroną oraz jakie standardy i procedury zostaną zastosowane.
2. Koordynacja reagowania na incydenty – obie strony muszą mieć jasno określone obowiązki informacyjne, kanały komunikacji i czasy reakcji.
3. Wspólne audyty i przeglądy – regularna wymiana informacji o wynikach audytów, testów penetracyjnych i zmianach konfiguracji.

Model współdzielonej odpowiedzialności zyskuje coraz większe znaczenie także w obszarze chmur obliczeniowych. Europejskie wytyczne ENISA i Komisji Europejskiej dotyczące tzw. *Cloud Service Provider Assurance* wskazują, że bezpieczeństwo chmury jest efektem wspólnego działania dostawcy infrastruktury i użytkownika – odpowiedzialność rozkłada się w zależności od modelu (IaaS, PaaS,

SaaS). Podobne podejście powinno być stosowane w zamówieniach publicznych, gdzie złożone relacje kontraktowe obejmują często kilku podwykonawców i integratorów.

Współodpowiedzialność ma również wymiar formalny. Zgodnie z art. 474 Kodeksu cywilnego, wykonawca odpowiada za działania i zaniechania swoich podwykonawców jak za własne. Zamawiający natomiast odpowiada za nadzór i dopilnowanie, by relacje kontraktowe nie naruszały obowiązujących przepisów ani nie zagrażały bezpieczeństwu informacji.

Przykład:
*W kontrakcie na rozwój systemu ewidencji ludności, zamawiający wprowadził do umowy postanowienie, że każdy podwykonawca mający dostęp do środowiska produkcyjnego musi przejść audyt bezpieczeństwa przed rozpoczęciem prac. W efekcie wykryto, że jedna z firm utrzymaniowych korzysta z nieaktualnych bibliotek kryptograficznych – dzięki czemu możliwe było usunięcie podatności jeszcze przed wdrożeniem.*

Współdzielona odpowiedzialność za ryzyko wymaga jednak kultury współpracy i dojrzałości organizacyjnej po obu stronach. Zamawiający powinien zapewnić jasne zasady nadzoru, a dostawca – transparentność i otwartość w komunikacji o zagrożeniach. W ten sposób ryzyko staje się elementem współzarządzanym, a nie jednostronnym obowiązkiem. To z kolei znacząco podnosi poziom zaufania i bezpieczeństwa w długofalowych relacjach kontraktowych.

### 4.1.4. Łańcuch dostaw ICT jako źródło ryzyk wielowarstwowych

Współczesny łańcuch dostaw ICT to skomplikowana sieć powiązań, w której uczestniczą dziesiątki, a czasem setki podmiotów — od producentów sprzętu, przez dostawców oprogramowania, po integratorów, serwisantów, konsultantów i operatorów chmur. Każdy z nich wnosi własne komponenty, usługi, procesy, ale też własne ryzyka.

Zarządzanie ryzykiem w takim środowisku wymaga rozpoznania, że zagrożenia te nie są jednowymiarowe. Można wyróżnić co najmniej pięć nakładających się warstw: techniczną, organizacyjną, prawną, geopolityczną i operacyjną.

1. Warstwa techniczna – obejmuje błędy w oprogramowaniu, podatności typu zero-day, złośliwe komponenty w bibliotekach open source, błędne konfiguracje i nieautoryzowane modyfikacje firmware'u. Wystarczy jedno niezweryfikowane źródło aktualizacji lub komponent sprzętowy

pochodzący z niepewnego łańcucha produkcji, aby wprowadzić do systemu trwałe ryzyko kompromitacji.

2. Warstwa organizacyjna – odnosi się do ludzi i procesów. Brak szkoleń, nadzoru nad personelem, planów ciągłości działania czy rotacji pracowników w kluczowych funkcjach bezpieczeństwa często staje się początkiem incydentu. W praktyce administracji publicznej wiele naruszeń wynikało nie z luk technicznych, lecz z błędów proceduralnych — np. pozostawienia aktywnych kont byłych pracowników podmiotów zewnętrznych.
3. Warstwa prawna i regulacyjna – ryzyko powstaje w wyniku niezgodności z przepisami: RODO, KSC, CRA czy ustawą Pzp. Brak właściwych klauzul umownych lub zapisów dotyczących ochrony danych może prowadzić do odpowiedzialności finansowej i reputacyjnej.
4. Warstwa geopolityczna – dotyczy źródła pochodzenia sprzętu i oprogramowania oraz możliwości ingerencji państw trzecich. Unia Europejska i ENISA w ostatnich latach zwracają uwagę na potrzebę oceny ryzyka geopolitycznego w dostawach ICT.
5. Warstwa operacyjna – związana z utrzymaniem systemów, reagowaniem na incydenty i zapewnieniem redundancji. Brak planów awaryjnych, uzależnienie od pojedynczego dostawcy czy niedostateczne SLA (Service Level Agreement) to klasyczne ryzyka eksploatacyjne.

W praktyce każdy z tych poziomów nakłada się na pozostałe, tworząc złożoną strukturę powiązań. Dlatego analiza ryzyka w łańcuchu dostaw musi być prowadzona interdyscyplinarnie – przez zespół złożony z ekspertów technicznych, prawników, audytorów i analityków bezpieczeństwa.

Przykład:

*Podczas analizy łańcucha dostaw w projekcie budowy systemu zarządzania transportem miejskim, zespół audytowy odkrył, że część urządzeń telemetrycznych pochodzi z linii produkcyjnych poza UE i nie posiadała certyfikatów bezpieczeństwa wymaganych przez CRA. Zamawiający wprowadził wymóg homologacji urządzeń zgodnej z europejskim systemem certyfikacji cyberbezpieczeństwa (EUCC), co pozwoliło uniknąć opóźnień i ryzyka braku zgodności.*

Zarządzanie ryzykiem w tak rozproszonym środowisku wymaga tworzenia map łańcucha dostaw – graficznych lub tabelarycznych odwzorowań wszystkich uczestników procesu oraz ich zależności. Takie mapy pozwalają określić, które

elementy są krytyczne, które można zastąpić alternatywnymi dostawcami, a które wymagają szczególnego nadzoru (np. audytu on-site).

Finalnym celem nie jest całkowita eliminacja ryzyka — to w praktyce niemożliwe — lecz jego utrzymanie na poziomie akceptowalnym i zapewnienie, że każdy uczestnik łańcucha ma świadomość swojej roli w systemie bezpieczeństwa.

Tym samym zarządzanie ryzykiem w łańcuchu dostaw ICT przestaje być domeną techników i audytorów. Staje się elementem zarządzania publicznego, a jego skuteczność wymaga kultury organizacyjnej opartej na odpowiedzialności, transparentności i ciągłym doskonaleniu.

## 4.2. Identyfikacja i klasyfikacja dostawców pod kątem cyberzagrożeń

Identyfikacja i klasyfikacja dostawców to proces, który pozwala instytucjom publicznym i zamawiającym sektorowym zrozumieć, kim są ich partnerzy w łańcuchu dostaw, jakie pełnią funkcje, do jakich zasobów mają dostęp i w jaki sposób mogą wpływać na bezpieczeństwo organizacji. W kontekście zamówień publicznych i zarządzania ryzykiem cyberbezpieczeństwa jest to proces o znaczeniu fundamentalnym. Trudno bowiem chronić to, czego nie da się precyzyjnie zidentyfikować ani uporządkować.

Zgodnie z normami ISO/IEC 27036-1 i 27036-3, identyfikacja dostawców to nie tylko ustalenie listy kontrahentów. To także mapowanie powiązań, przepływu danych, zależności funkcjonalnych i relacji odpowiedzialności, które kształtują bezpieczeństwo całego systemu. Dyrektywa NIS2 i nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa wskazują wprost, że podmioty kluczowe i ważne muszą posiadać wiedzę o swoich dostawcach, w tym o poddostawcach, którzy mają wpływ na bezpieczeństwo usług lub danych.

### 4.2.1. Metodyka identyfikacji dostawców i poddostawców (mapowanie łańcucha dostaw)

Identyfikacja dostawców jest pierwszym etapem skutecznego zarządzania ryzykiem. Jej celem jest rozpoznanie wszystkich podmiotów, które w sposób bezpośredni lub pośredni wpływają na bezpieczeństwo procesów, systemów i danych. Odpowiednio przeprowadzony proces pozwala stworzyć mapę łańcucha dostaw, która ukazuje rzeczywiste zależności między uczestnikami projektu.

**Analiza łańcucha wartości i powiązań operacyjnych**

Podstawowym narzędziem w tym procesie jest **analiza łańcucha wartości** (ang. *Value Chain Analysis*), która pozwala zidentyfikować, w jakich miejscach powstaje wartość dodana, a w jakich — potencjalne ryzyka. W praktyce polega to na zmapowaniu wszystkich działań, od pozyskania komponentów lub danych, poprzez ich przetwarzanie, integrację, aż po dostarczenie usługi końcowej użytkownikowi. W sektorze publicznym taką analizę można przeprowadzić np. dla systemu obsługi e-zdrowia:

- dostawca oprogramowania aplikacyjnego,
- dostawca infrastruktury serwerowej,
- operator centrum danych,
- firma utrzymaniowa,
- dostawcy podzespołów (np. producent sprzętu sieciowego),
- oraz podwykonawcy zewnętrznych usług diagnostycznych.

Każdy z tych podmiotów jest częścią łańcucha wartości i potencjalnym źródłem ryzyka.

**Modele identyfikacji wg ENISA i ISO**

Agencja ENISA zaleca, aby proces identyfikacji dostawców był prowadzony metodycznie, w oparciu o cztery kroki:

1. Zdefiniowanie krytycznych usług i zasobów,
2. Zidentyfikowanie wszystkich podmiotów, które mają wpływ na te zasoby,
3. Określenie ich ról i odpowiedzialności,
4. Analizę wzajemnych zależności między nimi.

Z kolei norma ISO/IEC 27036-3 zaleca, aby organizacja dokonała tzw. *supplier mapping* – tworząc graficzne odwzorowanie wszystkich relacji i przepływu informacji między podmiotami. W szczególności należy uwzględnić:

- kto ma dostęp do danych osobowych i informacji niejawnych,
- gdzie są przetwarzane dane (lokalizacja centrów danych),
- kto odpowiada za ich ochronę, backup i utrzymanie,
- jakie technologie lub komponenty są wbudowane w systemy zamawiającego.

**Znaczenie mapowania dla zarządzania ryzykiem**

Tak zbudowana mapa łańcucha dostaw pozwala wskazać punkty krytyczne — miejsca, w których utrata integralności, poufności lub dostępności informacji mogłaby mieć najpoważniejsze skutki. Mapowanie jest nie tylko narzędziem

analizy, ale także narzędziem komunikacji — umożliwia wszystkim interesariuszom (zarządowi, audytorom, inspektorom ochrony danych) zrozumienie struktury zależności.

Przykład:

*W sektorze energetycznym operator systemu przesyłowego przeprowadził mapowanie łańcucha dostaw dla systemu SCADA. Okazało się, że serwis jednego z komponentów zlecono firmie z państwa trzeciego. Dzięki mapie zależności udało się zidentyfikować to ryzyko i zastąpić podwykonawcę dostawcą certyfikowanym w UE.*

### 4.2.2. Kategorie dostawców w ujęciu ryzyka

Nie wszyscy dostawcy w łańcuchu dostaw stanowią takie samo zagrożenie. Jedni mogą decydować o bezpieczeństwie całej infrastruktury, inni mają znaczenie marginalne – np. dostarczają jedynie materiały biurowe. Dlatego jednym z kluczowych elementów systemowego zarządzania ryzykiem jest sklasyfikowanie dostawców według ich wpływu na bezpieczeństwo informacji i ciągłość działania organizacji.

Taka klasyfikacja pozwala racjonalnie rozłożyć środki i uwagę – instytucja publiczna czy sektorowy zamawiający nie jest w stanie jednakowo kontrolować wszystkich podmiotów, z którymi współpracuje. Musi więc wiedzieć, którzy z nich mają charakter krytyczny, a którzy pełnią rolę wspierającą lub marginalną.

**Dostawcy krytyczni**

Dostawcy krytyczni to „serce" łańcucha bezpieczeństwa – podmioty, których działalność jest niezbędna dla funkcjonowania podstawowych procesów i usług. Często posiadają oni dostęp do danych wrażliwych, infrastruktury ICT lub systemów krytycznych. Do tej grupy zaliczają się m.in.:

- dostawcy sprzętu i oprogramowania o kluczowym znaczeniu (systemy ERP, ewidencje państwowe, oprogramowanie sterujące SCADA),
- operatorzy chmur obliczeniowych, serwerowni i centrów danych,
- dostawcy systemów bezpieczeństwa (np. zapory sieciowe, oprogramowanie antywirusowe),
- integratorzy systemów w projektach sektorowych (energetyka, transport, zdrowie).

Zamawiający powinni traktować takich dostawców jak partnerów strategicznych w zakresie bezpieczeństwa. Wymagania wobec nich powinny być najwyższe – nie

tylko formalne (certyfikaty, deklaracje zgodności), ale też operacyjne: regularne audyty, raporty bezpieczeństwa, testy penetracyjne i obowiązek niezwłocznego raportowania incydentów.

Przykład (sektor medyczny):

*W systemie obsługi elektronicznej dokumentacji pacjentów dostawca oprogramowania, który odpowiadał za serwery centralne, został uznany za dostawcę krytycznego. Wprowadzono z nim umowę bezpieczeństwa z osobnymi klauzulami dot. szyfrowania danych, testów kodu oraz lokalizacji serwerów wyłącznie w EOG.*

Przykład (energetyka):

*W operatorze sieci przesyłowej dostawca urządzeń SCADA uznany został za kluczowego, a jego produkty poddawano corocznym audytom bezpieczeństwa zgodnie z ISO/IEC 62443.*

**Dostawcy wspierający**

Drugą grupę stanowią dostawcy wspierający – czyli tacy, których usługi lub produkty są potrzebne dla funkcjonowania organizacji, ale ich przerwanie nie powoduje natychmiastowej utraty ciągłości działania.

Do tej grupy można zaliczyć:

- firmy serwisowe i utrzymaniowe,
- operatorów helpdesków,
- dostawców licencji pomocniczych,
- konsultantów IT,
- dostawców zewnętrznych usług szkoleniowych, testów bezpieczeństwa, integracji systemów.

Dostawcy wspierający powinni być objęci umiarkowanym nadzorem. Od nich również wymaga się stosowania podstawowych standardów bezpieczeństwa – np. polityki dostępu, szyfrowania danych, zarządzania incydentami – ale niekoniecznie certyfikacji systemowej. Istotne jest jednak, by zamawiający ustalił z nimi granice odpowiedzialności: np. kto odpowiada za kopie zapasowe danych, a kto za ochronę środowiska testowego.

Przykład (transport):

*W projekcie inteligentnego systemu zarządzania ruchem miejskim serwisant oprogramowania klasyfikowany był jako dostawca wspierający. Otrzymał dostęp tylko do środowiska testowego, a w umowie zapisano obowiązek anonimizacji danych.*

### Dostawcy niskiego wpływu

Trzecią grupę stanowią dostawcy niskiego wpływu – czyli tacy, którzy nie mają bezpośredniego kontaktu z systemami informatycznymi ani z danymi. Przykłady to:

- dostawcy sprzętu biurowego,
- firmy sprzątające, transportowe, ochrony fizycznej,
- podmioty dostarczające elementy infrastruktury pomocniczej (np. klimatyzacja serwerowni).

Ryzyko w tej grupie jest ograniczone, ale nie zerowe. W praktyce wiele incydentów zaczynało się właśnie od tzw. „tylnego wejścia" – np. zainfekowanego pendrive'a użytego przez serwisanta lub pozostawionych otwartych drzwi do serwerowni. Dlatego i tu należy stosować minimalne zabezpieczenia, takie jak procedury dostępu, szkolenia z ochrony danych, kontrola wstępu do stref bezpieczeństwa. Klasyfikacja dostawców pozwala nie tylko na różnicowanie wymagań, ale także na racjonalne planowanie zasobów nadzoru. Dobrze prowadzona klasyfikacja to fundament proporcjonalności w zarządzaniu ryzykiem – zasada, która jest wspólnym mianownikiem wszystkich norm ISO i wymogów NIS2.

## 4.2.3. Czynniki ryzyka w klasyfikacji

Aby właściwie przyporządkować dostawcę do jednej z kategorii, niezbędna jest analiza czynników ryzyka, które decydują o jego wpływie na bezpieczeństwo organizacji.

W praktyce chodzi o zrozumienie nie tylko, *co* dostawca dostarcza, ale też *w jaki sposób* i *w jakim otoczeniu prawnym i technologicznym* działa.

### Pochodzenie i lokalizacja

Pierwszym i jednym z najważniejszych czynników ryzyka jest pochodzenie dostawcy oraz lokalizacja infrastruktury. Jurysdykcja prawna, w której funkcjonuje dostawca, determinuje, jakie obowiązki ciążą na nim w zakresie ochrony danych i współpracy z organami państwowymi.

Dostawcy spoza Unii Europejskiej mogą podlegać przepisom mniej restrykcyjnym niż te wynikające z RODO czy KSC. W niektórych przypadkach, jak przy dostawcach z państw objętych sankcjami lub o niskim poziomie zaufania, ryzyko staje się nieakceptowalne. Przy ocenie warto korzystać z list i rekomendacji instytucji takich jak ENISA, Komisja Europejska, Agencja Bezpieczeństwa Wewnętrznego czy krajowe centra certyfikacji.

*Przykład (sektor finansowy):*

*Dostawca usług chmurowych, którego centra danych znajdowały się w Azji, został sklasyfikowany jako wysokiego ryzyka ze względu na brak równoważnych gwarancji prawnych w zakresie ochrony danych osobowych.*

**Bezpieczeństwo organizacyjne i techniczne**

Kolejny czynnik to wewnętrzny poziom bezpieczeństwa dostawcy – jego procedury, kultura organizacyjna, polityki bezpieczeństwa, kompetencje personelu i stosowane technologie ochronne. W ocenie pomocne są pytania:

- Czy dostawca posiada ważne certyfikaty (np. ISO/IEC 27001 dla SZBI, ISO 22301 dla ciągłości działania, TISAX w automotive) i czy ich zakres obejmuje procesy/usługi istotne dla tego zamówienia?
- Jak wygląda cykl szkoleń bezpieczeństwa (onboarding + refresh), dla kogo są obowiązkowe i jak jest mierzona skuteczność (np. testy phishingowe, wskaźniki udziału)?
- Czy działa formalny proces zarządzania incydentami (IRP z RACI, progi notyfikacji, integracja z wymogami NIS2/UKSC) i kiedy ostatnio przeprowadzono ćwiczenia?
- Jak realizowane jest zarządzanie podatnościami i łatami (SLA dla CVSS ≥7/≥9, skany przyrostowe, przeglądy wyjątków, raportowanie terminowości)?
- Jak zarządzane są tożsamości i dostępy (zasada najmniejszych uprawnień, MFA dla ról uprzywilejowanych, recertyfikacja uprawnień, rozdział obowiązków)?
- Czy istnieje skuteczny monitoring i rejestrowanie zdarzeń (zakres źródeł logów, retencja, korelacja/SIEM, wskaźniki MTTD/MTTR) oraz dostęp zamawiającego do telemetrii?
- Jak dostawca kontroluje podwykonawców (sub-supply chain) — rejestr, wymogi „down-flow", zasady notyfikacji zmian, prawo sprzeciwu, audyty/oceny równoważności?
- Czy rozwój i utrzymanie oprogramowania podlega SSDLC (przeglądy kodu, SAST/DAST, zarządzanie tajemnicami, SBOM, podpisywanie artefaktów) i jak wygląda procedura reagowania na podatności łańcucha dostaw (np. w bibliotekach)?
- Jak zapewniona jest ciągłość działania i odtwarzanie (RTO/RPO, testy DR, geograficzna redundancja, wyniki ostatnich testów i działania korygujące)?

- Czy dostawca spełnia wymagania regulacyjne i certyfikacyjne właściwe dla przedmiotu (np. zgodność z CRA dla wyrobów z elementem cyfrowym, programy EUCS/EUCC lub krajowe schematy) i czy utrzymuje ich ważność przez cały okres umowy?

Brak dojrzałego podejścia do bezpieczeństwa po stronie dostawcy stanowi tzw. ryzyko organizacyjne – może skutkować błędami ludzkimi, zaniedbaniem obowiązków lub brakiem reakcji w sytuacji kryzysowej.

### Zależności operacyjne i interoperacyjność systemów

Współczesne systemy rzadko działają w izolacji. W realnych projektach ryzyko nie koncentruje się wyłącznie w obrębie pojedynczego systemu, lecz przede wszystkim w połączeniach pomiędzy systemami: interfejsach API, integracjach ETL, współdzielonych segmentach sieci, mechanizmach federacji tożsamości (SSO), kanałach serwisowych oraz ścieżkach zdalnego wsparcia. Oznacza to, że ocena dostawcy powinna obejmować nie tylko jego dojrzałość „wewnętrzną", ale również sposób, zakres i warunki komunikacji z innymi komponentami środowiska, w tym identyfikację stron inicjujących połączenia, używanych metod uwierzytelniania i autoryzacji oraz ochrony transmisji. Kluczowe staje się ustalenie, kto faktycznie kontroluje przepływ danych (procesowo i technicznie), jakie są granice odpowiedzialności za bezpieczeństwo na styku systemów oraz jakie mechanizmy segmentacji i izolacji ograniczają propagację incydentów. W praktyce należy przeanalizować ścieżki ruchu (North–South i East–West), zasady publikacji API, stosowane bramy bezpieczeństwa, zasady rotacji i przechowywania chronionych kluczy, a także tryb udostępniania danych partnerom oraz podwykonawcom. Dopiero taka, relacyjna ocena środowiska — uwzględniająca zarówno logikę integracji, jak i narzędzia kontroli dostępu, monitoringu i reakcji — pozwala wiarygodnie oszacować ekspozycję na zagrożenia i wyznaczyć adekwatne wymagania kontraktowe.

Co należy zidentyfikować?

- Mapa integracji i przepływów danych: lista API (kto woła kogo, jakie metody, jakie dane), kolejki/ESB, ETL, konektory, szyfrowanie w ruchu/spoczynku, miejsca składowania, kopie.
- Współdzielone zasoby: segmenty sieci, klastry, bazy, konta chmurowe, tożsamości i role (SSO, konta serwisowe).

- Zależności krytyczne: systemy, bez których usługa nie działa (np. DNS, PKI, IdP, billing, CRM), wraz z właścicielem i jurysdykcją.
- Kanały serwisowe i „tylne drzwi": VPN serwisowy, zdalny pulpit, porty zarządzania, break-glass accounts.

Przykład (telekomunikacja):

*W jednym z projektów teleinformatycznych wykazano, że zewnętrzny system fakturowania posiadał niezaszyfrowane połączenie z głównym serwerem danych. Po analizie interoperacyjności wprowadzono segmentację sieci i ograniczenie dostępu.*

**Reputacja, zdolność reakcji i dojrzałość bezpieczeństwa**

Reputacja dostawcy w obszarze bezpieczeństwa to nie kwestia wizerunkowa, lecz empiryczny wskaźnik ryzyka: pokazuje, jak firma zachowuje się pod presją, czy potrafi zarządzać kryzysem i czy traktuje klientów po partnersku. Wiarygodniejszy jest podmiot, który transparentnie ujawnia incydenty, publikuje biuletyny bezpieczeństwa, szybko dostarcza poprawki i prowadzi otwartą komunikację, niż ten, który opóźnia informacje, minimalizuje problem lub ogranicza dialog. Dlatego ocena reputacyjna powinna być ustrukturyzowana i oparta na mierzalnych śladach działania.

Po pierwsze, warto sprawdzić historię incydentów i sposób komunikacji: czy dostawca utrzymuje stałą stronę z biuletynami bezpieczeństwa, czy wydaje *security advisories* z CVE/CVSS i instrukcjami obejść, czy posiada formalną politykę koordynowanego ujawniania podatności (CVD) i aktywny PSIRT (Product Security Incident Response Team). Po drugie, należy zweryfikować zdolność reakcji operacyjnej w liczbach: średni czas detekcji (MTTD) i reakcji (MTTR) dla kategorii zagrożeń, medianę czasu publikacji łatek dla CVSS ≥9.0 oraz odsetek wdrożeń w deklarowanych terminach. Po trzecie, przydatne są zewnętrzne źródła: ostrzeżenia CERT/CSIRT, komunikaty ENISA, publiczne bazy incydentów, a także wyniki niezależnych audytów lub testów (jeśli publikowane). Po czwarte, należy ocenić kulturę przejrzystości: raporty roczne o bezpieczeństwie, program bug bounty, deklaracje zgodności z CRA/programami UE (EUCS/EUCC) lub krajowymi schematami, a także praktykę przekazywania SBOM.

W dokumentacji i umowie warto wiązać reputację z konkretnymi dowodami: obowiązek publikacji advisory do X godzin od potwierdzenia podatności, terminy łatania zależne od CVSS, cykliczne raporty z metrykami MTTD/MTTR, dostęp do

kanału PSIRT i harmonogram przeglądów bezpieczeństwa. Dodatkowo można zastrzec prawo do audytu incydentalnego, gdy pojawią się negatywne sygnały z CERT/ENISA lub gwałtowny wzrost niezgodności.

Przykład (przemysł):

*Przy wyborze dostawcy SCADA, dwie oferty były funkcjonalnie podobne, lecz tylko jedna firma utrzymywała publiczny rejestr advisory, publikowała poprawki w ciągu 72 godzin dla CVSS ≥9.0 i raportowała kwartalne MTTD/MTTR. W ocenie dojrzałości została uznana za niższe ryzyko operacyjne i wybrana jako bezpieczniejszy partner.*

### 4.2.4. Narzędzia i techniki oceny

Sama identyfikacja czynników ryzyka to dopiero początek. Kluczowe jest wdrożenie konkretnego zestawu narzędzi i technik oceny**,** które pozwolą te czynniki mierzyć, porównywać, priorytetyzować i rzetelnie dokumentować w całym cyklu życia umowy. Nowoczesne organizacje – zarówno publiczne, jak i prywatne – stosują tu podejście warstwowe**:** od ustrukturyzowanych ankiet samooceny i przeglądów dokumentacyjnych, przez due diligence techniczno-prawne oraz testy praktyczne (skany podatności, przeglądy konfiguracji, testy odtwarzania), aż po zaawansowane systemy analizy reputacyjnej i automatycznego monitoringu cyberryzyka (telemetria bezpieczeństwa, wskaźniki KRI, alerty z CERT/ENISA, obserwacja zewnętrznej powierzchni ataku). Warstwy te powinny być połączone jedną matrycą oceny i zasilane danymi źródłowymi o znanej jakości (artefakty NIST/ISO, certyfikacje UE/krajowe, SBOM, raporty z audytów i testów).

1. **Self-assessment (samoocena dostawcy)**

Samoocena to szybkie „sitko" ryzyka na wejściu: dostawca wypełnia krótki, ustrukturyzowany kwestionariusz oparty na ISO/IEC 27001 i 27036, a zamawiający zyskuje porównywalny obraz dojrzałości. Kluczem jest prostota i weryfikowalność – pytania powinny dotyczyć rzeczy mierzalnych (np. MFA dla ról admin, procedura IR, terminy łatania podatności), a odpowiedzi uzupełnione drobnym dowodem (nr certyfikatu, zrzut konfiguracji, link do polityki). Taki formularz pozwala szybko przypisać wykonawcę do kategorii ryzyka i zdecydować, czy przejść do pogłębionej weryfikacji.

Minimalnie warto uwzględnić:

- zakres i ważność certyfikacji (np. ISO/IEC 27001) oraz status ostatniego audytu nadzorczego,

- istnienie i podstawowe parametry IRP/BCP,
- sposób zarządzania podatnościami (SLA zależne od CVSS) i informację o podwykonawcach.

**2. Due diligence dostawcy**

Pogłębiona weryfikacja sprawdza „twarde" dowody: dokumenty, konfiguracje, wyniki testów i status certyfikacji. W praktyce oznacza to przejrzenie polityk i procesów (incydenty, ciągłość, zarządzanie dostępami), weryfikację zakresu certyfikatów i ich aktualności, a przy komponentach cyfrowych — także zgodności z CRA i dostępności SBOM. Wykonuje się też przegląd próbek konfiguracji (szyfrowanie, segmentacja, MFA), a przy wyższym ryzyku — przegląd raportów ze skanów i testów penetracyjnych wraz z planami działań korygujących. Wynik powinien kończyć się decyzją: akceptacja, akceptacja warunkowa (z CAP) lub odrzucenie.

Minimalnie warto uwzględnić:

- potwierdzenie zakresu certyfikacji (czy pokrywa usługi z kontraktu),
- SBOM i ścieżkę łatania krytycznych CVE,
- rejestr podwykonawców i zasady „down-flow" (przenoszenie wymagań na łańcuch).

Przykład (branża wodno-kanalizacyjna):

*W projekcie inteligentnego systemu monitorowania ciśnienia dostawca urządzeń został zobowiązany do przedstawienia SBOM. Dzięki temu ujawniono użycie komponentu open source z luką bezpieczeństwa, który został zastąpiony przed wdrożeniem.*

**3. Zewnętrzne bazy ryzyka i analityka cyberzagrożeń**

Ocena „z zewnątrz" uzupełnia obraz dostawcy danymi niezależnymi od jego deklaracji. Publiczne raporty (np. ENISA, CERT) oraz komercyjne ratingi powierzchni ataku pokazują, czy domeny są właściwie skonfigurowane, certyfikaty aktualne, a reputacja sieciowa stabilna. Takie źródła warto traktować jako czujnik wczesnego ostrzegania — sygnał do zadania pytań i poproszenia o dowody, a nie samodzielny wyrok. W umowie przydaje się prosty mechanizm: jeśli wskaźnik spada poniżej progu albo pojawia się alert z CERT/ENISA, wykonawca przedstawia wyjaśnienia i plan naprawczy, a zamawiający może uruchomić audyt incydentalny.

Praktycznie sprawdza się, gdy monitorujemy:

- nagłe pogorszenie oceny/reputacji lub wyciek związany z domeną dostawcy,
- przeterminowane certyfikaty i ekspozycję usług,
- korelację alertów z realnymi dowodami (logi, zgłoszenia, zmiany konfiguracji).

### 4.2.5. Dokumentowanie i klasyfikowanie wyników – rejestr ryzyk dostawców (Supplier Risk Register)

Rejestr ryzyk dostawców powinien być centralnym systemem pracy, a nie archiwalnym plikiem. Jego zadaniem jest nie tylko „zapisać wynik oceny", lecz uruchamiać działania: wyznaczać priorytety przeglądów, automatycznie podbijać poziom nadzoru po incydencie, przypominać o wygaśnięciu certyfikatu czy eskalować sprawy, gdy przekroczone zostaną progi ryzyka.

W dobrze zaprojektowanym rejestrze powinny znaleźć się:

- dane identyfikacyjne dostawcy (nazwa, NIP, lokalizacja, właściciel),
- opis zakresu współpracy (produkt, usługa, system),
- poziom ryzyka (np.: A – wysoki, B – umiarkowany, C – niski),
- uzasadnienie klasyfikacji (główne czynniki ryzyka),
- zastosowane środki kontroli (audyt, monitoring, klauzule bezpieczeństwa),
- termin i wynik ostatniej weryfikacji,
- osoba odpowiedzialna za relację i nadzór.

Rejestr powinien być ściśle skorelowany z procesem zakupowym i operacjami. Należy definiować zdarzenia, które automatycznie aktualizują poziom nadzoru: zmiana zakresu umowy, pojawienie się nowego podwykonawcy, migracja danych poza EOG, zawieszenie/wygaśnięcie certyfikacji (ISO 27001/EUCS/EUCC/krajowy schemat), publikacja krytycznego CVE w SBOM, alert z CERT/ENISA, istotny wzrost MTTD/MTTR. Po każdym takim zdarzeniu rejestr powinien generować zadanie: przegląd ryzyka (27005), aktualizację CAP, ewentualnie uruchomienie audytu incydentalnego. Praktyczny rejestr ryzyk to panel sterowania: pokazuje, którym dostawcom należy poświęcić uwagę dziś, jakie dowody są zaległe, gdzie zbliża się termin audytu, a gdzie trzeba natychmiast uruchomić CAP. Dzięki temu nadzór nad łańcuchem dostaw jest ciągły, proporcjonalny i obronny dowodowo — dokładnie taki, jakiego wymagają współczesne regulacje i standardy.

*Przykład (branża medyczna):*

*W szpitalu realizującym zamówienia w trybie PZP rejestr ryzyk ujawnił, że dwaj niezależni dostawcy usług SaaS korzystają z tego samego podwykonawcy tożsamości (IdP). Gdy pojawił się alert o kradzieży tokenów u jednego z dostawców, zamawiający*

*— mając w rejestrze powiązania i SBOM integracji — w ciągu kilkunastu minut odnalazł drugi, analogiczny punkt zależności. Natychmiast uruchomiono rotację kluczy, skrócenie TTL tokenów, wymuszono mTLS na krytycznych ścieżkach oraz czasowo zablokowano wybrane integracje API do czasu retestu. Dzięki z góry zdefiniowanym progom KRI i ścieżce CAP incydent ograniczono do krótkiej przerwy w dostępie bez utraty danych i bez wpływu na systemy o najwyższej krytyczności. W sektorze publicznym rejestr ryzyk może też pełnić rolę narzędzia kontroli międzyresortowej – np. umożliwia przekazywanie informacji o dostawcach wysokiego ryzyka między instytucjami, co znacząco podnosi odporność całego systemu administracji*.

## 4.3. Weryfikacja zgodności wykonawców z wymaganiami prawnymi i technicznymi

Proces weryfikacji wykonawców, jakkolwiek często postrzegany jako formalny etap w toku postępowania o udzielenie zamówienia publicznego, w istocie stanowi jedno z kluczowych ogniw zarządzania ryzykiem w całym łańcuchu dostaw, ponieważ to właśnie na tym etapie zapada decyzja o tym, komu powierzona zostanie odpowiedzialność za integralność, dostępność i bezpieczeństwo zasobów informacyjnych zamawiającego. Nie jest to zatem wyłącznie kwestia zgodności dokumentacyjnej, lecz moment, w którym teoria zarządzania ryzykiem spotyka się z praktyką — a zamawiający, kierując się zasadą należytej staranności, musi umieć rozpoznać, które z ryzyk są akceptowalne, które wymagają ograniczenia, a które – z racji swojej skali lub charakteru – powinny skutkować wykluczeniem oferenta z dalszego postępowania.

W praktyce weryfikacja zgodności wykonawców stanowi więc narzędzie nie tylko prawne, ale strategiczne: pozwala bowiem przełożyć złożone wymogi regulacyjne, normatywne i branżowe na konkretne kryteria oceny bezpieczeństwa, które następnie można wykorzystać w analizie ryzyka kontraktowego i w budowaniu kultury cyberodporności całej organizacji.

### 4.3.1. Wymagania związane z zarządzaniem ryzykiem wynikające z przepisów UE i krajowych (NIS2, CRA, RODO, UKSC, Pzp)

Ramowy kontekst prawny, w którym funkcjonują współczesne zamówienia publiczne, tworzy system spójny, choć wielowarstwowy – system, w którym bezpieczeństwo informacyjne, ochrona danych i zarządzanie ryzykiem są ze sobą nierozerwalnie związane. Każdy z aktów prawnych — NIS2, CRA, RODO, UKSC czy Prawo zamówień publicznych — wnosi odmienny akcent do tego pejzażu, lecz

dopiero ich wspólne zastosowanie pozwala na zbudowanie realnej, a nie deklaratywnej odporności organizacyjnej.

Dyrektywa NIS2, będąca fundamentem europejskiego systemu cyberbezpieczeństwa, przenosi odpowiedzialność z reaktywnego na proaktywne zarządzanie ryzykiem. Oznacza to, że zamawiający – podmiot publiczny nie może ograniczyć się do badania, czy wykonawca posiada „system bezpieczeństwa", lecz powinien zrozumieć, w jaki sposób ten system działa w praktyce, czy jest on powiązany z mechanizmami oceny ryzyka oraz czy obejmuje swoim zakresem także łańcuch dostaw i podwykonawców. Zarządzanie ryzykiem w duchu NIS2 nie polega więc na statycznym spełnieniu wymogów formalnych, ale na utrzymaniu dynamicznej zdolności do reagowania, co wymaga nie tylko kompetencji technicznych, lecz również dojrzałości organizacyjnej i świadomości odpowiedzialności prawnej.

CRA – ryzyko „wbudowane w produkt" i obowiązki poprodukcyjne. CRA doprecyzowuje, że wyrób z elementem cyfrowym wnosi własne ryzyko, za które odpowiada producent i – po stronie zamawiającego – proces zakupowy. Ocena ofert nie może zatem kończyć się na parametrach i cenie. Musi obejmować:

(1) zgodność projektową (security by design),

(2) bezpieczne ustawienia domyślne (security by default),

(3) zarządzanie lukami w całym cyklu życia (polityka aktualizacji, kanał zgłoszeń podatności, SBOM). Po wyborze oferty wymagania te trzeba utrzymać umownie: czasy reakcji na krytyczne CVE, zasady komunikacji o podatnościach, dowody wdrożenia poprawek oraz powiązanie z monitoringiem KRI po stronie zamawiającego.

RODO, czyli ogólne rozporządzenie o ochronie danych, wprowadza w tę układankę wymiar etyczny i społeczny – przypomina, że ryzyko nie dotyczy jedynie systemów informatycznych, lecz realnych ludzi, których dane są powierzane instytucjom publicznym.
Weryfikacja wykonawcy w świetle RODO nie może zatem sprowadzać się do formalnej klauzuli o przetwarzaniu danych, lecz powinna obejmować ocenę zdolności organizacji do zapewnienia rozliczalności, prowadzenia analiz ryzyka (DPIA) oraz reagowania na incydenty naruszenia poufności.

W UKSC zamawiający nie jest „obserwatorem" bezpieczeństwa swoich wykonawców, lecz uczestnikiem krajowego mechanizmu zarządzania ryzykiem: identyfikuje ekspozycję, nadaje wymogi proporcjonalne do ryzyka, zbiera dowody ich spełniania, a w razie potrzeby aktywnie współpracuje z właściwymi CSIRT-ami (MON, NASK, GOV) i organami nadzoru. Przekłada się to na obowiązki zarówno ex ante (jak konstruujemy postępowanie i umowę), jak i ex post (jak prowadzimy nadzór w trakcie realizacji).

Po pierwsze, każdy wybór dostawcy jest akceptacją określonego poziomu ryzyka. UKSC implikuje więc konieczność kategoryzacji dostawców (np. krytyczni / wspierający / niskiego wpływu) i „doszycia" do kategorii adekwatnego rygoru: od wymogów dojrzałości organizacyjnej (np. ISO/IEC 27001 w zakresie obejmującym świadczenie) po dowody na poziomie komponentu/usługi (certyfikacja UE/krajowa, zgodność z CRA, SBOM). W praktyce oznacza to, że już w OPZ i aneksie bezpieczeństwa należy zdefiniować minimalne kontrolki (monitoring, logowanie, zarządzanie podatnościami z terminami zależnymi od CVSS), zasady dla podwykonawców (down-flow), a także metryki, które będą później sprawdzane (MTTD/MTTR, terminowość łatek, status certyfikacji).

Po drugie, nadzór ex post w UKSC jest obowiązkowy i ciągły, a nie „od audytu do audytu". Zamawiający prowadzi rejestr ryzyk dostawców i regularne przeglądy profilu ryzyka (np. kwartalnie dla kategorii wysokiej), utrzymuje progi eskalacyjne (co wywołuje działania nadzwyczajne) oraz ma gotowe ścieżki reagowania: audyt incydentalny, plan działań korygujących (CAP) z terminami i właścicielami, a w skrajnych przypadkach – wstrzymanie świadczenia lub odstąpienie (proporcjonalnie do ryzyka). Progi eskalacji powinny być mierzalne i z góry ogłoszone wykonawcy: zawieszenie certyfikacji, poważny alert CSIRT/ENISA dotyczący wykorzystywanego komponentu, niespełnienie SLA łatek dla CVSS ≥9, istotna zmiana w łańcuchu poddostawców lub migracja danych poza EOG bez uprzedniej oceny ryzyka.

UKSC zakłada także gotowość do współpracy operacyjnej z CSIRT-ami. Wymusza to po stronie zamawiającego utrzymywanie telemetrii i logów (zdefiniowane źródła, czas retencji, integralność), aby móc szybko dokonać triage'u incydentu i – gdy zachodzi obowiązek – notyfikować w wymaganych horyzontach czasowych (wstępna informacja, raport uzupełniający, raport końcowy). Żeby ta współpraca była realna, w umowie należy zastrzec dostęp do niezbędnych danych (logi, konfiguracje, artefakty z testów), punkty kontaktowe (24/7) oraz obowiązek

koordynowanego ujawniania podatności, tak aby wykonawca nie opóźniał informacji o lukach czy poprawkach.

Istotnym elementem UKSC jest spójność nadzoru w łańcuchu dostaw. Zamawiający powinien mieć prawo do informacji i wglądu także u podwykonawców kluczowych (przynajmniej w zakresie dowodów zgodności i reakcji na incydenty), a zmiany w sub-supply chain muszą być uprzednio zgłaszane i akceptowane po krótkiej ocenie ryzyka. Wpisuje się w to zasada „jednego biletu eskalacyjnego": jeśli sygnał ryzyka dotyczy komponentu wspólnego dla kilku usług, jeden proces eskalacji obejmuje wszystkie kontrakty dotknięte tym komponentem. Na końcu UKSC wzmacnia rozliczalność: każdy wymóg powinien mieć odpowiadający mu dowód (artefakt) i częstotliwość dostarczania, a każde przekroczenie progu – udokumentowaną reakcję. Dzięki temu zgodność z ustawą przestaje być deklaracją w SWZ/OPZ, a staje się działającym reżimem zarządczym: wiadomo, jakie ryzyko przyjęto, jakie dowody to potwierdzają, kiedy należy eskalować i jak zamyka się działania korygujące.

Prawo zamówień publicznych, choć nie odnosi się bezpośrednio do cyberbezpieczeństwa, wyraźnie nakłada na zamawiających obowiązek zachowania należytej staranności, przejrzystości i proporcjonalności w konstruowaniu wymagań.

Z perspektywy zarządzania ryzykiem oznacza to, że każde postępowanie o udzielenie zamówienia publicznego jest procesem równoważenia wartości – pomiędzy efektywnością ekonomiczną a bezpieczeństwem systemowym.

### 4.3.2. Wymagania normatywne i branżowe (ISO/IEC 27001, 27002, 27005, 27036, 28000, NIST SP 800-161)

Normy i standardy branżowe pełnią rolę pomostu między prawem a praktyką. Podczas gdy przepisy określają, co należy osiągnąć, normy precyzują, jak to zrobić — w sposób systemowy, powtarzalny i możliwy do weryfikacji. W tym sensie stanowią one język zarządzania ryzykiem, zrozumiały zarówno dla informatyków, jak i prawników, menedżerów, audytorów czy inspektorów bezpieczeństwa. Ich znaczenie w zamówieniach publicznych rośnie z roku na rok, ponieważ pozwalają zamawiającym dokonywać oceny nie intuicyjnie, ale według wspólnych, obiektywnych kryteriów.

Norma **ISO/IEC 27001** jest kamieniem węgielnym systemowego podejścia do bezpieczeństwa informacji.

Nie ogranicza się ona do wskazania wymagań, lecz tworzy spójny model zarządzania, w którym proces identyfikacji, analizy i traktowania ryzyka jest cyklem ciągłym, obejmującym zarówno fazę planowania, jak i kontrolę efektywności działań. Dla zamawiającego publicznego oznacza to, że wykonawca posiadający certyfikat ISO/IEC 27001 nie tylko wdrożył określone procedury, ale dowiódł, iż rozumie logikę ryzyka i potrafi ją stosować w codziennej praktyce organizacyjnej. Taki wykonawca jest partnerem, który nie reaguje na incydenty przypadkowo, lecz w ramach uporządkowanego mechanizmu decyzyjnego.

**ISO/IEC 27002** rozszerza tę koncepcję o konkretne środki bezpieczeństwa – od zarządzania dostępem i kryptografii, przez bezpieczeństwo chmurowe, aż po nadzór nad dostawcami zewnętrznymi.

Można powiedzieć, że ISO/IEC 27001 określa architekturę systemu bezpieczeństwa, natomiast ISO/IEC 27002 opisuje jego wyposażenie techniczne i operacyjne. Dzięki temu zamawiający ma możliwość nie tylko weryfikacji formalnej zgodności, ale także oceny, czy wykonawca stosuje rozwiązania proporcjonalne do rodzaju danych, jakie będą przetwarzane, i do ryzyk, jakie niesie dany projekt. W praktyce często spotyka się sytuacje, w których organizacja deklaruje wdrożenie ISO/IEC 27001, lecz nie utrzymuje zgodności z kontrolami ISO/IEC 27002 — dlatego kluczowe jest, aby zamawiający analizował oba standardy łącznie, traktując je jako element jednej struktury zarządzania ryzykiem.

Norma **ISO/IEC 27005** jest swoistym „mózgiem” całego systemu, ponieważ to właśnie ona definiuje proces identyfikacji i oceny ryzyk. W jej duchu ocena wykonawcy nie polega na pytaniu, czy posiada zabezpieczenia, lecz raczej czy wie, przed czym się zabezpiecza i dlaczego w taki sposób. Zarządzanie ryzykiem staje się tu procesem poznawczym – metodą, dzięki której organizacja rozumie, jakie czynniki mogą zagrozić jej misji i jak można je ograniczyć w sposób racjonalny ekonomicznie. Dla zamawiających to szczególnie cenne, gdyż pozwala nie tylko na obiektywną ocenę dojrzałości dostawcy, ale także na porównywanie wielu wykonawców na wspólnej osi ryzyka.

Z kolei **ISO/IEC 27036** wprowadza zasady bezpieczeństwa w relacjach zewnętrznych, obejmujących dostawców, partnerów i podwykonawców. Jej kluczową wartością jest podejście relacyjne — norma uczy, że zarządzanie ryzykiem w łańcuchu dostaw jest procesem obustronnym. Nie wystarczy, że zamawiający wprowadzi wymogi, a wykonawca je spełni; istotne jest, by obie strony potrafiły współdziałać w utrzymaniu bezpieczeństwa i otwarcie komunikować się w sytuacjach kryzysowych. Tym samym ISO/IEC 27036 promuje model partnerstwa opartego na zaufaniu, ale i kontroli – równowadze pomiędzy przejrzystością a odpowiedzialnością.

Warto również wspomnieć o normie ISO/IEC **28000**, która wywodzi się z zarządzania bezpieczeństwem w logistyce i transporcie, lecz z powodzeniem znajduje zastosowanie w sferze cyfrowej. Wskazuje ona, że bezpieczeństwo łańcucha dostaw nie jest zagadnieniem wyłącznie informatycznym, lecz ma charakter interdyscyplinarny – obejmuje przepływ danych, materiałów, energii i ludzi. W kontekście zamówień publicznych, szczególnie w sektorach infrastrukturalnych i energetycznych, stanowi ona cenne narzędzie identyfikacji punktów krytycznych w całym procesie realizacji umowy.

Wreszcie NIST SP 800-161, będący jednym z najdojrzalszych opracowań z obszaru zarządzania ryzykiem w łańcuchach dostaw, proponuje model, w którym kluczowe znaczenie mają czynniki jakościowe: reputacja dostawcy, przejrzystość procesu wytwórczego, historia incydentów bezpieczeństwa czy stopień kontroli nad komponentami oprogramowania. Dla zamawiających w Unii Europejskiej może on stanowić inspirację do pogłębienia własnych procedur oceny – zwłaszcza tam, gdzie łańcuchy dostaw są rozległe i obejmują podmioty spoza UE.

### 4.3.3. Mechanizmy weryfikacji w dokumentacji o udzielenie zamówienia publicznego.

Jeśli normy stanowią teoretyczne ramy zarządzania ryzykiem, to dokumenty zamówienia są jego praktycznym laboratorium. To w nich – w SWZ, w OPZ, w projektach umów i załącznikach technicznych – materializuje się to, co wcześniej określono w strategiach bezpieczeństwa czy w politykach zarządzania ryzykiem. Dlatego też prawidłowo skonstruowana dokumentacja postępowania o udzielenie

zamówienia publicznego nie jest zbiorem formalnych wymogów, lecz narzędziem zarządzania ryzykiem kontraktowym, pozwalającym zamawiającemu przewidzieć, ograniczyć i rozłożyć ryzyka jeszcze przed podpisaniem umowy.

Weryfikacja wykonawcy zaczyna się zwykle od złożenia oświadczeń i dokumentów (np. certyfikatów). Choć mają one charakter formalny, ich znaczenie nie może być bagatelizowane, ponieważ stanowią one podstawowy filtr odpowiedzialności — pierwsze sito, które pozwala odróżnić wykonawców poważnych od przypadkowych. Oświadczenia powinny jednak zawsze być poparte dowodami: certyfikatami ISO, raportami z audytów, potwierdzeniami zgodności z CRA czy dokumentami potwierdzającymi wdrożenie zasad RODO. Każdy z tych dokumentów nie tylko dowodzi zgodności, ale pełni funkcję wskaźnika kultury bezpieczeństwa danej organizacji.

Kolejnym poziomem weryfikacji są raporty z audytów lub testów penetracyjnych, które stanowią empiryczny dowód stanu bezpieczeństwa. W praktyce coraz częściej zamawiający wymagają przedstawienia wyników audytu z ostatnich dwunastu miesięcy, obejmujących m.in. ocenę zabezpieczeń sieciowych, kontroli dostępu i mechanizmów reagowania na incydenty. Takie raporty pozwalają na porównanie faktycznej dojrzałości różnych wykonawców i ustalenie, czy deklarowana zgodność jest rzeczywiście utrzymywana w czasie.

Nie można również pomijać potwierdzeń zgodności z rozporządzeniem CRA, które nabierają szczególnego znaczenia w kontekście zakupu sprzętu i oprogramowania ICT. Wymaganie od wykonawców certyfikatów bezpieczeństwa produktów nie jest przejawem nadmiernej ostrożności, lecz racjonalnym sposobem ograniczania ryzyka wprowadzenia do systemu elementów o nieznanym pochodzeniu lub z nieujawnionymi podatnościami. Zamawiający, który wprowadza takie wymogi, w istocie inwestuje w spokój operacyjny na lata.

Wreszcie, nieocenioną rolę w dokumentach zamówienia odgrywają klauzule kontraktowe dotyczące bezpieczeństwa i zarządzania ryzykiem. Ich treść decyduje o tym, jak zamawiający będzie mógł egzekwować zgodność w trakcie realizacji umowy – czy będzie miał prawo do audytu, jak będą raportowane incydenty, kto ponosi koszty działań naprawczych, a także jak wygląda proces przekazania danych po zakończeniu współpracy. W ten sposób prawo i bezpieczeństwo spotykają się w jednym punkcie: w praktyce egzekwowania odpowiedzialności.

### 4.3.4. Weryfikacja ex ante i ex post – rola zamawiającego jako strażnika ryzyka.

Zarządzanie ryzykiem w łańcuchu dostaw nie jest wydarzeniem jednorazowym, lecz ciągłym procesem**,** który obejmuje cały cykl życia kontraktu — od pierwszych założeń i wszczęcia postępowania, przez ocenę ofert, negocjacje (w zależności od trybu udzielenie zamówienia) i wdrożenie, aż po utrzymanie, zmiany zakresu oraz uporządkowane zakończenie współpracy. W każdym z tych etapów profil ryzyka może się istotnie zmieniać: pojawiają się nowe integracje, podwykonawcy, aktualizacje oprogramowania, a także uwarunkowania prawne i organizacyjne, które wpływają na odpowiedzialność stron. Dlatego zarządzanie ryzykiem wymaga rytmu i dyscypliny — regularnych przeglądów, udokumentowanych decyzji o akceptacji lub redukcji ryzyka oraz spójnej ścieżki eskalacji, gdy parametry bezpieczeństwa zaczynają odbiegać od przyjętych progów.

W tym kontekście weryfikacja wykonawców powinna mieć charakter dwufazowy: prewencyjny (ex ante) i kontrolny (ex post). Faza ex ante pozwala świadomie zdefiniować akceptowalny poziom ryzyka przed wyborem oferty — zweryfikować dojrzałość dostawcy, jego łańcuch poddostawców, gwarancje prawne i techniczne oraz spójność proponowanych środków ochrony z wymaganiami zamawiającego. Faza ex post utrzymuje ten poziom w praktyce: zapewnia ciągłość nadzoru, dostarcza świeżych danych o zgodności i incydentach, wymusza aktualizację wymagań przy zmianach technologicznych czy organizacyjnych i zamyka pętlę doskonalenia (lessons learned → poprawione zapisy umowne i procedury). Tylko takie podejście — łączące przezorność na wejściu z konsekwentnym monitorowaniem w trakcie — pozwala reagować proporcjonalnie do realnych zagrożeń, zamiast polegać na jednorazowej deklaracji zgodności.

**Weryfikacja ex ante** to moment, w którym zamawiający – zanim jeszcze złoży podpis pod umową – świadomie waży ryzyka: nie tylko te widoczne w tabeli parametrów, ale też te „miękkie", związane z reputacją, praktyką zarządzania i kulturą bezpieczeństwa wykonawcy. Ocenie podlega więc nie tylko sama oferta, lecz także sposób, w jaki dostawca zarządza ryzykiem: czy ma działający SZBI (np. ISO/IEC 27001) o właściwym zakresie, czy potrafi dokumentować zgodność z kontrolkami (ISO/IEC 27002), czy zna i stosuje zasady dla relacji z podwykonawcami (ISO/IEC 27036) oraz czy jego produkty/usługi wchodzące do ekosystemu spełniają wymogi CRA i – tam gdzie to właściwe – programów certyfikacji UE lub krajowych. Równolegle analizuje się wiarygodność operacyjną**:** wyniki audytów i testów bezpieczeństwa, gotowość do przekazywania SBOM, wskaźniki reakcji na podatności (terminy łatek vs. CVSS), a także stabilność finansową i organizacyjną**,** bo ryzyko utraty ciągłości dostaw bywa tak samo

dotkliwe, jak podatność techniczna. Dobrze przeprowadzona ocena ex ante kończy się jasnym sformułowaniem poziomu ryzyka akceptowalnego dla danego postępowania i wpisaniem tego poziomu do rejestru ryzyk wraz z planem zabezpieczeń (np. wymagana certyfikacja, rytm raportów, prawo audytu). Celem nie jest ograniczanie konkurencji ani „odsiewanie" wykonawców dla samego odsiewania, lecz świadome przyjęcie takiego poziomu ryzyka, który — przy odpowiednich środkach kontraktowych i technicznych — pozostaje proporcjonalny do korzyści i możliwy do nadzorowania.

**Weryfikacja ex post**, prowadzona już w trakcie realizacji umowy, zamienia deklaracje z etapu ofertowego w sprawdzalne fakty**.** Zamawiający, który dba o bezpieczeństwo kontraktu, nie poprzestaje na ocenie wstępnej: utrzymuje rytm nadzoru (raporty z KRI, przeglądy ryzyka, spotkania operacyjne), weryfikuje dostarczane dowody (logi, wyniki skanów, status certyfikacji, aktualizacje SBOM), nadzoruje zarządzanie zmianą (nowe wersje, nowi podwykonawcy, zmiany lokalizacji danych) oraz – gdy to konieczne – uruchamia działania korygujące (CAP) lub audyty incydentalne. Ten nadzór ma charakter partnerski: chodzi o wspólne podtrzymywanie zdolności do wykrywania i ograniczania ryzyk, a nie o szukanie potknięć. Dlatego ex post obejmuje również reakcję na sygnały z zewnątrz (np. alerty CSIRT/ENISA, nowe CVE o wysokim CVSS), aktualizację wymagań w odpowiedzi na zmiany regulacyjne lub techniczne i – w razie potrzeby – przegląd poziomu ryzyka wpisanego w rejestrze. Tam, gdzie ten dialog i dyscyplina dowodowa są utrzymane, ryzyko stabilnie maleje; tam, gdzie kontrola wygasa po podpisaniu umowy, ryzyko nie znika, a jedynie ukrywa się do czasu kolejnego incydentu.

Rola zamawiającego w tym układzie jest niezwykle istotna: nie jest on biernym odbiorcą usług, ale **strażnikiem ryzyka** – podmiotem, który nie tylko analizuje i ocenia, ale również kształtuje świadomość bezpieczeństwa w całym łańcuchu dostaw. Dobrze zaprojektowany system kontroli ex post pozwala na wczesne wykrywanie niezgodności, identyfikację nowych zagrożeń, a także adaptację wymagań do zmieniających się realiów technologicznych.
W ten sposób zamawiający przestaje być administratorem umowy, a staje się aktywnym uczestnikiem systemu cyberodporności.

W praktyce można powiedzieć, że to właśnie etap weryfikacji ex post decyduje o tym, czy zarządzanie ryzykiem jest żywym procesem, czy tylko deklaracją. Tam, gdzie zamawiający utrzymuje regularny dialog z wykonawcą, reaguje na wyniki

audytów, analizuje incydenty i aktualizuje swoje wymagania, tam ryzyko maleje. Tam zaś, gdzie kontrola ustaje po podpisaniu umowy, ryzyko nie znika – po prostu przechodzi w stan utajony.

### 4.4. Monitorowanie i audyt dostawców w trakcie realizacji umowy

Etap realizacji umowy w zamówieniach publicznych to moment prawdy dla bezpieczeństwa łańcucha dostaw: dopiero tutaj widać, czy zaprojektowane wcześniej mechanizmy zarządzania ryzykiem są wystarczająco skuteczne, odporne i elastyczne, by sprostać realnym zagrożeniom i zmianom organizacyjnym. Profil ryzyka nie jest stały — ewoluuje wraz z kolejnymi wdrożeniami, aktualizacjami oprogramowania, pojawieniem się nowych integracji i podwykonawców, a także wraz ze zmianami regulacyjnymi. Dlatego to, co zadziałało na etapie ex ante, trzeba utrzymywać, mierzyć i korygować przez cały okres obowiązywania kontraktu.

Współczesne organizacje — zarówno publiczne, jak i z sektorów strategicznych — coraz wyraźniej widzą, że nadzór nad dostawcami nie może ograniczać się do jednorazowej weryfikacji, lecz musi przybrać formę ciągłego, wielowymiarowego monitoringu. Chodzi o takie ułożenie procesu, aby dane operacyjne (telemetria, logi, wskaźniki KRI), obserwacje audytowe (planowe i incydentalne) oraz wnioski z incydentów i testów (np. DR, testy bezpieczeństwa) tworzyły zintegrowany obraz ryzyka i prowadziły do świadomych decyzji: wzmocnienia zabezpieczeń, działań korygujących (CAP), zmian w łańcuchu poddostawców albo — jeśli trzeba — modyfikacji wymagań umownych.

Właściwie zaprojektowany system monitorowania i audytu ma charakter proaktywny: jego zadaniem jest nie tylko wychwytywanie odchyleń od normy, ale także analiza trendów (np. wydłużający się MTTR, spadek terminowości łatek dla CVSS≥7, wzrost incydentów w określonej klasie systemów) i prognozowanie skutków, zanim zaczną materializować się straty. Taki system działa najlepiej wtedy, gdy jest „zszyty” z architekturą wymagań: korzysta z tych samych definicji i dowodów, które pojawiły się w OPZ i aneksie bezpieczeństwa (np. SBOM, raporty z testów, status certyfikacji UE/krajowej, zgodność z CRA), a jego progi eskalacyjne korespondują z zapisami o audycie incydentalnym i CAP.

Nie jest to zatem mechanizm „polowania na błędy”, lecz narzędzie zarządzania strategicznego: pozwala zamawiającemu kształtować relacje z dostawcami w

modelu partnerskim — opartym na zaufaniu, odpowiedzialności i wspólnym rozumieniu tego, że bezpieczeństwo to wspólna praca po obu stronach umowy. W tak ustawionym nadzorze regularny dialog operacyjny, transparentne raportowanie i konsekwentne domykanie działań korygujących sprawiają, że ryzyko jest utrzymywane na poziomie świadomie zaakceptowanym, a nie pozostawione przypadkowi. Kolejne podrozdziały — o monitoringu ciągłym (continuous assurance), wskaźnikach ryzyka (KRI), typach audytów, obsłudze incydentów i „uczeniu się" organizacyjnym — pokazują, jak ten model przełożyć na praktykę dnia codziennego.

### 4.4.1. Ciągłość oceny ryzyka – monitoring dynamiczny

Współczesny łańcuch dostaw, zwłaszcza w środowisku ICT, jest jak żywy organizm – stale się zmienia, reaguje na bodźce, podlega ewolucji technologicznej i organizacyjnej. Dlatego tradycyjny model „raz wykonanej oceny ryzyka", sporządzonej na początku projektu, traci sens, gdy tylko pojawiają się pierwsze aktualizacje systemów, rotacja personelu czy zmiany w konfiguracji środowiska technicznego. W takich warunkach skuteczność zarządzania ryzykiem wymaga wprowadzenia ciągłego monitorowania, które działa niczym system czujników – stale odczytuje parametry bezpieczeństwa i alarmuje, gdy któreś z nich odbiega od normy. Ciągłość oceny ryzyka (continuous assurance) polega na systematycznym gromadzeniu, analizie i weryfikacji informacji o stanie bezpieczeństwa – nie poprzez jednorazowe audyty, ale w sposób ciągły i oparty na danych.

W ujęciu praktycznym continuous assurance to nie „więcej raportów", lecz stały obieg wiarygodnych danych o bezpieczeństwie, z którego wynikają szybkie i udokumentowane decyzje. Rdzeń tego podejścia tworzą trzy elementy: (1) regularny dopływ sygnałów (telemetria techniczna, wskaźniki organizacyjne, alerty zewnętrzne), (2) z góry zdefiniowane progi eskalacyjne, po których następują działania korygujące (CAP), oraz (3) weryfikacja efektów — sprawdzamy, czy ryzyko faktycznie spadło, a nie tylko „odfajkowaliśmy" zadania. Taki układ zmienia logikę z reaktywnej na predykcyjną: korygujemy kurs zanim zdarzenie się zmaterializuje**.**

Istotne jest łączenie strumieni danych w jeden obraz ryzyka. Dane techniczne od dostawcy (logi, alarmy, raporty SOC, statystyki dostępności, skany podatności)

należy zestawiać z wskaźnikami organizacyjnymi (zmiany w łańcuchu podwykonawców, status certyfikacji ISO/UE/krajowej) oraz sygnałami zewnętrznymi (alerty CERT/CSIRT, ENISA). W praktyce warto prowadzić jedną kartę oceny na dostawcę: w górnej części wskaźniki (KRI/KPI i trend 3–6-miesięczny), w środkowej — istotne zmiany organizacyjne i notyfikacje, w dolnej — otwarte działania korygujące z terminami i odpowiedzialnością. Dzięki temu na jednym ekranie widać zarówno co dzieje się teraz, jak i pamięć organizacyjną (co już zrobiliśmy, co jeszcze zalega).

Warto ściśle określić metryki i progi — co monitorować, kiedy reagować. Nie chodzi o dziesiątki wskaźników, lecz o krótki zestaw, który „prowadzi" decyzje**.** W kontraktach ICT zwykle sprawdza się następujące minimum operacyjne:

- MTTD/MTTR dla incydentów bezpieczeństwa i awarii — trend rosnący przez 2–3 miesiące to sygnał degradacji.
- Terminowość łatek zależna od ważności (np. CVSS) — przekroczenie SLA uruchamia CAP.
- Higiena integracji: odsetek wywołań API odrzuconych z powodu błędnej autoryzacji/schematu.
- Status certyfikacji: zmiana zakresu, zawieszenie, negatywne wnioski z audytu nadzorczego — próg do przeglądu ryzyka.
- Powtarzalność niezgodności: ten sam typ uchybienia drugi raz w kwartale = eskalacja poziomu nadzoru.
- Ekspozycja zewnętrzna: alert z CERT/ENISA lub wpis o poważnej luce – sprawdź listę komponentów (SBOM) i ustal szybki plan naprawy**.**

Progi powinny być opisane przed startem usługi (w aneksie bezpieczeństwa) i zmapowane na reakcje: „próg przekroczony → działanie X w Y godzin/dni". Dzięki temu eskalacja nie jest sporem interpretacyjnym, tylko wykonaniem wcześniej uzgodnionej procedury.

Rytm przeglądów i odpowiedzialności dobrze działa według zasady „krótko-średnio-długo":

- Co miesiąc**:** lekki przegląd operacyjny (metryki, incydenty, status CAP, drobne korekty).
- Co kwartał: przegląd ryzyka zgodny z ISO/IEC 27005 (trend KRI, zmiany w łańcuchu, wnioski z testów DR i audytów), aktualizacja klasy ryzyka w rejestrze.

- Co rok: audyt planowy (ISO/IEC 27001/19011 lub równoważny) z próbkami dowodów i testem wybranych kontrolek.

Monitoring musi także „widzieć" to, czego wymagają przepisy: gotowość do notyfikacji (UKSC), zgodność cyklu życia wyrobu (CRA: zarządzanie podatnościami, aktualizacje), ochronę danych (RODO: rozliczalność, rejestrowanie czynności). Dlatego w pakiecie danych przekazywanych co miesiąc warto utrzymywać: wyciąg z logów istotnych dla rozliczalności, status poprawek w kontekście SBOM i raport zgodności z wymogami certyfikacyjnymi (UE/krajowe), jeżeli dotyczą przedmiotu zamówienia.

Każdy „czerwony" sygnał powinien kończyć się krótką notatką decyzyjną: co robimy teraz (np. obejście, tymczasowe ograniczenie funkcji), co robimy docelowo (patch, zmiana konfiguracji, dodatkowa kontrola), kiedy i jak sprawdzimy efekt (retst, przegląd wskaźników). CAP bez weryfikacji bywa iluzją — dlatego po zamknięciu działania należy sprawdzić, czy metryka wróciła do normy i czy nie pojawił się efekt uboczny.

Przykład**:**

*W systemie obiegu dokumentów rośnie liczba nieudanych logowań, a dostawca spóźnia się z ważnymi aktualizacjami. To przekracza ustalone progi. W ciągu 24 godzin włączono dwuskładnikowe logowanie (MFA) dla wrażliwych ról i ustalono plan nadrobienia aktualizacji z terminem 14 dni. Zamawiający otworzył plan działań korygujących (CAP)**,** wpisał zdarzenie do rejestru ryzyk i poprosił o krótki retest po wdrożeniu zmian. Miesiąc później wskaźniki wróciły do normy; pozostawiono „znacznik", że powtórka w pół roku uruchomi audyt doraźny.*

Na start wystarczy wspólny szablon raportu miesięcznego (1–2 strony, stały zestaw metryk i zdarzeń), arkusz rejestru ryzyk z kolorową sygnalizacją progów oraz krótki protokół przeglądu kwartalnego (wnioski, decyzje, zadania). Z czasem można dołożyć integrację z SIEM, zautomatyzować zbieranie KRI czy wdrożyć panel w narzędziu GRC — jednak fundamentem pozostaje dyscyplina danych i decyzji.

W ten sposób continuous assurance przestaje być hasłem i staje się codziennym rytuałem zarządzania kontraktem: dane → próg → decyzja → działanie →

weryfikacja → aktualizacja ryzyka. Dzięki temu zamawiający utrzymuje kontrolę nad profilem ryzyka nie „od audytu do audytu", ale każdego dnia.

### 4.4.2. Wskaźniki ryzyka dostawcy (KRI) i mechanizmy reagowania na zmiany profilu ryzyka

Skuteczny nadzór nad dostawcami zaczyna się od policzalnego obrazu ryzyka. Bez liczb nie ma ani porównywalności ofert, ani sensownej kontroli w trakcie umowy — są tylko deklaracje. Dlatego w centrum systemu monitorowania stoją wskaźniki ryzyka (KRI): proste, mierzalne sygnały, które pokazują, czy bezpieczeństwo utrzymuje się w granicach uzgodnionej tolerancji, oraz dają wczesne ostrzeżenie, że trend skręca w złą stronę. KRI spajają to, co ustalono ex ante (poziom ryzyka akceptowalnego) z tym, co dzieje się ex post (rzeczywista jakość usług i reakcji), a w modelu continuous assurance stają się elementem codziennego rytmu: dane → próg → decyzja.

Warunkiem ich użyteczności jest dobór „pod kontrakt". Inne KRI będą potrzebne, gdy zamawiamy usługę zarządzaną SOC, inne – gdy kupujemy wyrób z elementem cyfrowym objęty CRA, a jeszcze inne – gdy kluczowa jest dostępność usług dla obywateli. Wskaźniki muszą więc odzwierciedlać kontekst operacyjny, potencjalny wpływ na bezpieczeństwo publiczne oraz rolę danej usługi lub produktu w infrastrukturze krytycznej. Dobrze zaprojektowany zestaw nie jest długi ani przypadkowy: obejmuje tylko te miary, które realnie prowadzą do działania (np. uruchamiają plan naprawczy, przegląd ryzyka czy audyt doraźny), dzięki czemu KRI są nie dodatkiem do raportu, lecz mechanizmem sterującym nadzorem nad dostawcą.

Budowa systemu KRI opiera się na trzech zasadach:

1. Proporcjonalność **-** wskaźniki muszą „ważyć" tyle, ile ryzyko — ani mniej, ani więcej. Przy usługach krytycznych (np. systemy obywatelskie on-line) potrzebne są KRI o krótkich horyzontach i ostrych progach (np. terminy łatek według CVSS, MTTD/MTTR), natomiast przy dostawach niskiego wpływu wystarczy lżejszy zestaw i rzadszy przegląd. Zasada jest jedna: poziom pomiaru i częstość oceny rosną wraz z ekspozycją i złożonością łańcucha dostaw.
2. Obiektywność **-** każdy KRI musi opierać się na danych, które da się policzyć i zweryfikować — w logach, raportach, certyfikatach, wynikach testów czy SBOM. Unikamy wskaźników „miękkich" bez dowodów. Dla każdego KRI

powinno być jasne: skąd bierzemy dane, kto je dostarcza, jak je weryfikujemy i w jakim formacie są raportowane (tak, by dwie kolejne iteracje były porównywalne).

3. Aktualność **-** KRI mają wartość tylko wtedy, gdy są świeże i analizowane w rytmie ciągłym, zgodnym z continuous assurance. Oznacza to z góry ustalony cykl: bieżące alerty dla przekroczeń progów, miesięczne przeglądy trendów i kwartalne decyzje o zmianie poziomu nadzoru. Dzięki temu reagujemy zanim ryzyko się zmaterializuje, a nie „po fakcie".

Wśród typowych wskaźników ryzyka w relacjach z dostawcami wymienia się m.in.:

- poziom zgodności z wymaganiami normatywnymi i certyfikacyjnymi - nie wystarcza sama informacja, że „certyfikat jest"; liczy się jego zakres i aktualność oraz wyniki audytów nadzorczych. Zamawiający weryfikuje, czy obszary objęte certyfikacją (np. ISO/IEC 27001) rzeczywiście pokrywają procesy i systemy wykorzystywane do świadczenia usługi, a jeśli w grę wchodzą programy unijne lub krajowe (EUCS/EUCC/krajowe schematy), czy wykonawca utrzymuje status bez zastrzeżeń. Stabilny status certyfikacji to zwykle pośredni dowód dojrzałości procesów.
- częstotliwość i charakter niezgodności w raportach bezpieczeństwa - zwracamy uwagę nie tylko na liczbę uchybień, ale też ich wagę, czas zamykania oraz powtarzalność tych samych problemów. Dane czerpiemy z cyklicznych raportów i rejestru CAP. Jeśli drobne niezgodności szybko znikają — proces działa; jeśli te same uchybienia wracają co kwartał, mamy do czynienia z luką systemową, która wymaga innej interwencji niż pojedyncza poprawka.
- czas reakcji na incydenty - analizujemy nie tyle wynik pojedynczego zdarzenia, ile trend z kilku okresów: wydłużanie się MTTD/MTTR bywa pierwszym sygnałem, że zespół traci sprawność albo obciążenie rośnie szybciej niż zasoby. Źródłem danych są rejestr incydentów i raporty z przeglądów po incydentach. To wskaźnik, który bezpośrednio łączymy z progami eskalacyjnymi i działaniami korygującymi.
- liczbę komponentów wymagających aktualizacji bezpieczeństwa - patrzymy na liczbę komponentów oczekujących na łatkę oraz terminowość łatania względem ustalonych progów ważności (np. według CVSS), a także na skalę wyjątków od polityki (tzw. waivery) i czas ich utrzymywania. Dane wynikają z SBOM, raportów z łat oraz skanów podatności. Rosnące zaległości to

rosnące prawdopodobieństwo incydentu, dlatego ten KRI zwykle ma skojarzone krótkie terminy reakcji.

- częstotliwość przeglądów wewnętrznych po stronie wykonawcy - jak często recertyfikowane są uprawnienia, jak systematycznie weryfikowane są konfiguracje i czy wykryte błędy są domykane w terminie. Tu liczy się regularność i dowodowość — protokoły przeglądów, listy uprawnień przed i po zmianach, potwierdzenia wdrożenia poprawek.

Kluczowe w systemie KRI jest to, by nie kończył się na pomiarze, lecz naturalnie przechodził w decyzję. Wskaźnik ma wartość dopiero wtedy, gdy jest powiązany z progiem i z góry ustaloną reakcją: jeśli trend lub wartość przekracza uzgodnioną granicę, uruchamia się konkretne działanie — od krótkiego planu naprawczego (CAP) i przeglądu ryzyka, po czasowe ograniczenie funkcji czy, w skrajnych sytuacjach, rewizję zapisów umowy. Taki mechanizm powinien być opisany w dokumentacji kontraktowej (aneks bezpieczeństwa) w sposób jednoznaczny: który KRI obserwujemy, jaka wartość oznacza „żółte" i „czerwone" światło, kto podejmuje decyzję, w jakim czasie i jak ją dokumentuje (np. wpis w rejestrze ryzyk).

Dobrze działa tu prosta drabina eskalacji: najpierw krótkie działanie korygujące z terminem i właścicielem, następnie — jeśli wskaźnik nie wraca do normy — przegląd ryzyka i zwiększenie nadzoru (częstsze raporty, audyt doraźny), a w razie dalszej nieskuteczności — decyzje kontraktowe. Ważne, by każdą reakcję domykała weryfikacja efektu (czy KRI realnie się poprawił) oraz krótka notatka w rejestrze, tak aby decyzje były powtarzalne i obronne dowodowo. W tym ujęciu KRI przestają być narzędziem kontroli „dla kontroli", a stają się instrumentem zarządzania — pomagają utrzymać bezpieczeństwo na poziomie świadomie zaakceptowanym i dostosowywać je do zmieniającego się otoczenia zagrożeń.

### 4.4.3. Audyty bezpieczeństwa dostawców

Audyty bezpieczeństwa są jednym z głównych punktów oparcia dla nadzoru nad dostawcami: wnoszą niezależne spojrzenie na to, czy deklarowane praktyki i postanowienia umowne rzeczywiście działają w codziennej eksploatacji. Ich sens nie kończy się na „odhaczaniu" zgodności — audyt ma sprawdzić skuteczność zastosowanych środków kontrolnych oraz wykryć luki i słabe miejsca, które mogą eskalować do realnych zdarzeń w łańcuchu dostaw. Ważny jest tu także wymiar dojrzałości: audyt ocenia nie tylko, czy kontrola istnieje, ale czy jest utrzymywana, mierzona i doskonalona w czasie.

W praktyce audyt konfrontuje trzy warstwy: normy i przepisy (wymagania UKSC, RODO, CRA oraz odpowiednie normy ISO), postanowienia kontraktowe (aneks bezpieczeństwa, KRI, progi eskalacyjne, CAP) oraz działanie systemu „na żywo" (procedury, konfiguracje, logi, ślady incydentów). Dochodzi do tego aspekt sprawdzania spójności dowodów: to, co zapisano w polityce, musi zgadzać się z konfiguracją i potwierdzać w rejestrach operacyjnych. Dzięki temu audyt odpowiada na dwa kluczowe pytania: czy robimy to, co obiecaliśmy (zgodność), i czy to, co robimy, rzeczywiście obniża ryzyko (skuteczność). Wyniki nie pozostają na papierze — wracają do rejestru ryzyk, aktualizują KRI, zasilają continuous assurance i – gdy trzeba – uruchamiają działania korygujące, wzmacniając odporność całego łańcucha dostaw.

W podejściu zalecanym przez ISO/IEC 19011 oraz praktykę systemów zarządzania jakością i bezpieczeństwem informacji audyt nie powinien ograniczać się do jednego wymiaru. Chodzi o trzy komplementarne perspektywy, które razem dają rzetelny obraz:

- ocenę zgodności (compliance) – to sprawdzenie, czy wymagania formalne i kontraktowe są spełnione — od przepisów (np. UKSC, RODO, CRA), przez normy i standardy (ISO/IEC), po zapisy umowy (aneks bezpieczeństwa, KRI, progi eskalacji). Audytor weryfikuje dokumenty, uprawnienia, konfiguracje i dowody operacyjne. Wynik mówi wprost: czy robimy to, do czego się zobowiązaliśmy,
- ocenę skuteczności (effectiveness) – sama obecność kontrolki nie oznacza jeszcze, że działa. Tu badamy, czy zastosowane środki rzeczywiście osiągają zakładany cel — czy wykrywają incydenty w założonym czasie, czy ograniczają liczbę niezgodności, czy obniżają ryzyko resztkowe. Audyt porównuje deklaracje z rezultatami (np. metrykami MTTD/MTTR, terminowością łatek, spadkiem powtarzalnych usterek), aby odpowiedzieć, na ile kontrola jest użyteczna, a nie tylko „obecna",
- ocenę dojrzałości (maturity) – To spojrzenie, czy organizacja potrafi utrzymywać i rozwijać swój system bezpieczeństwa w czasie: czy przegląda uprawnienia, reaguje na wnioski z audytów i incydentów, aktualizuje polityki wraz ze zmianami technologicznymi i prawnymi, a zmiany są udokumentowane i konsekwentnie wdrażane. Innymi słowy — czy to, co dziś działa, będzie działało jutro, bo stoi za tym proces, a nie jednorazowy wysiłek.

W relacji zamawiający–wykonawca audyty powinny być planowane z wyprzedzeniem i proporcjonalnie do ryzyka: częstsze tam, gdzie usługa jest krytyczna lub łańcuch poddostawców rozbudowany, rzadsze przy niskim wpływie. Ich forma i zakres nie mogą być jednorodne — obok audytów planowych (rocznych/półrocznych) trzeba przewidzieć audyt incydentalny uruchamiany po sygnale z KRI lub alertach zewnętrznych, a także dobrać tryb pracy: audyt zdalny, gdy weryfikujemy dokumenty, logi i konfiguracje, oraz terenowy (on-site), gdy konieczne jest obejrzenie środowiska, pobranie próbek dowodów czy rozmowy z personelem operacyjnym. Każdy audyt powinien mieć jasno określone cele, listę dowodów, kryteria oceny i harmonogram, a wyniki — spójny format, który da się porównać w czasie.

Na samym raporcie sprawa się nie kończy. Wyniki trzeba czytać „w trendzie": czy liczba i waga niezgodności maleje, czy skraca się czas ich zamykania, czy nie powracają te same uchybienia. Dopiero taka analiza pozwala odróżnić jednorazowe potknięcie od luki systemowej, która wymaga innego podejścia (zmiany procesu, doposażenia zespołu, korekty wymagań umownych). Wnioski z audytów powinny wracać do rejestru ryzyk, aktualizować KRI i uruchamiać CAP z terminami i odpowiedzialnością — w przeciwnym razie audyt staje się ćwiczeniem formalnym.

Kluczowa jest też komunikacja. W modelu partnerskim audyt to nie polowanie na błędy, lecz wspólne spojrzenie na skuteczność środków bezpieczeństwa. Dlatego dobrą praktyką jest, by każdy audyt kończył się nie tylko raportem, ale także krótkim warsztatem poaudytowym: strony przeglądają najważniejsze ustalenia, uzgadniają priorytety działań korygujących, przypisują właścicieli zadań i terminy, a następnie ustalają sposób weryfikacji efektów. Taki rytuał zamyka pętlę: od dowodów, przez decyzje, po realne obniżenie ryzyka.

### 4.4.4. Monitorowanie incydentów i niezgodności w relacji kontraktowej

System monitorowania incydentów i niezgodności to praktyczny kręgosłup zarządzania ryzykiem w łańcuchu dostaw: od jego jakości zależy, czy organizacja utrzyma ciągłość działania w momentach zakłóceń oraz czy potrafi przekuć doświadczenia kryzysowe w trwałe usprawnienia procedur. Aby działał skutecznie, musi opierać się na klarownych definicjach. W tym ujęciu „incydent" to nie wyłącznie zmaterializowane naruszenie bezpieczeństwa, lecz także istotne odchylenie od przyjętych norm i parametrów, które może do takiego naruszenia doprowadzić (np. powtarzalne błędy uwierzytelniania, opóźnienia w krytycznych

poprawkach, nieautoryzowana zmiana konfiguracji). Takie, prewencyjne rozumienie pojęć pozwala wyłapywać problemy wcześnie, zanim staną się krytyczne, i uruchamiać działania korygujące z odpowiednim wyprzedzeniem.

System powinien być jednocześnie sformalizowany i czasowo zdyscyplinowany. Zgodnie z NIS2 i UKSC raportowanie incydentów wymaga zdefiniowanych kanałów, terminów i poziomów eskalacji — od zgłoszenia wstępnego, przez raport uzupełniający, aż po raport końcowy — a dokumentacja musi wskazywać kto, co, kiedy i jak przekazuje (zakres danych, format, odpowiedzialności). Te zasady trzeba odzwierciedlić w umowie: wykonawca ma obowiązek niezwłocznego zgłaszania zdarzeń mogących wpływać na świadczenie usług publicznych lub bezpieczeństwo danych, przekazywania niezbędnych artefaktów (logi, konfiguracje, oś czasu zdarzeń) oraz współpracy przy analizie przyczyn i działaniach korygujących.

W kwestii dostępności kontaktu operacyjnego należy przyjąć podejście oparte na krytyczności: dla usług i systemów kluczowych wymagany jest punkt kontaktowy z gotowością 24/7 i jasno zdefiniowanymi czasami reakcji; dla usług o umiarkowanym wpływie wystarczają rozszerzone godziny pracy z mechanizmem eskalacji na dyżur krytyczny; dla obszarów niskiego ryzyka — standardowe godziny z umówionym trybem zgłoszeń. Takie stopniowanie łączy wymóg czujności z proporcjonalnością obciążeń po stronie wykonawcy i zamawiającego.

Aby mechanizm był spójny w całym łańcuchu, warto doprecyzować matrycę ról i eskalacji (kto odbiera zgłoszenie, kto prowadzi ocenę wpływu, kto decyduje o komunikacji zewnętrznej), format zgłoszeń (krótkie, ujednolicone „karty incydentu” na start) oraz minimalny zestaw danych do wczesnej oceny (opis symptomów, zasięg, komponenty dotknięte, wpływ na użytkowników, pierwsze działania ograniczające). Dzięki temu monitoring incydentów i niezgodności jest działającym mechanizmem: wcześnie wychwytuje odchylenia, uruchamia właściwą ścieżkę reakcji i zasila pętlę uczenia się organizacji, a jednocześnie pozostaje proporcjonalny do ryzyka i możliwy do utrzymania w codziennej praktyce.

Kluczowym elementem tego procesu jest tzw. cykl reagowania i uczenia się, który obejmuje etapy:

1. Identyfikacja i wstępna kwalifikacja zdarzenia - rejestracja sygnału, weryfikacja, czy to incydent/naruszenie/niezgodność, wstępna klasyfikacja ważności.

2. Ocena wpływu i decyzja o eskalacji - szybka ocena zasięgu (dane, systemy, użytkownicy), decyzja o poziomie eskalacji, wyznaczenie ról.
3. Powiadomienia i komunikacja regulacyjno - kontraktowa - notyfikacje wymagane UKSC/NIS2/RODO (jeśli dotyczy), poinformowanie zamawiającego/podwykonawców zgodnie z umową; ustalenie częstotliwości aktualizacji statusu.
4. Działania natychmiastowe - ograniczenie skutków, odseparowanie komponentów, blokady dostępu, obejścia - tak, by zahamować rozprzestrzenianie się incydentu.
5. Usunięcie przyczyny i przywrócenie działania - łatki/zmiany konfiguracji, czyszczenie artefaktów ataku, kontrolowany powrót usług (z testami akceptacyjnymi),
6. Działania korygujące z odpowiedzialnością i terminami - formalny plan naprawczy obejmujący także elementy procesowe (np. zmiana procedury dostępu, recertyfikacja ról),
7. Analiza przyczyn źródłowych i czynniki sprzyjające - nie tylko „co zawiodło", ale „dlaczego mogło zawieść": brak zasobów, luki w procesie, szkolenia, nadzór nad podwykonawcami.
8. Środki zapobiegawcze i utrwalające - modyfikacje architektury/kontrolek, aktualizacja polityk, doprecyzowanie progów KRI, wzmocnienie wymogów wobec podwykonawców (down-flow).
9. Weryfikacja efektów i uczenie się organizacyjne - retest/ponowny pomiar KRI, aktualizacja rejestru ryzyk, przegląd lessons learned, ewentualnie korekta zapisów umownych/OPZ; zamknięcie incydentu dopiero po potwierdzonej poprawie.

Takie podejście pozwala nie tylko usuwać skutki, ale także modyfikować system zarządzania ryzykiem w sposób ewolucyjny – każdy incydent staje się impulsem do doskonalenia procesów.

### 4.4.5. Uczenie się organizacyjne – wykorzystanie wyników monitoringu w procesie doskonalenia SZBI i polityki zakupowej

Największą wartością monitoringu nie jest sam raport, lecz wiedza przekuta w decyzje i zmiany, które realnie obniżają ryzyko. Dane o incydentach, niezgodnościach i trendach nabierają znaczenia dopiero wtedy, gdy pomagają odpowiedzieć na proste pytania: co poprawiamy teraz, co zmieniamy w procesie na stałe, a co włączamy do kolejnych postępowań. Każde zdarzenie — od drobnego odstępstwa po poważny incydent — dostarcza materiału do usprawnień zarówno w warstwie technicznej (konfiguracje, aktualizacje, integracje), jak i organizacyjnej (role i odpowiedzialności, przepływ informacji z wykonawcą i jego podwykonawcami, rytm przeglądów).

W tym ujęciu monitorowanie i audytowanie dostawców stają się mechanizmem uczenia się całej instytucji: wnioski z raportów i przeglądów trafiają do polityk i procedur bezpieczeństwa informacji, do matryc wymagań oraz do dokumentacji zakupowej (OPZ, klauzule bezpieczeństwa, kryteria oceny). Dzięki temu kolejne umowy opierają się na doświadczeniu, a nie na założeniach sprzed miesięcy. Praktycznie oznacza to trzy równoległe strumienie: po pierwsze, szybkie działania korygujące po zdarzeniach (z właścicielem i terminem); po drugie, trwałe zmiany procesowe wynikające z analizy przyczyn źródłowych (np. doprecyzowanie progów KRI, dopasowanie harmonogramu łatek, doprecyzowanie odpowiedzialności w łańcuchu poddostawców); po trzecie, aktualizacje wzorców postępowania o udzielenie zamówienia publicznego — tak, by wymagania i kryteria w nowych postępowaniach odzwierciedlały to, czego organizacja nauczyła się w toku realizowanych kontraktów.

Taki sposób pracy tworzy pętlę doskonalenia: obserwacja → wniosek → decyzja → zmiana → weryfikacja efektu. Jeśli pętla ma właścicieli (po stronie bezpieczeństwa, zakupów i biznesu) oraz stały rytm przeglądu wniosków, instytucja zyskuje przewagę: szybciej reaguje na ryzyka, lepiej dobiera środki ochrony i świadomiej projektuje kolejne zamówienia. Zamiast gromadzić raporty, organizacja buduje pamięć operacyjną i przenosi ją w przyszłość — do umów, procedur i praktyk współpracy z dostawcami. Dzięki temu bezpieczeństwo przestaje być wyłącznie kosztem czy obowiązkiem, a staje się elementem jakości zarządzania i reputacji.

Uczenie się organizacyjne oznacza, że instytucja potrafi przekuć doświadczenia z realizacji umów — w tym wnioski z incydentów, niezgodności oraz sprawdzonych praktyk — w jasne reguły postępowania, które następnie są konsekwentnie stosowane. W praktyce działa to na trzech, wzajemnie uzupełniających się poziomach:

1. Poziom operacyjny **-** to szybkie reagowanie na bieżące problemy i wdrażanie korekt po incydentach czy niezgodnościach. Chodzi o to, by wnioski z konkretnego zdarzenia (np. opóźniona łatka, błędna konfiguracja, luka w komunikacji) natychmiast przekładały się na zadania z właścicielem i terminem oraz na weryfikację efektu w kolejnych raportach. Na tym poziomie liczy się dyscyplina zamykania działań korygujących i to, czy wskaźniki (KRI) faktycznie wracają do normy.
2. Poziom systemowy **-** to już nie pojedyncze poprawki, lecz trwałe zmiany w procesach i standardach**.** Tu organizacja aktualizuje procedury (np. rytm

przeglądów dostępów, progi dla terminowości łatek, wymagany zakres raportów od dostawcy), doprecyzowuje odpowiedzialności w łańcuchu podwykonawców i ujednolica format dowodów. W praktyce oznacza to modyfikację polityk i instrukcji bezpieczeństwa informacji, szablonów planów reagowania oraz matryc wymagań w dokumentacji zakupowej — tak, aby kolejny kontrakt był lepiej „ustawiony" już na starcie.

3. Poziom strategiczny **-** to modyfikacja polityki bezpieczeństwa, modelu kontraktowania i podejścia do ryzyka**.** Na tym poziomie zapadają decyzje o zmianie tolerancji ryzyka dla kluczowych usług, o wprowadzeniu lub podniesieniu wymogów certyfikacyjnych (np. ISO/IEC 27001, programy unijne/krajowe), o przesunięciu ciężaru na dłuższe utrzymanie czy większy nacisk na zgodność z CRA. Tu także odświeża się kryteria oceny ofert, doprecyzowuje klauzule bezpieczeństwa i ustala „standardy minimum" dla całej organizacji, tak aby doświadczenia z jednego projektu przechodziły do praktyki ogólnej**.**

Dojrzałe organizacje spinają te trzy poziomy w jeden proces ciągłego doskonalenia: wyniki monitoringu i audytów nie trafiają do archiwum, lecz do rejestru wniosków, który ma właścicieli, rytm przeglądów i ścieżkę wdrażania zmian. Każda informacja zwrotna z realizacji — wzrost drobnych niezgodności, opóźnienia w aktualizacjach, powracające trudności w komunikacji między zespołami — staje się impulsem do modyfikacji odpowiednich procedur, wymagań lub zapisów umownych, a następnie jest weryfikowana przez pomiar efektu (czy KRI się poprawiły, czy spadła liczba niezgodności, czy skrócił się czas reakcji). Tym właśnie różni się organizacja ucząca się od biurokratycznej: pierwsza nie tylko zbiera dane, ale nadaje im znaczenie i wdraża wnioski, budując pamięć operacyjną, która realnie obniża ryzyko w kolejnych umowach.

Warto podkreślić, że uczenie się organizacyjne jest pracą zespołową. Nie może pozostawać domeną pojedynczego audytora czy inspektora bezpieczeństwa, bo wtedy kończy się na sprawozdaniu. Włączeni muszą być: kierownictwo (które nadaje priorytety i akceptuje ryzyko), dział zamówień (który przenosi wnioski do OPZ, kryteriów i klauzul), IT/operacje (wdrażające techniczne zmiany i mierzące ich efekt), compliance/dział prawny (dbające o spójność z regulacjami i kontraktami) oraz użytkownicy końcowi (sygnalizujący problemy, które często nie widać w dashboardach). Dopiero taka szeroka współpraca sprawia, że monitoring i audyty wchodzą do codziennego obiegu decyzji, a nie funkcjonują jako doraźny wymóg formalny.

W dłuższej perspektywie organizacja, która potrafi przekuwać wyniki monitoringu w zmiany, przedefiniowuje bezpieczeństwo: z pozycji kosztu lub obowiązku na element jakości zarządzania i reputacji. Oznacza to bardziej przewidywalne projekty, mniej „gaszenia pożarów" i lepszą pozycję negocjacyjną wobec dostawców. Kluczowe jest domykanie pętli: doświadczenia z bieżących kontraktów powinny wracać do planowania kolejnych postępowań - poprzez aktualizację kryteriów oceny ofert, doprecyzowanie standardów klauzul bezpieczeństwa, ujednolicenie wymaganych dowodów (np. zakres raportów, rytm przeglądów, progi KRI) oraz wskazanie warunków minimalnych (np. certyfikacja, zasady dla podwykonawców). Dzięki temu każdy następny kontrakt startuje z wyższego poziomu dojrzałości i jest mniej podatny na ryzyko już na starcie.

# 5. Praktyki i standardy branżowe

## 5.1. Znaczenie standaryzacji w bezpieczeństwie łańcucha dostaw

Standaryzacja w bezpieczeństwie łańcucha dostaw to dziś warunek sterowalności ryzyka, a nie tylko dodatkowy element dokumentacji. Gwałtowna cyfryzacja usług publicznych, gęsta sieć integracji między systemami oraz rosnąca presja regulacyjna (UKSC, CRA, DORA, RODO) powodują, że bez wspólnego języka wymagań i dowodów trudno rzetelnie porównać oferty, egzekwować umowy i prowadzić nadzór w czasie ich trwania. Standardy (ISO, wytyczne ENISA/NIST, programy certyfikacji UE/krajowe) dostarczają właśnie takiego języka: precyzują, co trzeba zabezpieczyć, jak to mierzyć i jakimi dowodami potwierdzić zgodność.

Z perspektywy zamówień publicznych standardy rozwiązują trzy praktyczne problemy. Po pierwsze – porównywalność: gdy wymagania i kontrolki są zdefiniowane w oparciu o uznane normy, różne oferty można ocenić tymi samymi kryteriami, a spory interpretacyjne ograniczyć do minimum. Po drugie – rozliczalność: standard określa nie tylko oczekiwany stan, lecz także rodzaj i format dowodów (raporty, certyfikaty, wyniki audytów), dzięki czemu łatwiej przełożyć zapisy OPZ na konkretne wskaźniki, progi i działania korygujące. Po trzecie – ciągłość: standaryzacja „przyspawa" etap wyboru wykonawcy do etapu nadzoru (continuous assurance) — te same wymogi, na które wykonawca odpowiada w ofercie, później stają się osią KRI, audytów i przeglądów.

Ujednolicone wymagania zmniejszają także ryzyko systemowe: ułatwiają zarządzanie poddostawcami (down-flow wymagań), ograniczają ryzyko

uzależnienia od jednego dostawcy (przenaszalne kontrolki i dowody), a w przypadku produktów cyfrowych z elementem oprogramowania – umożliwiają spójne egzekwowanie zasad security by design/default i cyklu życia poprawek (CRA). Co ważne, standaryzacja działa ponad granicami: gdy zamawiający stosuje uznane normy, łatwiej prowadzić postępowania z udziałem wykonawców z różnych jurysdykcji i utrzymać zgodność z prawem unijnym oraz krajowym.

Krótko mówiąc, standardy są narzędziem zarządczym: porządkują wymagania, zwiększają przejrzystość oceny, upraszczają nadzór i – co kluczowe – pozwalają mierzyć skuteczność środków bezpieczeństwa w całym cyklu życia umowy. Dzięki temu bezpieczeństwo w łańcuchu dostaw staje się nie tyle deklaracją w SWZ, ile praktyką, którą da się konsekwentnie planować, weryfikować i doskonalić.

### 5.1.1. Standardy jako narzędzie zgodności i ujednolicenia praktyk w zamówieniach publicznych

W zamówieniach publicznych dotyczących usług i produktów ICT standardy pełnią rolę wspólnego języka: definiują, *co* należy zabezpieczyć, *jak* mierzyć skuteczność, *czym* potwierdzać zgodność i *kiedy* reagować. Dzięki temu zamawiający może przełożyć ogólne wymagania prawne (NIS2, UKSC, RODO, CRA, DORA) na konkretne oczekiwania operacyjne i dowody, które da się zweryfikować przed wyborem wykonawcy oraz monitorować w trakcie realizacji umowy. Bez tego „języka" porównywanie ofert i egzekwowanie zapisów kontraktu staje się uznaniowe, a nadzór – rozproszony.

Logika jest prosta i przyczynowo-skutkowa: standard → mierzalny wymóg → dowód → próg → reakcja. Dzięki temu łączą się etapy ex ante (warunki udziału, kryteria oceny) i ex post (KRI, audyty planowe/incydentalne, działania korygujące), co buduje spójny łańcuch odpowiedzialności.

Standardy (np. ISO/IEC 27001, 27002, 27005, 27036, 28000) porządkują praktykę tak, by była spójna z wymaganiami prawnymi, nie mnożąc odrębnych, lokalnych procedur. W praktyce oznacza to:

- NIS2 i UKSC: standardy przekładają obowiązek „zarządzania ryzykiem i łańcuchem dostaw" na zestaw kontrolek, ról i procesów (np. rejestr ryzyk dostawców, okresowe przeglądy dostępów, zarządzanie podatnościami według poziomów ważności).

- RODO: katalog kontrolek z ISO/IEC 27001 pomaga spełniać zasadę rozliczalności i „privacy by design” (np. pseudonimizacja, rejestrowanie czynności przetwarzania, testy skutków dla ochrony danych).
- CRA: normy i programy certyfikacyjne ułatwiają egzekwowanie „security by design/default” i cyklu życia poprawek (mapowanie wymagań w OPZ, dowody w postaci SBOM, terminowość łatek).
- DORA (dla podmiotów finansowych): spójny nadzór nad usługami ICT zewnętrznymi (dostawcy krytyczni, testy odporności, raportowanie incydentów) łatwiej wprowadzić, gdy wymogi opiera się na normach.

Kiedy SWZ/OPZ odwołuje się do uznanych norm, cały proces zaczyna „mówić tym samym językiem”: oferenci odpowiadają na jednolite, znormalizowane wymagania, a zamawiający nie musi już porównywać rozwiązań opisanych różnymi miarami. Znika problem „porównywania nieporównywalnego”, bo każdy opis produktu czy usługi mieści się w tej samej siatce kontrolek i dowodów. Dzięki temu ocena staje się porównywalna i weryfikowalna, a decyzje — mniej uznaniowe i łatwiejsze do uzasadnienia.

Na etapie zarządzania ryzykiem porządek zapewniają normy z rodziny ISO: 27036 wskazuje, jak identyfikować, klasyfikować i weryfikować dostawców; ISO/IEC 27005 porządkuje analizę ryzyka; ISO/IEC 27001 i 27002 definiują, jak zaprojektować i utrzymywać kontrolki; ISO/IEC 28000 dodaje ujęcie logistyczne i operacyjne. W praktyce oznacza to, że zasady — takie jak segmentacja dostępu, nadzór nad podwykonawcami czy testy akceptacyjne bezpieczeństwa — obowiązują równolegle po obu stronach kontraktu, u wykonawcy i u zamawiającego, co ogranicza miejsca potencjalnych nieścisłości na styku organizacji i zmniejsza pole do nieporozumień.

Standaryzacja porządkuje też kierunek przepływu wymagań i informacji. To, co wpisano do kontraktu głównego, powinno konsekwentnie być odzwierciedlone w umowach z podwykonawcami (down-flow), tak aby nie powstawały luki w łańcuchu. Jednocześnie sygnały o niezgodnościach, incydentach i zmianach istotnych dla ryzyka muszą wracać do zamawiającego (up-flow) w uzgodnionym formacie i terminie. Taki dwukierunkowy porządek — te same wymagania w dół, te same dane i dowody w górę — domyka pętlę: od specyfikacji przez realizację po nadzór, utrzymując cały łańcuch dostaw w jednym, spójnym modelu.

Na etapie przygotowania postępowania należy najpierw przełożyć wymagania prawne (NIS2, UKSC, RODO, CRA, DORA) na wymagania operacyjne, posługując się uznanymi standardami. Efektem tej pracy powinna być matryca wymagań, która jasno wskazuje warunki udziału (np. posiadanie i utrzymywanie ISO/IEC 27001 w zakresie obejmującym przedmiot zamówienia, doświadczenie w zarządzaniu łańcuchem dostaw zgodnie z ISO/IEC 27036), wymagania obligatoryjne do wpisania w OPZ (m.in. zarządzanie podatnościami z podziałem na poziomy ważności, utrzymywanie SBOM, prowadzenie rejestru ryzyk dostawców, raportowanie incydentów w rytmie zgodnym z UKSC) oraz katalog dowodów, które wykonawca ma dostarczać (certyfikaty z zakresem, raporty z audytów, przykładowe artefakty: procedury, zrzuty konfiguracji, logi, zapisy przeglądów). Praktyczny model wpięcia standardów w cykl zamówienia:

1. Faza (ex ante) należy wymagać dowodów równoważnych zgodnie z Pzp: jeżeli wykonawca nie posiada ISO/IEC 27001, powinien wykazać równoważny mechanizm o porównywalnym zakresie, poziomie pewności i nadzorze (np. program certyfikacyjny UE/krajowy lub audyt niezależny prowadzony zgodnie z ISO/IEC 19011). Zestaw oceny powinien obejmować nie tylko sam fakt certyfikacji, lecz także jej zakres, wyniki audytów nadzorczych, brak niezgodności głównych oraz mapę kontrolek do wymagań OPZ, aby porównanie ofert było rzetelne i obronne.
2. Faza (ex post) należy utrzymywać stały rytm dowodów: krótkie raporty miesięczne (KRI/KPI, zarejestrowane incydenty, status działań korygujących), przeglądy kwartalne ukierunkowane na trend ryzyka zgodnie z ISO/IEC 27005 oraz coroczny audyt według ISO/IEC 19011, który sprawdza zgodność, skuteczność i dojrzałość rozwiązań. Progi reakcji (np. „żółty” i „czerwony”) oraz ścieżki CAP należy z góry opisać w aneksie bezpieczeństwa, tak aby przekroczenie progu automatycznie uruchamiało uzgodnione działania.
3. Faza domknięcia pętli uczenia się: wnioski z nadzoru ex post powinny wracać do wzorów dokumentacji (OPZ, kryteria, klauzule) i do katalogu wymagań na przyszłe postępowania. Dzięki temu organizacja na bieżąco aktualizuje wymagania i dowody w świetle zebranych doświadczeń, a kolejne postępowania o udzielenie zamówienia publicznego startują z wyższego poziomu dojrzałości — praktyka rozwija się wraz z doświadczeniem, zamiast pozostawać niezmienna mimo zmieniającego się otoczenia ryzyka.

W standardach chodzi o to, by transparentność, odpowiedzialność i rozliczalność nie były deklaracją, lecz codzienną praktyką. Standaryzacja porządkuje zasady gry: z góry ustala, kto dostarcza jakie dane**,** w jakim formacie i w jakim rytmie. Po stronie zamawiającego przekłada się to na klarowny podział ról (właściciel kontraktu, właściciel ryzyka, punkt kontaktowy ds. incydentów, osoba odpowiedzialna za CAP) i na zdefiniowane ścieżki eskalacji; po stronie wykonawcy — na przewidywalny nadzór i jednoznaczne oczekiwania, bez domysłów i dowolnych interpretacji.

Kluczowe jest również oparcie oceny i nadzoru na dowodach, a nie na deklaracjach. W praktyce oznacza to wymaganie kompletnego, weryfikowalnego zestawu artefaktów: certyfikatu z precyzyjnym zakresem**,** wyników audytów i wniosków nadzorczych, zapisów rejestru incydentów i ich obsługi, potwierdzeń przeglądów dostępów**,** raportów z łatek i skanów podatności (z datami i poziomami ważności) oraz — w przypadku wyrobów z oprogramowaniem — SBOM z historią aktualizacji. Taki fundament sprawia, że decyzje (np. o eskalacji, działaniach korygujących czy audycie doraźnym) są obronne i oparte na danych, odpowiedzialność jest przypisana, a rozliczalność - możliwa do wykazania. Dzięki temu transparentność jest mierzalnym efektem dobrze zaprojektowanych wymagań.

Standaryzacja przynosi wymierne efekty w codziennej praktyce: usprawnia procesy, bo jednolite wymagania i formaty dowodów skracają czas oceny ofert i zmniejszają liczbę pytań, a audyty można prowadzić na tym samym szkielecie, na którym zbudowano ocenę ex ante; redukuje ryzyko, ponieważ ułatwia wczesne wykrywanie luk poprzez KRI i regularne przeglądy oraz przyspiesza wdrażanie działań korygujących i zapobiegawczych, co obniża zarówno prawdopodobieństwo incydentów, jak i ich wpływ; wzmacnia wiarygodność i zaufanie, gdyż zamawiający posługuje się uznanym aparatem pojęciowym i dowodowym, a wykonawcy dokładnie wiedzą, czego się od nich oczekuje — w efekcie jest mniej sporów, a więcej współpracy; wreszcie zmniejsza koszt całkowity, bo dobrze zaprojektowane, oparte na standardach wymagania i nadzór ograniczają liczbę awarii oraz „poprawek na produkcji".

Aby te korzyści rzeczywiście się zmaterializowały, wdrażając standardy do SWZ/OPZ należy zadbać o kilka praktycznych zasad. Po pierwsze, proporcjonalność: ciężar wymagań musi odpowiadać wpływowi usługi lub produktu na bezpieczeństwo publiczne i infrastrukturę — dla obszarów

krytycznych właściwy będzie pełny zestaw (certyfikacja, KRI, audyty na miejscu), a dla niskiego wpływu — zestaw uproszczony. Po drugie, precyzyjny zakres certyfikacji: sama informacja „mamy ISO/IEC 27001" nie wystarcza, trzeba potwierdzić, że zakres obejmuje dokładnie te obszary, które będą użyte przy realizacji zamówienia. Po trzecie, równoważność: jeśli dopuszcza się rozwiązania alternatywne, należy jasno opisać kryteria równoważności (poziom pewności, nadzór, zakres), aby uniknąć uznaniowości. Po czwarte, dowody i formaty: warto dołączyć matrycę dowodów z określeniem, co, jak często i w jakiej formie ma być dostarczane (np. raport KRI, rejestr incydentów, status łatek według poziomów ważności, wyniki audytów nadzorczych lub certyfikacyjnych). Po piąte, drabina eskalacji: każdy wymóg powinien mieć przypisany próg i odpowiadające mu działanie — od CAP, przez audyt doraźny, po podniesienie poziomu nadzoru — tak aby liczby przekładały się na decyzje, a nie kończyły na opisie.

### 5.1.2. Powiązanie standardów z regulacjami prawnymi – NIS2, CRA, DORA, RODO

W zamówieniach publicznych obowiązki prawne (NIS2, UKSC, RODO, CRA, DORA) wyznaczają **co** ma być zapewnione, natomiast standardy (ISO/IEC, wytyczne ENISA/NIST, programy certyfikacyjne) precyzują **jak** to zrobić, **jak to mierzyć** i **jakimi dowodami** wykazać zgodność. Zgodnie z art. 101 ust. 4 Pzp, gdy opis przedmiotu zamówienia odwołuje się do norm, specyfikacji technicznych lub równoważnych systemów odniesienia, odwołaniu temu muszą towarzyszyć słowa „**lub równoważne**", a równoważność podlega wykazaniu odpowiednimi środkami dowodowymi w rozumieniu art. 105 Pzp. Dlatego w całym niniejszym rozdziale wszystkie odniesienia do norm, wytycznych i programów certyfikacji należy rozumieć jako **wzorce odniesienia dopuszczalne w postaci rozwiązań równoważnych**. Wykonawca może wykazać równoważność poprzez zwięzłą mapę zgodności (najpierw wymóg, potem oferowane rozwiązanie a następnie dowód) oraz dostarcza środki dowodowe adekwatne do ryzyka i przedmiotu zamówienia. Takie spięcie prawa ze standardami zamienia ogólne wymogi w konkretne wymagania operacyjne (kontrolki, role, procedury, metryki), które można wpisać do OPZ/SWZ i monitorować w trakcie realizacji przedmiotu umowy — z korzyścią dla porównywalności ofert, rozliczalności wykonawców oraz spójności ex ante–ex post.

**NIS2 i UKSC**: zarządzanie ryzykiem i łańcuchem dostaw. W praktyce NIS2 i UKSC nakładają na jednostki publiczne oraz podmioty kluczowe/ważne obowiązek proaktywnego zarządzania ryzykiem, w tym ryzykiem w łańcuchu dostaw, oraz raportowania incydentów. Standardy zapewniają spójny zestaw narzędzi i mechanizmów, które pozwalają te obowiązki wdrożyć w sposób mierzalny i audytowalny:

- ISO/IEC 27001 – ramy systemu zarządzania bezpieczeństwem informacji: polityki, cele, odpowiedzialności, cykl PDCA; da się bezpośrednio zmapować na wymagania NIS2/UKSC dotyczące organizacji, ról i nadzoru.
- ISO/IEC 27002 – katalog kontrolek operacyjnych (m.in. zarządzanie dostępem, bezpieczeństwo zmian, logowanie i monitoring, zarządzanie podatnościami) – to materiał wejściowy do OPZ i późniejszych KRI.
- ISO/IEC 27005 – metoda analizy ryzyka (identyfikacja, ocena, traktowanie, akceptacja) – spina ocenę ex ante z monitoringiem trendów ex post.
- ISO/IEC 27036 (część 1–3) – bezpośrednio adresuje relacje z dostawcami ICT: klasyfikację dostawców, wymagania dla podwykonawców, dowody zgodności i mechanizmy audytu.

Efekt powiązania jest przyczynowo-skutkowy: określone przez NIS2/UKSC obowiązki → odpowiadające im kontrolki ISO → dowody (procedury, logi, raporty) → progi i reakcje (CAP, audyt doraźny, eskalacja). Dzięki temu wymagania prawne nie pozostają ogólne, tylko stają się mierzalne i egzekwowalne.

**CRA** to reguły bezpieczeństwa wyrobu i cykl życia poprawek. CRA przesuwa środek ciężkości na produkt z elementem cyfrowym (urządzenie, oprogramowanie, komponent) i jego pełny cykl życia: bezpieczeństwo projektowe (*by design*), bezpieczne ustawienia domyślne (*by default*), zarządzanie podatnościami, aktualizacje oraz transparentna komunikacja o lukach. W praktyce, aby przełożyć to na wymagania  postępowania o udzielenie zamówienia publicznego i nadzór, warto oprzeć się na następujących odniesieniach:

- **ISO/IEC 27036-3** – wymagania dla komponentów i dostawców oprogramowania, w tym obowiązek posiadania **SBOM** oraz **kryteriów akceptacji bezpieczeństwa** na etapie odbioru (np. testy podatności, skan zależności, weryfikacja konfiguracji).
- **ISO/IEC 27002** (obszary: zarządzanie zmianą, twardnienie konfiguracji, monitoring) – naturalnie łączy się z wymogami CRA dotyczącymi **kontrolowanego cyklu zmian** oraz ciągłego nadzoru nad konfiguracją i logowaniem.

Aby wymogi CRA realnie „zadziałały” w postępowaniu, należy wpisać je do OPZ w formie jasnych, mierzalnych obowiązków wykonawcy oraz oczekiwanych dowodów. W opisie przedmiotu zamówienia warto więc wskazać, że wraz z każdą dostawą oprogramowania lub urządzenia z elementem cyfrowym wykonawca przekazuje kompletną dokumentację, zawierającą m. in.: wykaz komponentów (SBOM) aktualizowany przy każdej wersji, z podaniem nazw, wersji i źródeł zależności oraz informacją o znanych podatnościach. Równolegle trzeba opisać wymóg posiadania i stosowania polityki zarządzania podatnościami i aktualizacjami (patch management), w której określone są maksymalne terminy usuwania luk w zależności od ich wagi, sposób komunikowania dostępności poprawek oraz forma potwierdzania wdrożenia (raport z datami, numerami wersji i zakresem zmian). Trzecim elementem, który należy ująć w OPZ, jest procedura obsługi zgłoszeń podatności: dedykowany kanał kontaktu (np. adres e-mail VDP), gwarantowane czasy reakcji i informowania zamawiającego, a także praktyka publikowania informacji o istotnych lukach. Warto dodać, że odbiór każdej wersji obejmuje przekazanie raportu bezpieczeństwa (wyniki skanów i testów, wnioski) oraz że niedotrzymanie terminów udostępniania poprawek lub brak wymaganych artefaktów traktowane jest jako przekroczenie progu ryzyka i uruchamia uzgodnioną ścieżkę CAP (działania korygujące) lub — gdy to konieczne — czasowe ograniczenie funkcji do czasu usunięcia słabości. Dzięki takiemu zapisowi OPZ łączy obowiązki CRA z konkretnymi dowodami i reakcjami, co umożliwia egzekwowanie zgodności przez cały cykl życia rozwiązania.

**DORA** formułuje wymogi odporność operacyjnej w ekosystemie finansowym. Stawia na to, by instytucje finansowe oraz ich dostawcy ICT utrzymywali zdolność do działania mimo incydentów i zakłóceń, a więc by nie tylko zapobiegali awariom, lecz także potrafili się na nie przygotować, je wykrywać, ograniczać ich skutki i wracać do normalnej pracy w kontrolowanym czasie. Standardy międzynarodowe porządkują ten wymóg na poziomie procesów, kontrolek i dowodów.

Normy i wytyczne wspierające zgodność z DORA (skrót mapowania):

- ISO/IEC 27001/27002 — SZBI, kontrolki dla usług krytycznych, logowanie/monitoring, zarządzanie dostępem, zarządzanie zmianą.
- ISO/IEC 27005 — metodyka oceny ryzyka i priorytety odtworzeniowe dla usług outsourcowanych.
- ISO 22301 — zarządzanie ciągłością działania (RTO/RPO, testy i ćwiczenia DR, przeglądy, doskonalenie).

- ISO/IEC 27036 — zarządzanie relacjami z dostawcami ICT: wymagania dla podwykonawców, przepływ wymagań (down-flow), mechanizmy audytu i dowody.
- *(opcjonalnie, gdy właściwe dla zakresu)* ISO/IEC 27031 — gotowość ICT na potrzeby ciągłości działania (planowanie, zasoby, testy techniczne).

Przekładając to na praktykę postępowania, warto budować prostą ścieżkę: wymagania DORA → kontrolki i testy z mapowaniem na ISO/IEC 27001/27002/22301 → weryfikowalne dowody → z góry ustalone reakcje. W OPZ można więc wskazać, że wykonawca utrzymuje i przedstawia plan odporności operacyjnej powiązany z analizą ryzyka (ISO/IEC 27005) oraz że podlega cyklicznym ćwiczeniom DR zgodnie z ISO/IEC 22301, których wyniki (raporty z testów, wnioski, czasy przywrócenia) są udostępniane zamawiającemu. Warto też zdefiniować zestaw metryk operacyjnych, które będą monitorowane w trakcie umowy — na przykład MTTD/MTTR dla incydentów bezpieczeństwa i awarii — oraz powiązać określone poziomy tych wskaźników z decyzjami nadzorczymi (np. podniesienie poziomu nadzoru, audyt doraźny, wzmocnienie zasobów). Wymóg kontroli łańcucha dostaw należy domknąć zapisami wynikającymi z ISO/IEC 27036: te same wymagania i standardy mają obowiązywać podwykonawców, a wykonawca odpowiada za ich egzekwowanie oraz dostarczanie jednolitych dowodów (raporty testów, rejestry incydentów, wyniki klasyfikacji dostawców). Taki układ sprawia, że odporność operacyjna wymagana przez DORA jest opisana a także mierzona, raportowana i egzekwowana na całej długości łańcucha dostaw.

**RODO** wymaga, aby administrator i podmiot przetwarzający nie tylko wdrożyli odpowiednie zabezpieczenia, lecz także potrafili wykazać ich stosowanie (rozliczalność) oraz projektowali rozwiązania w duchu privacy by design/by default. Standardy porządkują te obowiązki na poziomie procesów, kontrolek i dowodów, dzięki czemu da się je wpisać w OPZ i późniejszy nadzór.

Normy i wytyczne wspierające zgodność z RODO:

- ISO/IEC 27001 / 27002 — ramy SZBI oraz kontrolki istotne dla RODO: kontrola dostępu i minimalizacja uprawnień, segmentacja i szyfrowanie, logowanie i rozliczalność, zarządzanie zmianą, testowanie zabezpieczeń.
- ISO/IEC 27018 — ochrona danych osobowych w chmurze dla procesorów (role, rejestrowanie operacji, zasady udostępniania, subprocessing, przejrzystość).

- *(uzupełniająco, gdy to właściwe)* ISO/IEC 27701 — rozszerzenie 27001/27002 o system zarządzania informacją prywatną (PIMS), ułatwiający DPIA, role ADO/PDO, klauzule powierzenia i wykazanie rozliczalności.

W zamówieniach publicznych przekład wymogów RODO na praktykę postępowania i nadzoru polega na opisaniu wymagań funkcjonalnych i dowodowych, a nie na żądaniu określonej pieczęci. Należy więc wskazać, że wykonawca zapewnia system i kontrolki odpowiadające dobrym praktykom (np. tym opisanym w ISO/IEC 27001/27002, 27018, 27701), albo rozwiązania równoważne, które osiągają ten sam poziom ochrony i rozliczalności. W OPZ i aneksie bezpieczeństwa warto zastrzec obowiązek przedkładania weryfikowalnych dowodów: mapy kontrolek do wymogów RODO, rejestrów czynności, wyników DPIA, ustawień prywatności domyślnej (retencja, pseudonimizacja, maskowanie), logów dostępu, raportów z testów i przeglądów oraz — w usługach chmurowych — mechanizmów właściwych dla roli procesora (np. zasady subprocesorów, lokalizacja danych, transfery poza EOG). Dopuszczalne dowody równoważne to m.in. raport niezależnego audytu (wg ISO/IEC 19011), certyfikacje branżowe lub unijne, wyniki testów technicznych i przeglądów organizacyjnych — o ile zakres, poziom pewności i nadzór są porównywalne z praktykami referencyjnymi. Każdy wymóg powinien mieć przypisany próg (np. opóźnienia w realizacji praw podmiotów danych, wzrost nieuprawnionych dostępów, braki w logach rozliczalności) i reakcję (CAP z terminami, przegląd uprawnień, dodatkowe zabezpieczenia, a przy naruszeniu — powiadomienie zgodnie z RODO i UKSC), tak aby zgodność z RODO była mierzalna i możliwa do egzekwowania przez cały okres trwania umowy — bez obowiązku posiadania konkretnego certyfikatu, lecz przy zachowaniu zasady równoważności.

Podsumowując, aby opisywany mechanizm rzeczywiście wspierał zgodność z NIS2/UKSC, CRA, DORA i RODO, warto potraktować go jak instrukcję operacyjną do OPZ i aneksu bezpieczeństwa — taką, którą można bezpośrednio zastosować przy ocenie ofert oraz w nadzorze realizacji. Klucz polega na spięciu przepisów ze standardami, standardów z konkretnymi wymaganiami, a wymagań z dowodami i reakcjami, tak aby cały obieg informacji był spójny od etapu ex ante po ex post.

Po pierwsze: matryca zgodności prawo → standard → wymóg → dowód. Dla każdego obowiązku (np. NIS2/UKSC: zarządzanie podatnościami; RODO: rozliczalność; CRA: cykl życia poprawek; DORA: testy DR) należy wskazać odpowiadającą sekcję norm (np. ISO/IEC 27002, 27036-3, 27005, 22301), zapisać w

OPZ „co ma być zrobione i utrzymywane” (kontrolki, role, czasy reakcji), a obok zdefiniować dowód: co dostawca dostarcza, w jakiej formie i jak często (np. raport KRI, rejestr incydentów, status łatek wg ważności, SBOM z aktualizacjami, wyniki testów DR, wyciągi z logów rozliczalności). Taka tabela staje się wspólnym językiem dla oceny ofert i późniejszego nadzoru.

Po drugie: progi i reakcje, czyli jak liczby zamieniają się w decyzje**.** Do kluczowych wymogów należy przypisać progi (np. opóźnienia w aktualizacjach względem wagi luki, wzrost incydentów, zawieszenie certyfikacji) oraz działania po ich przekroczeniu: CAP z terminami i właścicielami, audyt incydentalny, podniesienie poziomu nadzoru, a w skrajnych przypadkach — ograniczenie funkcji do czasu naprawy. To jest moment, w którym wymagania regulacyjne przekładają się na konkretne działania operacyjne i zaczynają realnie sterować kontraktem.

Po trzecie: ciągłość dowodów od ex ante do ex post. Te same wymagania, które były badane przy ocenie ofert, muszą później zasilać monitoring w trakcie umowy: lekkie raporty miesięczne (KRI/KPI, incydenty, status działań korygujących, postęp łatek), przeglądy kwartalne (trend ryzyka wg ISO/IEC 27005, istotne zmiany organizacyjne, wnioski z testów i audytów) oraz audyt roczny wg ISO/IEC 19011 (zgodność, skuteczność, dojrzałość). Dzięki temu dzięki temu weryfikacja ofert i późniejszy nadzór opierają się na tym samym zestawie wymagań i dowodów — proces pozostaje spójny od etapu ex ante do ex post.

### 5.1.3. Wartość certyfikacji w procesie oceny ofert i zarządzania dostawcami

Certyfikacja w kontekście zamówień publicznych jest jednym z kluczowych mechanizmów zapewniających zgodność z wymaganiami prawnymi i normatywnymi, a także ograniczających ryzyko związane z bezpieczeństwem informacji i cyberzagrożeniami. Certyfikaty i programy oceny zgodności (np. ISO/IEC 27001, programy UE na gruncie rozporządzenia 2019/881/UE — tzw. ENISA, oceny zgodności w CRA), a także certyfiakcja w oparciu o ustawę z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa stanowią formalny, weryfikowalny dowód, że dostawcy stosują rozpoznane standardy bezpieczeństwa i zarządzania ryzykiem. Dla zamawiającego to realne narzędzie oceny ofert i późniejszego nadzoru: ułatwia weryfikację wymagań bezpieczeństwa oraz szacowanie poziomu ryzyka związanego z wyborem wykonawcy. W cyklu życia kontraktu certyfikacja (lub równoważna ścieżka dowodowa) stabilizuje oczekiwania i ułatwia egzekwowanie umowy.

1. **ISO/IEC 27001** – System zarządzania bezpieczeństwem informacji

Na czym polega: ISO/IEC 27001 potwierdza, że organizacja utrzymuje system zarządzania bezpieczeństwem informacji (SZBI), obejmujący m.in. ocenę ryzyka, polityki, role, nadzór i doskonalenie. W procesie oceny i nadzoru (skutek):

- Zgodność z regulacjami: dobrze udokumentowane mechanizmy zarządzania ryzykiem, reagowania na incydenty i ochrony danych wspierają wymogi NIS2/UKSC oraz RODO.
- Przejrzysta ocena ryzyka dostawcy: certyfikacja (lub równoważny audyt) potwierdza istnienie formalnych procesów identyfikacji, oceny i traktowania ryzyka; zmniejsza niepewność decyzyjną po stronie zamawiającego.
- Ciągły nadzór: audyty nadzorcze i recertyfikacyjne zapewniają cykliczne „punkty kontrolne" w trakcie trwania umowy (zasilają KRI i przeglądy kwartalne).

2. **CRA** – ocena zgodności wyrobów z elementem cyfrowym

Na czym polega: Cyber Resilience Act wprowadza obowiązki producentów i importerów dotyczące bezpieczeństwa produktu w całym cyklu życia (by design/by default, zarządzanie podatnościami, aktualizacje, komunikacja). CRA przewiduje ocenę zgodności odpowiednią do klasy ryzyka (nie zawsze będzie to „certyfikacja" w ścisłym znaczeniu). W procesie oceny i nadzoru (skutek):

- Odporność produktu: zamawiający otrzymuje weryfikowalne potwierdzenie, że wyrób/komponent spełnia wymogi bezpieczeństwa (w tym aktualizacje i obsługę podatności).
- Spójność z prawem UE: ocena zgodności CRA wspiera wymogi unijne wobec produktów cyfrowych — istotne zwłaszcza przy integracji z infrastrukturą publiczną i krytyczną.
- Ciągłość działania: obowiązki poprodukcyjne (np. publikacja informacji o lukach) można wprost wpiąć w raportowanie ex post.

3. **ENISA** – unijne programy certyfikacji cyberbezpieczeństwa (rozporządzenie 2019/881/UE)

Na czym polega: rozporządzenie (2019/881/UE) ustanawia ramy unijnych programów certyfikacji (np. dla usług chmurowych, komponentów, usług ICT) z poziomami pewności (Basic/Substantial/High).

W procesie oceny i nadzoru (skutek):

- Jednolity punkt odniesienia w UE: łatwiejsza porównywalność ofert i spójna ocena ryzyka między zamawiającymi.

- Wysoki poziom pewności: programy UE określają zakres badań i nadzór, co wzmacnia wiarygodność dowodów.
- Zgodność prawna: ułatwia wykazanie spełniania wymogów UE w obszarze cyberbezpieczeństwa.

4. **Krajowy System Certyfikacji Cyberbezpieczeństwa** (ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa Dz.U. 2025 r., poz. 1017)

Na czym polega: państwowe, akredytowane (PCA) ramy certyfikacji dla wyrobów, usług i procesów ICT, z nadzorem po wydaniu certyfikatu. Wypełnia lukę tam, gdzie brak jeszcze programu UE lub gdzie potrzebne są precyzyjne wymogi krajowe. W procesie oceny i nadzoru (skutek):

- Porównywalne i egzekwowalne dowody: decyzja nie opiera się na deklaracjach, lecz na audytowalnym procesie zgodności.
- Elastyczne osadzenie w umowie: obowiązek utrzymania certyfikatu przez cały okres, notyfikacje o zawieszeniu/ograniczeniu, prawo do audytu kontraktowego, CAP i sankcje proporcjonalne do ryzyka.
- Kompatybilność z UE: gdy pojawi się program unijny — możliwość migracji wymogu z okresem przejściowym; krajowy schemat może funkcjonować jako równoważny, o ile spełnia kryteria zakresu/pewności/nadzoru.

Certyfikacje i oceny zgodności porządkują wymagania i dostarczają sprawdzalnych dowodów. Dają zamawiającemu dwie korzyści: po pierwsze — lepszą ocenę ex ante (mniej niepewności co do dojrzałości i odporności dostawcy/produktu), po drugie — stabilny nadzór ex post (raporty z audytów nadzorczych, status certyfikatów, rejestr niezgodności, CAP). Przy zachowaniu zasady równoważności z ustawą Pzp, certyfikacja staje się praktycznym językiem łączącym prawo, standardy i codzienne decyzje operacyjne — wspiera transparentną, obiektywną ocenę ofert i realne zarządzanie ryzykiem w całym łańcuchu dostaw.

### 5.2. Normy ISO i ich zastosowanie w zamówieniach publicznych (ujęcie eksperckie, osadzone w praktyce PZP)

Normy ISO z rodzin 2700x i 2800x to kompletne modele zarządcze, które — właściwie zastosowane w cyklu postępowania i umowy — pozwalają zamawiającemu przełożyć ogólne wymagania cyberbezpieczeństwa na konkretne, mierzalne zobowiązania wykonawcy. Kluczowe jest, aby: (1) poprawnie odwzorować ryzyko związane z przedmiotem zamówienia na adekwatne normy i

poziomy dowodów; (2) ułożyć wymagania tak, by łączyły warstwę organizacyjną (system zarządzania) z warstwą produktowo-usługową (kontrole, konfiguracja, utrzymanie, testowanie); (3) egzekwować te wymagania poprzez precyzyjnie zdefiniowane dowody, wskaźniki oraz klauzule utrzymaniowe.

### 5.2.1. ISO/IEC 27001 i 27002 – systemowe podejście do zarządzania bezpieczeństwem informacji

W realiach Pzp ISO/IEC 27001 nie „gwarantuje bezpieczeństwa", lecz potwierdza, że u wykonawcy działa system zarządzania bezpieczeństwem informacji (SZBI) oparty na cyklu PDCA: ryzyka są identyfikowane i oceniane, cele oraz środki dobierane świadomie, skuteczność mierzona, a proces doskonalony. Z punktu widzenia zamawiającego stanowi to twardy dowód dojrzałości organizacyjnej — czy dostawca faktycznie zarządza uprawnieniami i kontami uprzywilejowanymi, incydentami i podatnościami, ciągłością działania i zmianami, a także relacjami w łańcuchu dostaw — oraz czy potrafi udokumentować te praktyki w sposób powtarzalny i weryfikowalny.

ISO/IEC 27002 pełni rolę praktycznego „słownika kontrolek", który przekłada ujęcie systemowe ISO/IEC 27001 na konkretne wymagania operacyjne. Zamiast ogólnych sformułowań o „bezpiecznym systemie", można precyzyjnie wskazać, co ma być wdrożone i jak będzie wykazane. W dokumentacji technicznej (OPZ) warto więc wymagać m.in. właściwego zarządzania tożsamością i dostępem (w tym dostępami uprzywilejowanymi), twardnienia konfiguracji i segmentacji środowisk, szyfrowania kluczowych strumieni danych, rejestrowania i korelacji zdarzeń, cyklicznego zarządzania łatkami oraz podatnościami, zabezpieczeń interfejsów API, kontroli środowisk deweloperskich i testowych, a także uporządkowanego nadzoru nad poddostawcami (z uwzględnieniem sub-supply chain). Dobrą praktyką jest dopisanie do każdej kontrolki oczekiwanego „śladu dowodowego" (np. zrzuty konfiguracji, raporty z narzędzi skanujących, logi zmian), co upraszcza późniejszą weryfikację.

Te normy można płynnie wpiąć w dokumentację postępowania o udzielenie zamówienia publicznego i umowę. W warunkach udziału należy wymagać dojrzałości równoważnej ISO/IEC 27001, przy czym zakres musi odpowiadać przedmiotowi zamówienia (wprost wskazać objęte lokalizacje, procesy i usługi). W OPZ należy selektywnie przywołać kontrolki z ISO/IEC 27002 jako wymagania

minimalne oraz określić formę dowodów i ich częstotliwość, tak aby materiał raportowy zasilający miesięczne przeglądy i kwartalne oceny ryzyka był spójny. W umowie warto zapisać kwartalne przeglądy elementów SZBI wykonawcy skorelowane z ryzykami zamawiającego, przekazywanie podsumowań audytów nadzorczych oraz śledzenie metryk skuteczności — takich jak czas publikacji i wdrożenia poprawek, odsetek nieudanych wdrożeń, czas wykrycia anomalii czy liczba powtarzalnych niezgodności. Dodatkowo warto wskazać zasadę równoważności: dopuszcza się inne mechanizmy o porównywalnym poziomie pewności i nadzoru, jeżeli dostarczają dowodów równej jakości.

W praktyce pojawiają się dwie typowe pułapki. Pierwsza to „certyfikat w szufladzie" — ryzyko, że dokument istnieje, ale proces nie żyje; temu zapobiega wymaganie aktualnego podsumowania ostatniego audytu nadzorczego i statusu działań korygujących. Druga to zbyt wąski zakres — gdy certyfikacja nie obejmuje obszarów, które faktycznie będą świadczyć usługę; dlatego należy doprecyzować, że zakres musi objąć właściwe funkcje i środowiska (np. centrum przetwarzania, usługi chmurowe, zespół utrzymania, SOC). Uzupełniająco warto powiązać wskazane kontrolki z progami reakcji i planami działań korygujących (CAP), tak aby liczby z raportów automatycznie prowadziły do decyzji. W tym układzie ISO/IEC 27001 i 27002 są użytecznym mechanizmem kontraktowym: wymagania są mierzalne, dowody jednoznaczne, a nadzór — powtarzalny, skuteczny i proporcjonalny do ryzyka.

### 5.2.2. ISO/IEC 27005 – metodologia zarządzania ryzykiem w łańcuchu dostaw

ISO/IEC 27005 jest dla zamówień publicznych istotnym narzędziem: nie narzuca jednego sposobu liczenia ryzyka, ale porządkuje cały tok rozumowania i dokumentowania tak, aby ścieżka od identyfikacji problemu do decyzji była spójna i możliwa do weryfikacji. W praktyce zaczyna się od jasnego nazwania tego, co chronimy — danych, usług, interfejsów, środowisk — oraz od rozpoznania zależności: kto i co dostarcza, gdzie znajdują się newralgiczne komponenty, które elementy łańcucha są zewnętrzne. Do tego dochodzi katalog realistycznych scenariuszy: awarie, błędy operacyjne, nadużycia, ataki. Dopiero na takim fundamencie sensownie opisuje się skutki, akceptowalny poziom ryzyka, a następnie dobiera środki zaradcze i sposób ich mierzenia. Ta dyscyplina sprawia, że wymagania w OPZ są proporcjonalne do ekspozycji, a nie przypadkowo „doklejone".

Zastosowanie ISO/IEC 27005 dobrze widać jeszcze przed ogłoszeniem postępowania. Zamawiający sporządza krótką, ale rzeczową macierz ryzyk, z której wynika, jakie obszary wymagają twardszych wymogów (np. kontrolki ISO/IEC 27002 dotyczące tożsamości, zarządzania zmianą i rejestrowania zdarzeń), a gdzie potrzebne są również ramy relacji z wykonawcą i jego poddostawcami (ISO/IEC 27036) lub ujęcie logistyczne i sprzętowe (ISO/IEC 28001). W tym samym kroku definiuje się poziomy tolerancji i apetytu na ryzyko (czyli poziomu ryzyka, który organizacja świadomie akceptuje, aby osiągnąć swoje cele), które później staną się progami wskaźników KRI oraz zapisami w aneksie bezpieczeństwa. Dzięki temu specyfikacja nie jest zbiorem ogólnych życzeń, tylko konsekwencją rozpoznanej sytuacji.

Moment składania ofert daje szansę, by zobaczyć, czy wykonawcy myślą o ryzyku równie systemowo. Zamiast deklaracji „zapewniamy bezpieczeństwo" należy wymagać zwięzłego rejestru ryzyk dla przedmiotu zamówienia, przygotowanego według logiki ISO/IEC 27005, wraz z propozycją traktowania (redukcja, transfer, unikanie, akceptacja) i metrykami monitoringu. Taki materiał pozwala porównać nie stylistykę oferty, lecz dojrzałość podejścia: czy dostawca widzi zależności w łańcuchu, czy rozpoznaje krytyczne interfejsy, czy planuje nadzór nad podatnościami i jasno opisuje eskalację. W efekcie ocena staje się porównywalna i obronna.

W trakcie realizacji umowy ISO/IEC 27005 „prowadzi" rytm nadzoru. Re-ocena ryzyka wykonywana cyklicznie — rozsądnie co kwartał — korzysta z tych samych miar, które zasilają wskaźniki KRI. Jeżeli trend ryzyka rośnie, mechanizm z góry uruchamia zagęszczenie testów i monitoringu: częstsze skany podatności, poszerzone próby odtworzeniowe, przeglądy uprawnień o większej szczegółowości. W tym samym czasie uruchamia się plan działań korygujących (CAP) z terminami i przypisaną odpowiedzialnością, a po wdrożeniu korekt mierzy się efekt — czy wskaźniki rzeczywiście wróciły do normy. Całość pozostaje spójna z obowiązkami regulacyjnymi: tam, gdzie w grę wchodzi ochrona danych, analiza ryzyka wskazuje, kiedy potrzebna jest DPIA i jak dowody z systemu bezpieczeństwa organizacji wspierają rozliczalność RODO; gdzie pojawiają się wyroby z elementem cyfrowym, wnioski z ISO/IEC 27005 przekładają się na zarządzanie podatnościami i komunikację zgodną z CRA.

Najważniejszy efekt dla zamawiającego to ciąg logiczny, który porządkuje zarówno dokumentację, jak i praktykę nadzoru: od ryzyka, przez wymagania i dowody, po

wskaźniki i egzekwowanie. Taki układ ogranicza uznaniowość, nie zostawia miejsca na marketingowe deklaracje i pozwala prowadzić rozmowę z wykonawcą w języku mierzalnych zobowiązań oraz sprawdzalnych rezultatów. Dzięki temu ISO/IEC 27005 jest osią, wokół której realnie buduje się wymagania, kontrolę i decyzje w całym cyklu życia zamówienia.

### 5.2.3. ISO/IEC 27036 (części 1–4) – relacje z dostawcami ICT i ocena ryzyka podwykonawców

ISO/IEC 27036 to zestaw norm, którego wewnętrzna numeracja porządkuje kolejne obszary (terminologię, cykl życia relacji, chmurę, łańcuch sprzętowy), ale z perspektywy zamawiającego najważniejsza jest treść: jak wbudować bezpieczeństwo w relację handlową i utrzymać je od pierwszego kontaktu aż po kontrolowane zakończenie umowy.

Na początku normy porządkują język i podstawowe zasady współpracy, co ogranicza rozbieżne interpretacje w SWZ/OPZ i umowach. Dalej prowadzą przez cały cykl życia relacji: od rozpoznania i weryfikacji (due diligence), przez sformułowanie kluczowych klauzul, aż po monitorowanie i „bezpieczne wyjście" z kontraktu (wycofanie dostępów, zwrot lub zniszczenie danych z potwierdzeniem). Istotny blok dotyczy usług chmurowych: podziału odpowiedzialności (shared responsibility), lokalizacji danych i jurysdykcji, wymagań konfiguracyjnych bezpieczeństwa (tenanci), logowania i udostępniania logów oraz testów bezpieczeństwa w środowiskach cloud. Osobny akcent pada na łańcuch sprzętowy: pochodzenie komponentów, kontrolę integralności i ryzyko manipulacji lub podróbek, a także reguły serwisu i procesu RMA, które często są niedoszacowanym źródłem ryzyka.

Przekład na dokumenty postępowania o udzielenie zamówienia publicznego i umowę zaczyna się od klasyfikacji dostawcy względem wpływu na usługi i dane. Od tej klasyfikacji powinna zależeć głębokość weryfikacji wstępnej, poziom wymaganych dowodów równoważnych certyfikacji, rygor klauzul bezpieczeństwa i zakres zastrzeżonego prawa audytu. W samej umowie warto wprost zapisać mechanizmy rekomendowane przez ISO/IEC 27036: rejestr podwykonawców i zależności (z prawem sprzeciwu do zmian), obowiązek notyfikacji i uzyskania zgody na modyfikacje architektury, lokalizacji lub hostingu, wymagania dotyczące rejestrowania zdarzeń i udostępniania logów w uzgodnionym formacie, testy akceptacyjne bezpieczeństwa przy odbiorze oraz po zmianach istotnych, a także

procedury „exit” (harmonogram, standard zwrotu/usunięcia danych i forma potwierdzenia). W rozwiązaniach chmurowych należy doprecyzować przenoszalność usług i danych: jak, w jakim terminie i w jakim formacie wykonawca udostępni materiały niezbędne do migracji bez przestojów.

Nadzór po podpisaniu umowy powinien być opisany równie jednoznacznie: kiedy i w jakim zakresie stosuje się audyty planowe, a kiedy doraźne; które kontrole można prowadzić zdalnie, a które wymagają wizyty on-site; jakie są minimalne progi raportowania incydentów i podatności; w jakich terminach mają powstawać działania korygujące. Taka konstrukcja zapewnia przewidywalność po obu stronach — wykonawca wie, jakie dowody i w jakiej formie ma dostarczać, a zamawiający dysponuje klarowną podstawą do egzekwowania wymagań.

Efekt zastosowania ISO/IEC 27036 jest praktyczny: bezpieczeństwo staje się integralnym parametrem relacji handlowej. Decyzje opiera się na jasno zdefiniowanych klauzulach i sprawdzalnych dowodach, a zarządzanie ryzykiem w łańcuchu dostaw — również w warstwie chmurowej i sprzętowej — pozostaje spójne z celami zamawiającego przez cały cykl życia kontraktu. Numeracja poszczególnych części normy służy tu jedynie jako układ odniesienia; w praktyce liczy się spójne zastosowanie jej zaleceń w dokumentacji i nadzorze.

### 5.2.4. ISO 28000 i 28001 – bezpieczeństwo łańcucha dostaw w ujęciu logistycznym i operacyjnym

W przypadku zamówień obejmujących sprzęt fizyczny ryzyko często ujawnia się nie w samej aplikacji, lecz w całej drodze urządzenia: od fabryki, przez magazyny i transport, aż po instalację i późniejszy serwis. Właśnie tu swoją wartość pokazują ISO/IEC 28000 (system zarządzania bezpieczeństwem łańcucha dostaw) i ISO/IEC 28001 (praktyki operacyjne). Te normy porządkują kwalifikowanie przewoźników i operatorów logistycznych, wymagania wobec zabezpieczeń magazynowych i kontroli stref, sposoby zapobiegania manipulacji ładunkiem oraz utrzymanie pełnej ciągłości dowodowej (chain-of-custody) dla każdego egzemplarza. Efekt jest praktyczny: zamawiający może wykazać, że sprzęt, który trafia do środowiska produkcyjnego, jest oryginalny, nie był podmieniany ani modyfikowany, a jego ścieżka od producenta do miejsca instalacji jest przejrzysta i możliwa do audytu.

Aby te wymagania działały, warto w dokumentacji postępowania o udzielenie zamówienia publicznego i w umowie opisać mechanizmy operacyjne i dowodowe wynikające z ISO/IEC 28001 w sposób spójny z kontrolkami IT z ISO/IEC 27002. W praktyce oznacza to włączenie: potwierdzenia pochodzenia (oświadczenia producenta/dystrybutora oraz ścieżka zakupowa po numerach seryjnych), kontroli integralności opakowań i plomb w każdym punkcie przekazania, zdefiniowanych procedur przyjęć i wydań magazynowych (role, protokoły, zapisy, próbkowanie kontroli), zasad fizycznego bezpieczeństwa miejsc składowania (strefy, dostęp, monitoring, retencja nagrań), a także reguł dla serwisu i logistyki zwrotnej/RMA (kto przejmuje, jak zabezpiecza, jak raportuje zgodność numerów seryjnych po powrocie). Dobrą praktyką jest wskazanie formy i częstotliwości dowodów: list przewozowych z odnotowanymi plombami, protokołów kontroli stanu, raportów z inspekcji magazynu oraz zestawień numerów seryjnych zarówno przy odbiorze, jak i po serwisie. Tak opisane wymagania logistyczne domykają luki w „sprzętowym" łańcuchu dostaw, które później są najkosztowniejsze i najtrudniejsze do naprawienia, a jednocześnie tworzą spójny komplet z wymaganiami ISO/IEC 27002 dotyczącymi konfiguracji, utrzymania i monitoringu.

### 5.2.5. Integracja ISO z systemem zamówień publicznych: kwalifikacja, wymagania, weryfikacja

Integracja norm ISO z systemem zamówień publicznych zaczyna się od ryzyka, a nie od szablonu. Przed opracowaniem dokumentacji należy wykonać zwięzłą analizę zgodną z ISO/IEC 27005: określić krytyczność usług i danych, prześledzić architekturę interfejsów i jurysdykcji, zidentyfikować zależności od podwykonawców oraz komponentów fizycznych. Z takiej diagnozy wynikają proporcjonalne wymagania: czasem wystarczy dojrzałość organizacyjna równoważna ISO/IEC 27001 u wykonawcy i wybrane kontrolki z ISO/IEC 27002, innym razem — ze względu na ekspozycję — potrzebne będzie dołożenie certyfikacji rozwiązania w programie unijnym (CSA/ENISA) lub w schemacie krajowym oraz, jeśli zamówienie obejmuje wyroby cyfrowe, spełnienie obowiązków wynikających z CRA. Taki porządek logiczny uzasadnia „twardsze" żądania i chroni przed zarzutem nadmiernego ograniczania konkurencji.

1. **Kwalifikacja wykonawcy (dojrzałość równoważna 27001, właściwy zakres)**

Należy w warunkach udziału wskazać, które obszary muszą być objęte dojrzałością równoważną ISO/IEC 27001 (np. SOC, utrzymanie, chmura, konkretne lokalizacje i procesy) oraz poprosić o krótkie podsumowanie ostatniego audytu nadzorczego i status niezgodności. To pozwala odróżnić symboliczny certyfikat od realnie działającego systemu.

2. **OPZ jako „język" kontrolek (**ISO/IEC **27002) i operacji (**ISO/IEC **27036/28001)**
   Należy zapisywać konkretne praktyki 27002 wraz z wymaganymi dowodami (konfiguracje, zrzuty ustawień, raporty z monitoringu, harmonogramy aktualizacji, zapisy testów odtworzeniowych). Przy podwykonawcach/chmurze należy dodać elementy ISO/IEC 27036 (rejestr sub-supply chain, notyfikacje zmian, dostęp do logów, testy akceptacyjne, zasady „exit"), a przy sprzęcie i logistyce — elementy ISO/IEC 28001 (integralność dostaw, pochodzenie, chain-of-custody).

3. **Hierarchia dowodów i wagi**
   Należy ustalić kolejność i znaczenie: (a) dojrzałość organizacji — dowód równoważny ISO/IEC 27001; (b) zaufanie do komponentu — certyfikacja produktu/usługi (program UE lub schemat krajowy); (c) bieżąca zgodność — konfiguracje i logi; (d) skuteczność — testy (skany podatności, testy konfiguracji, próby odtworzeniowe); (e) doskonalenie — raporty z audytów i przeglądów. Dla każdej kontrolki należy przypisać wymagany dowód i częstotliwość.

4. **Weryfikacja i nadzór w rytmie stałym, z progami eskalacji**
   Należy w umowie zapisać miesięczne raporty operacyjne (SOC/monitoring), kwartalne przeglądy ryzyka (wg ISO/IEC 27005) oraz roczne audyty nadzorcze i testy przyrostowe. Progi (przekroczenia KRI, opóźnienia w krytycznych aktualizacjach, zawieszenie certyfikacji) powinny uruchamiać ustaloną ścieżkę: eskalację, CAP, dodatkowe testy, ewentualnie kary lub wymianę komponentu. Przy chmurze i złożonych łańcuchach należy przewidzieć audyt incydentalny zgodny z duchem ISO/IEC 27036.

5. **Mechanizm zmiany w toku kontraktu („migracja" wymagań)**
   Należy przewidzieć, że pojawienie się programu unijnego dla klasy produktu dotąd objętej tylko schematem krajowym może skutkować migracją wymogu w określonym czasie (np. 12–18 miesięcy), z zapewnieniem ciągłości świadczenia i poziomu bezpieczeństwa.

6. **Spójność z regulacjami — ISO jako narzędzie dowodowe**
   Należy jasno wskazać, które dowody ISO wspierają konkretne obowiązki prawne: rejestry incydentów i oceny skutków (DPIA) na potrzeby RODO, procedury zarządzania podatnościami i aktualizacjami na potrzeby CRA, zapisy ISO/IEC 27036 o łańcuchu dostaw na potrzeby NIS2/UKSC. Dzięki temu wymagania są mierzalne, a nadzór przewidywalny.
7. **Proporcjonalność i konkurencyjność**
   Należy utrzymać relację między poziomem wymagań a wpływem zamówienia na bezpieczeństwo publiczne i infrastrukturę krytyczną. W praktyce oznacza to różnicowanie ciężaru dowodów i częstotliwości nadzoru: dla rozwiązań o wysokiej ekspozycji — pełny zestaw wymagań i przeglądów; dla usług o niskim wpływie — zestaw ograniczony, przy zachowaniu kluczowych mechanizmów rozliczalności.

## 5.3. Standardy i wytyczne NIST oraz ENISA

Punktem wspólnym dla NIST i ENISA jest operacjonalizacja wymagań: oba podejścia pokazują, jak przełożyć ogólne cele bezpieczeństwa na konkretne zapisy w dokumentacji postępowania o udzielenie zamówienia publicznego i w umowie. NIST dostarcza szczegółowych mechanizmów zarządzania ryzykiem łańcucha dostaw (m.in. klasyfikacja komponentów i dostawców, wymagania dowodowe, scenariusze testów i kryteria akceptacji), a ENISA porządkuje dobre praktyki europejskie i wskazuje minimalne oczekiwania wobec produktów/usług ICT oraz relacji z podwykonawcami. W realiach PZP oznacza to gotowe wzorce do włączenia w SWZ/OPZ i kontrakt: precyzyjne wymagania kontrolne, listy dowodów zgodności, rytm raportowania (SLA/OLA), zestawy wskaźników KRI i reguły działań korygujących (CAP). Z tych materiałów szczególnie korzystają postępowania o podwyższonej ekspozycji – z wieloma integracjami, elementami chmury, zależnościami w software supply chain czy komponentami brzegowymi – gdzie zamawiający potrzebuje nie tylko „co" ma być bezpieczne, ale „jak" to mierzyć, weryfikować i egzekwować w całym cyklu życia umowy.

### 5.3.1. SP 800-161 – zarządzanie ryzykiem łańcucha dostaw (ICT SCRM)

NIST SP 800-161 opisuje kompletny system SCRM dla rozwiązań ICT, osadzony w pełnym cyklu życia: od planowania postępowania, przez kwalifikację i wybór dostawców, po eksploatację, zmiany oraz zamknięcie umowy. Kluczową cechą jest

kaskadowość wymagań: to, co zamawiający uzgadnia z głównym wykonawcą, powinno być spójnie przeniesione na wszystkich podwykonawców (tzw. down-flow), a dowody zgodności muszą być porównywalne i audytowalne na każdym poziomie łańcucha. W praktyce PZP daje to bardzo użyteczną logikę „od ryzyka do dowodu": zidentyfikowane zagrożenia → przypisane kontrolki i obowiązki → konkretne artefakty → rytm weryfikacji i progi reakcji.

W praktyce zamówień publicznych warto zacząć od przygotowania zwięzłego profilu zagrożeń SCRM jeszcze przed publikacją OPZ. Taki profil porządkuje aktywa i krytyczne zależności, wskazuje typowe scenariusze zagrożeń oraz definiuje oczekiwany poziom pewności dowodów. Z niego powinny wynikać konkretne zapisy specyfikacji: wymóg przedstawienia SBOM dla komponentów oprogramowania, zakres i częstotliwość testów integralności i konfiguracji, a także warunki dotyczące dostawców elementów kryptograficznych czy kontroli jurysdykcji przetwarzania danych.

Kolejnym krokiem jest konsekwentne przeniesienie wymagań w dół łańcucha dostaw. W umowie należy jasno określić, że klauzule bezpieczeństwa, poziomy usług (SLA/OLA) oraz obowiązki raportowe obowiązują nie tylko głównego wykonawcę, lecz również wszystkich podwykonawców. Wymaga to prowadzenia aktualnego rejestru sub-supply chain z prawem sprzeciwu zamawiającego wobec zmian, a także wprowadzenia obowiązku niezwłocznej notyfikacji każdej istotnej zmiany po stronie dostawców (np. nowa lokalizacja przetwarzania, zmiana modelu świadczenia usługi).

Aby nadzór był mierzalny, trzeba z góry wskazać oczekiwane artefakty zgodności i rytm ich dostarczania. Po stronie wykonawcy powinien powstać plan bezpieczeństwa rozwiązania i utrzymania, który opisuje granice systemu, interfejsy, role i zastosowane kontrolki. Równolegle należy prowadzić plan działań korygujących (POA&M/CAP) z terminami i właścicielami zadań, utrzymywać aktualny SBOM wraz z informacją o podatnościach i ścieżką ich usuwania oraz cyklicznie przekazywać raporty testowe: z twardnienia konfiguracji, integralności komponentów, skanów podatności i testów regresji po zmianach. Częstotliwość tych raportów powinna być proporcjonalna do klasy ryzyka zamówienia.

Wreszcie, zarządzanie zmianą musi uwzględniać perspektywę SCRM. Każda istotna modyfikacja – wersja komponentu, zmiana dostawcy, przeniesienie danych do innej lokalizacji lub innej jurysdykcji, zmiana modelu chmurowego – wymaga

wcześniejszej notyfikacji, oceny wpływu na ryzyko oraz, gdy to zasadne, ponownego testu bezpieczeństwa i aktualizacji dokumentacji (SBOM). Dzięki temu powstaje „żywy" reżim SCRM, w którym z góry określone progi (np. opóźnienia w aktualizacjach krytycznych, negatywne wyniki testów integralności, zawieszenie certyfikacji w łańcuchu) automatycznie uruchamiają uzgodnione działania korygujące, a odpowiedzialności są jednoznaczne na każdym poziomie dostaw.

### 5.3.2. NIST Cybersecurity Framework (CSF) – pięć funkcji: *Identify, Protect, Detect, Respond, Recover*

NIST Cybersecurity Framework (CSF) to opracowany przez NIST ustandaryzowany model zarządzania cyberbezpieczeństwem, który porządkuje praktyki w pięciu funkcjach: Identify, Protect, Detect, Respond i Recover (w wydaniu 2.0 dodatkowo silniej akcentuje ład i odpowiedzialności – governance – oraz bezpieczeństwo łańcucha dostaw). Każda funkcja dzieli się na kategorie i podkategorie działań, a całość uzupełniają poziomy dojrzałości (Tiers) i tzw. Profil, który pozwala opisać stan obecny i cel do osiągnięcia. Taki układ ułatwia powiązanie wymagań regulacyjnych (NIS2, UKSC, RODO, CRA) z praktyką operacyjną i przeniesienie ich do języka postępowań Pzp.

W dokumentacji postępowania o udzielenie zamówienia publicznego warto zacząć od obszaru odpowiadającego Identify: wymagane powinny być aktualne spisy aktywów i zależności (mapy integracji, przepływy danych), klasyfikacja informacji oraz analiza ryzyka zgodna z ISO/IEC 27005, uzupełniona rejestrem dostawców i podwykonawców. Jako dowody sprawdzają się: wykaz aktywów, mapa danych, rejestr ryzyk wraz z właścicielami i datami przeglądów. Taki pakiet tworzy przejrzysty punkt wyjścia do oceny wpływu zmian i planowania kontroli.

Część korespondująca z Protect powinna opisywać codzienną ochronę: zarządzanie tożsamością i dostępami (w tym dostęp uprzywilejowany i zasada minimalnych uprawnień), twardnienie konfiguracji, szyfrowanie w spoczynku i w ruchu, kopie zapasowe z testami odtworzeniowymi oraz program szkoleń. Dowodami są polityki i konfiguracje, raporty z przeglądów uprawnień, rejestry kluczy i certyfikatów, protokoły testów DR. Warto doprecyzować parametry, np. maksymalny czas wdrożenia poprawek według ważności podatności oraz zakres ról objętych MFA.

W zakresie zbieżnym z Detect należy wymagać monitoringu i korelacji zdarzeń opartej o zdefiniowane źródła logów, reguły wykrywania i progi eskalacji. Raporty

SOC/SIEM, metryki MTTD, listy źródeł logów oraz opis przypadków użycia (use cases) stanowią weryfikowalne dowody. Dobrą praktyką jest wskazanie minimalnego zestawu telemetrycznego (np. logi uwierzytelniania, administracji, zmian konfiguracji, ruchu na krytycznych API) oraz częstotliwości przeglądu alertów i dopasowania reguł.

Część odpowiadająca Respond powinna opisywać plan reagowania na incydenty: role i odpowiedzialności (np. macierz RACI), sposób współpracy z zamawiającym, progi i terminy notyfikacji zgodne z UKSC, a także rytm ćwiczeń scenariuszowych. Dowodami są plan IRP, raporty z ćwiczeń, dzienniki incydentów i plany działań korygujących (CAP) z terminami i właścicielami. Warto jasno opisać integrację z procesem zgłoszeń formalnych (kanał, format, czas) oraz sposób włączania wniosków z incydentów do przeglądów kwartalnych.

Obszar Recover powinien zawierać wymagania dotyczące odtwarzania i odporności: zdefiniowane RTO/RPO dla usług, harmonogram i scenariusze testów DR, priorytety odtworzeń oraz zasady komunikacji po incydencie. Dowody to raporty z testów DR, wyniki walidacji RTO/RPO i wykaz działań naprawczych po testach. Przy usługach krytycznych warto dodać wymóg niezależnej weryfikacji wyników testów lub wspólnego przeglądu z zamawiającym.

Aby CSF pracował w całym cyklu życia umowy, profil obecny i docelowy należy opisać już na etapie oceny ofert (ex ante), a następnie powiązać z monitoringiem ex post: miesięcznymi raportami (KRI/KPI, incydenty, status działań CAP), przeglądami kwartalnymi (trend ryzyka wg ISO/IEC 27005, wnioski z testów DR i audytów) i audytem rocznym. Przekroczenie progów – np. spadek poziomu dojrzałości w wybranej funkcji, wzrost MTTD, opóźnienia we wdrożeniu poprawek – powinno automatycznie wywoływać uzgodnioną reakcję (CAP, audyt doraźny, podniesienie poziomu nadzoru). Dzięki temu CSF staje się praktyczną matrycą wymagań, dowodów i wskaźników: umożliwia porównywanie ofert w spójny sposób i egzekwowanie jakości bezpieczeństwa przez cały okres trwania umowy, a jednocześnie zachowuje zgodność z regulacjami i normami ISO/IEC.

### 5.3.3. ENISA

Podejście ENISA do bezpieczeństwa łańcucha dostaw jest praktyczne i „systemowe”[1]: zaczyna się od rozpoznania zależności międzyorganizacyjnych i ryzyka „ataku przez zaufanie” (kompromitacja jednego ogniwa otwiera drogę do kolejnych), a kończy na doborze proporcjonalnych środków technicznych,

organizacyjnych i kontraktowych. Kluczowym krokiem jest profilowanie dostawców według krytyczności i wpływu na usługi – od niskiego do najwyższego poziomu – oraz powiązanie każdej kategorii z adekwatnym zestawem wymagań i dowodów. Dzięki temu powstaje spójny program, w którym ten sam język wymagań stosuje się u zamawiającego i u wykonawcy (oraz u jego podwykonawców), a zgodność przestaje być statyczną deklaracją i staje się cyklem mierzalnych działań i przeglądów.

W praktyce ENISA zaleca, by zacząć od pełnego „obrazu łańcucha": inwentaryzacji systemów, komponentów i usług zewnętrznych, w tym bibliotek oprogramowania, usług chmurowych, repozytoriów i usługodawców wsparcia. Taki obraz nie kończy się na pierwszej linii dostawców – należy sięgnąć w głąb do podwykonawców oraz źródeł komponentów, tak aby wiedzieć, gdzie mogą pojawić się punkty styku jurysdykcji, zmiany lokalizacji danych czy nietypowe zależności operacyjne. Dopiero na tym fundamencie sens ma kategoryzacja dostawców i przypisanie „poziomów rygoru": dla dostawców niskiego wpływu zestaw minimalny, dla krytycznych – pełne wymagania wraz z prawem audytu i precyzyjnymi progami eskalacji.

Warstwa techniczna w ujęciu ENISA obejmuje w szczególności silne uwierzytelnianie i kontrolę dostępu (w tym dostępy uprzywilejowane), twardnienie konfiguracji i segmentację, szyfrowanie danych w ruchu i spoczynku, regularne skanowanie podatności oraz przejrzystość komponentów oprogramowania poprzez utrzymywanie wykazów elementów (np. list komponentów). Warstwa organizacyjna to m.in. szkolenia ukierunkowane na ryzyka łańcucha dostaw, rozdział obowiązków, cykliczne przeglądy uprawnień i zmian, a także jasne zasady zarządzania podwykonawcami. Wreszcie warstwa kontraktowa: prawo audytu planowego i doraźnego, obowiązek niezwłocznej notyfikacji incydentów i istotnych zmian w łańcuchu podwykonawców, wymagania dotyczące działań korygujących z terminami i odpowiedzialnością oraz zasady „wyjścia" z umowy, w tym potwierdzanie usunięcia danych i kontrola przekazania artefaktów.

Drugim filarem jest ciągłość monitorowania. ENISA kładzie nacisk na mierzalne wskaźniki ryzyka oraz jasne progi reakcji. Wskaźniki powinny obejmować co najmniej terminowość aktualizacji w relacji do wagi luk, liczbę i charakter niezgodności, zmienność podwykonawców i lokalizacji danych, a także sygnały zewnętrzne (np. publikacje o podatnościach czy ostrzeżenia branżowe). Przekroczenie progów nie może kończyć się „odnotowaniem w rejestrze" – musi

skutkować działaniami korygującymi, planem naprawczym z terminami i późniejszą weryfikacją efektu. Dzięki temu nadzór przechodzi od podejścia reaktywnego do przewidywalnego i powtarzalnego.

Równie istotne jest domykanie pętli uczenia się po incydentach i niezgodnościach. Wnioski z analizy przyczyn źródłowych powinny wracać do wymagań technicznych (np. zaostrzenie polityk aktualizacji), do klauzul kontraktowych (np. doprecyzowanie obowiązków raportowych podwykonawców) oraz do szablonów dokumentacji przetargowej na kolejne postępowania. ENISA podkreśla, że ataki często wykorzystują elementy pośrednie – komponent biblioteczny, mały podwykonawca z uprawnieniami serwisowymi, zaniedbana integracja API – dlatego „mikro-wnioski" z pojedynczych zdarzeń należy zamieniać na „makro-zmiany" w sposobie stawiania wymagań i prowadzenia nadzoru.

Z perspektywy zamawiającego wytyczne ENISA ułatwiają zamienienie ogólnych zasad na konkretne zapisy w dokumentacji i w umowie: kategoryzacja dostawców wraz z przypisanym poziomem kontroli; wymagania dotyczące przejrzystości komponentów i łańcucha podwykonawców; jednolite formaty raportów z bezpieczeństwa; prawo audytu oparte na z góry ustalonych scenariuszach (planowe, doraźne, tematyczne); a także klarowna „drabina reakcji", w której progi prowadzą do konkretnych działań (plan naprawczy, rozszerzony monitoring, audyt incydentalny, zawężenie funkcji, a w ostateczności – zmiana dostawcy komponentu). Taki, skalowalny model daje lekkość tam, gdzie wpływ jest niewielki i zdecydowany rygor tam, gdzie ryzyko jest najwyższe – zawsze z uzasadnieniem opartym na rozpoznanym profilu ryzyka i na dowodach, które można regularnie weryfikować.

### 5.3.4. Porównanie podejść: NIST vs. ENISA vs. ISO – różnice w modelach i dojrzałości systemowej

ISO (27001/27002/27005/27036/28001) to przede wszystkim porządek systemowy: jak zorganizować bezpieczeństwo, jak je utrzymywać i jak udowodnić, że działa. ISO/IEC 27001 nadaje strukturę (polityki, role, cykl PDCA) i pozwala wykazać dojrzałość organizacyjną w sposób powtarzalny (audyt, raport z niezgodności, działania korygujące). ISO/IEC 27002 przekłada ryzyko na praktyki operacyjne i techniczne, które można wpisać do OPZ jako wymagania minimalne wraz z formą dowodu. ISO/IEC 27005 porządkuje sposób myślenia o ryzyku i jego traktowaniu — od identyfikacji aktywów po akceptację ryzyka — dzięki czemu

wymagania przestają być „oderwane" od ekspozycji. ISO/IEC 27036 i 28001 osadzają te założenia w relacji kontraktowej oraz procesach logistycznych (podwykonawcy, łańcuch dostaw sprzętu, chain-of-custody). Z punktu widzenia Pzp właśnie ISO stanowi „materiał konstrukcyjny" SWZ/OPZ i umowy: umożliwia spójne projektowanie wymagań, wskazywanie dowodów, planowanie audytów i przeglądów oraz definiowanie progów eskalacji. Trzeba przy tym pamiętać, że ISO to ramy i mechanika zgodności — ich siłą jest audytowalność i porównywalność, a ograniczeniem bywa mniejsza szczegółowość w codziennych procedurach operacyjnych.

NIST SP 800-161 oraz NIST CSF mają charakter bardziej operacyjny: pokazują, jak ułożyć praktykę zarządzania ryzykiem łańcucha dostaw na co dzień. NIST SP 800-161 rozwija spojrzenie na zależności podwykonawcze i wymaga konsekwentnego przenoszenia wymagań na cały łańcuch (down-flow) wraz ze spójnymi dowodami zgodności i kontrolą zmian. CSF porządkuje komplet zabezpieczeń w pięciu funkcjach (Identify, Protect, Detect, Respond, Recover) i ułatwia ich mierzenie językiem zrozumiałym dla biznesu oraz komitetów sterujących. W zamówieniach publicznych NIST świetnie doprecyzowuje OPZ i nadzór: wskazuje oczekiwane artefakty (plany bezpieczeństwa rozwiązania, rejestry działań korygujących, wykazy komponentów oprogramowania/SBOM), metryki operacyjne (np. MTTD/MTTR, terminowość łatek według ważności), a także scenariusze ćwiczeń i sposób ich dokumentowania. NIST nie tworzy typowej „ścieżki certyfikacyjnej" jak ISO — jego wartość to gotowe wzorce praktyk, które można szybko włączyć do wymagań i raportowania.

ENISA (podejście do bezpieczeństwa łańcucha dostaw) akcentuje segmentację i zarządzanie zależnościami: najpierw klasyfikacja dostawców według wpływu i krytyczności, następnie przypisanie minimalnych wymagań technicznych, organizacyjnych i kontraktowych do każdej kategorii oraz utrzymanie stałego, proporcjonalnego monitoringu. To podejście wzmacnia dyscyplinę „na stykach" organizacji: obowiązek przejrzystości podwykonawców, jawne progi eskalacji, prawo audytu incydentalnego oraz cykliczne przeglądy wskaźników ryzyka (KRI). W Pzp ENISA dostarcza skali rygoru — lżejszej dla dostawców o niskim wpływie i zdecydowanie wyższej dla krytycznych — z czytelnym uzasadnieniem w

rozpoznanym profilu ryzyka. Jej przewagą jest praktyczna „mapa ciężaru wymagań" względem wpływu na usługę; ograniczeniem — mniejsza liczba formalnych mechanizmów dowodowych niż w ISO.

Wspólne wnioski są następujące: ISO buduje kręgosłup systemowy i język dowodów (certyfikacja, audyty, procedury), NIST doprecyzowuje warsztat operacyjny i konkretne artefakty oraz wymusza konsekwentne przeniesienie wymagań na podwykonawców, a ENISA wprowadza wymiar kategoryzacji i ciągłego nadzoru dopasowanego do wpływu. Z punktu widzenia dojrzałości systemowej ISO podnosi przewidywalność i rozliczalność, NIST — responsywność i jakość operacyjną, ENISA — spójność i proporcjonalność w łańcuchu. Razem tworzą komplementarny zestaw: od zasad i struktur, przez dokumenty robocze i metryki, po skalowanie wymagań i monitoringu adekwatnie do ryzyka.

Scalenie tych podejść w praktyce zamówień publicznych zaczyna się od ryzyka: przed publikacją OPZ należy wykonać zwięzłą analizę zgodną z ISO/IEC 27005 i na jej podstawie wyprowadzić wymagania techniczne, organizacyjne oraz dowodowe. W warunkach udziału należy odwołać się do dojrzałości równoważnej ISO/IEC 27001 z jasno wskazanym zakresem faktycznie obejmującym obszary pracy wykonawcy; w OPZ trzeba wskazać wybrane — i uzasadnione ryzykiem — kontrolki ISO/IEC 27002 wraz z oczekiwanymi formami dowodu spełnienia (konfiguracje, logi, raporty z testów). Tam, gdzie potrzebne jest doprecyzowanie praktyki operacyjnej i miar, należy korzystać z NIST SP 800-161 i NIST CSF: wymagane powinny być m.in. plany bezpieczeństwa rozwiązania, rejestry działań korygujących, wykazy komponentów (SBOM), metryki detekcji/reakcji oraz scenariusze i harmonogramy ćwiczeń. Dla uporządkowania nadzoru nad łańcuchem dostaw warto zastosować podejście ENISA: najpierw kategoryzacja dostawców według wpływu, następnie przypisanie adekwatnego poziomu rygoru (zakres audytów, intensywność monitoringu, wymagane dowody), z jasno zdefiniowanymi progami eskalacji i trybami audytu planowego oraz doraźnego. Jeżeli przedmiot zamówienia obejmuje wyroby lub usługi z elementem cyfrowym, należy — zależnie od klasy i dostępności programów — wymagać oceny zgodności/certyfikacji w programie unijnym lub krajowym oraz spełnienia obowiązków dotyczących cyklu życia poprawek i zarządzania podatnościami. W tak

ułożonym modelu ISO zapewnia porządek systemowy i rozliczalność, NIST dostarcza precyzyjnych artefaktów operacyjnych, a ENISA pilnuje, aby nadzór był proporcjonalny i obejmował cały łańcuch — dzięki czemu wymagania stają się spójne, mierzalne i egzekwowalne przez cały cykl życia umowy.

## 5.4. Integracja praktyk i standardów z systemem zamówień publicznych

Skuteczna integracja norm ISO, wytycznych NIST i ENISA oraz wymogów wynikających z UKSC/NIS2, CRA i unijnych programów certyfikacji wymaga zbudowania jednego, przejrzystego ciągu przyczynowo-skutkowego. Najpierw należy rozpoznać ryzyko właściwe dla przedmiotu zamówienia, następnie przełożyć je na konkretne wymagania techniczne i organizacyjne wraz z oczekiwanymi dowodami, a potem konsekwentnie egzekwować i doskonalić je w trakcie realizacji umowy. Dokumentacja postępowania o udzielenie zamówienia publicznego powinna „opowiadać" spójną historię: dlaczego ustanowiono właśnie takie wymogi (jaka ekspozycja stoi za decyzją), co dokładnie mają one zabezpieczać (usługi, dane, integracje, łańcuch podwykonawców) oraz w jaki sposób zostanie zweryfikowane ich spełnianie zarówno na starcie, jak i w toku świadczenia oraz przy zamknięciu kontraktu. Chodzi nie o sumę odrębnych standardów, lecz o jeden mechanizm: ryzyko prowadzi do wymagań, wymagania do dowodów, a dowody do decyzji i korekt. W takim ujęciu Pzp staje się narzędziem operacyjnego bezpieczeństwa — specyfikacja i umowa tworzą wspólną ramę, w której ISO nadaje strukturę i język dowodów, NIST doprecyzowuje praktykę i miary, a ENISA porządkuje kategoryzację dostawców oraz proporcjonalny nadzór nad łańcuchem dostaw.

### 5.4.1. Propozycje implementacji norm i standardów w dokumentacji postępowania o udzielenie zamówienia publicznego.

Na etapie przygotowawczym punkt wyjścia stanowi udokumentowana ocena ryzyka zgodna z ISO/IEC 27005. Powinna objąć: klasyfikację usług i danych (krytyczność, wrażliwość, wymogi regulacyjne), mapę integracji (interfejsy, przepływy i miejsca przetwarzania), identyfikację zależności (dostawcy, łańcuch podwykonawców, lokalizacje i jurysdykcje) oraz scenariusze zagrożeń (techniczne, organizacyjne, logistyczne, prawne). Dobrą praktyką jest krótkie rozeznanie rynku służące potwierdzeniu realności wymagań i weryfikacji dostępnych dowodów zgodności. Wyniki oceny należy przełożyć na podstawowy zestaw wymagań kontrolnych czerpany z ISO/IEC 27002, z jednoznacznym wskazaniem

oczekiwanych dowodów i częstotliwości ich dostarczania. W praktyce powinny tam trafić co najmniej: zarządzanie tożsamością i dostępem (uwierzytelnianie wieloskładnikowe, zasada najmniejszych uprawnień, przeglądy dostępów), twardnienie i standardy konfiguracji (systemy, urządzenia sieciowe, kontenery), szyfrowanie (w ruchu i spoczynku wraz z zarządzaniem kluczami), rejestrowanie i monitoring (źródła logów, retencja, korelacja), zarządzanie podatnościami (terminy wdrożeń poprawek zależne od wagi luk, testy przyrostowe), bezpieczeństwo SDLC/CI-CD (kontrola zmian, skany SAST/DAST, ochrona repozytoriów) oraz ciągłość działania/DR (RTO/RPO, testy odtworzeniowe). Warto od razu wskazać formaty dowodów (np. wyciągi z SIEM, zanonimizowane raporty testów, fragmenty konfiguracji) i minimalną szczegółowość, aby uniknąć rozbieżnych interpretacji.

Jeżeli przedmiot obejmuje produkty lub usługi ICT o podwyższonym ryzyku, warto odwołać się do unijnych programów oceny/certyfikacji (np. dla usług chmurowych lub komponentów), a w razie braku programu UE — do krajowych schematów certyfikacyjnych (akredytacja PCA). W dokumentacji należy wskazać oczekiwany poziom pewności oraz obowiązek utrzymania ważności certyfikacji przez cały okres umowy, łącznie z zasadami niezwłocznej notyfikacji zawieszenia, ograniczenia lub wygaśnięcia. Dla wyrobów z elementem cyfrowym należy zapewnić zgodność z przepisami o cyberodporności (m.in. deklaracja/ocena zgodności, obowiązki poprodukcyjne: publikacja i wdrażanie aktualizacji, obsługa podatności). Gdy zamówienie obejmuje komponent fizyczny lub część logistyczną, należy dołączyć wymagania z ISO 28001 (integralność dostaw, udokumentowany łańcuch przekazań, kontrola magazynowa, zabezpieczenie transportu, nadzór nad serwisem/RMA). Warto doprecyzować oczekiwane warunki lokalizacji i jurysdykcji danych (miejsce przetwarzania, transfery), aby ułatwić ocenę zgodności z prawem.

Warunki udziału powinny potwierdzać dojrzałość organizacyjną wykonawcy w zakresie bezpieczeństwa informacji na poziomie równoważnym ISO/IEC 27001 — z precyzyjnym wskazaniem zakresu adekwatnego do kontraktu (np. SOC, utrzymanie, środowiska chmurowe, lokalizacje, procesy). Należy przewidywać możliwość przedstawienia dowodów równoważnych (np. audyt niezależny zgodny z ISO/IEC 19011, program krajowy/UE o porównywalnym poziomie pewności i nadzoru), opisując kryteria równoważności (zakres, poziom pewności, nadzór i cykl audytów). Dobrym materiałem porównawczym będzie też zanonimizowane

podsumowanie ostatniego audytu nadzorczego wraz ze statusem niezgodności. Kryteria oceny powinny różnicować oferty jakościowo: wyższy poziom pewności w programie UE/krajowym niż wymagane minimum, szerszy i trafniej dopasowany zakres „ISO/IEC 27001-równoważny", dojrzałość procesów reagowania (np. MTTD/MTTR), gotowość do przekazywania wykazów komponentów (SBOM), wybranej telemetrii i raportów z testów DR, a także przejrzystość w zarządzaniu zmianą (wersje, komponenty, lokalizacja danych). Warto przewidzieć maksymalną objętość i strukturę załączników dowodowych, aby nie premiować objętości kosztem treści.

Postanowienia bezpieczeństwa w umowie (aneks bezpieczeństwa) powinny ustanawiać czytelne obowiązki po obu stronach. Po pierwsze, wymogi muszą „schodzić" do łańcucha podwykonawców: rejestr i aktualizacja listy podwykonawców, notyfikacja zmian, prawo sprzeciwu oraz wymóg utrzymania równoważnych standardów u podwykonawcy. Po drugie, należy zdefiniować rytm raportowania i przeglądów: krótkie raporty miesięczne (metryki KRI/KPI, incydenty, status działań korygujących), przeglądy kwartalne ryzyka zgodne z ISO/IEC 27005 oraz roczne audyty nadzorcze/tematyczne. Po trzecie, potrzebne są progi eskalacji (np. opóźnienia we wdrażaniu poprawek krytycznych, wzrost incydentów, zawieszenie certyfikacji) wraz z katalogiem reakcji: plan działań korygujących z terminami i odpowiedzialnościami, dodatkowe testy, możliwa wymiana komponentu, czasowe zawieszenie funkcji, a w sytuacjach skrajnych — odstąpienie proporcjonalne do ryzyka. Warto opisać minimalne treści raportów (sekcje, wskaźniki, wnioski) oraz formaty wymiany danych, co ułatwia automatyzację przeglądów.

W zakresie rozliczalności i ochrony danych osobowych należy wskazać, które dowody wynikające z praktyk ISO/IEC (np. rejestry incydentów, przeglądy dostępów, wyniki testów odtworzeniowych, zapisy DPIA) wspierają obowiązki regulacyjne i jak będą prezentowane w raportach okresowych. Dobrze działa przypisanie ról po obu stronach: właściciel kontraktu, właściciel ryzyka, punkt kontaktowy ds. incydentów, osoba odpowiedzialna za CAP i za akceptację zmian. Przy rozwiązaniach chmurowych warto przewidzieć wizyty techniczne lub przeglądy zdalne z próbkami dowodów oraz jasno opisać granice dostępności informacji (aby pogodzić audytowalność z poufnością).

Dobrą praktyką jest dołączenie do OPZ/SWZ matrycy „wymaganie → źródło (norma/wytyczna) → typ dowodu → częstotliwość → próg akceptacji →

konsekwencja", z kolumną wskazującą właściciela po stronie wykonawcy. Uzupełniająco można dodać krótkie wzory: raportu miesięcznego (1–2 strony), protokołu przeglądu kwartalnego oraz szablonu CAP. Taki układ tworzy jedną, spójną ścieżkę: od ryzyka, przez wymagania i dowody, po egzekwowanie i doskonalenie — w sposób przejrzysty, proporcjonalny do ekspozycji i zgodny z zasadą równoważności przewidzianą w Pzp. Dzięki temu zamawiający unika zarówno nadmiernego obciążania wykonawców, jak i zbyt ogólnych zapisów, które trudno nadzorować w trakcie realizacji.

### 5.4.2. Harmonizacja wymogów ISO/NIST/ENISA z ustawą o UKSC i rozporządzeniem CRA

Harmonizacja polega na przełożeniu obowiązków regulacyjnych na działające procesy oraz sprawdzalne dowody ze standardów — tak, aby „co wymaga prawo" miało w dokumentacji i w praktyce swój odpowiednik „kto, jak, czym i kiedy to wykazuje". Dla UKSC/NIS2, które nakładają m.in. obowiązki zgłaszania incydentów, zarządzania ryzykiem w łańcuchu dostaw i utrzymania ciągłości działania, warto powiązać: (a) dojrzałość równoważną ISO/IEC 27001 (plan reagowania na incydenty, ciągłość/DR, przeglądy elementów SZBI), (b) wybrane kontrolki ISO/IEC 27002 (telemetria i logowanie, kopie zapasowe, kontrola dostępu, segmentacja), (c) miary z NIST CSF w obszarach Respond/Recover (np. czasy reakcji, kompletność procedur, wyniki ćwiczeń) oraz (d) kategoryzację dostawców według ENISA z odpowiadającymi im baseline'ami wymagań. Wprost w dokumentacji należy wskazać łańcuch: „zgłoszenie incydentu w X godzin" jest wsparte planem IR z rolami i RACI oraz progami notyfikacji (UKSC/NIS2), a także techniczną podstawą w postaci źródeł logów i retencji, praktyk DR (RTO/RPO i testy), oraz ram KRI, w których wzrost liczby i wagi incydentów automatycznie uruchamia eskalację i działania korygujące (CAP). Dobrym uzupełnieniem jest przypisanie właścicieli wskaźników po stronie wykonawcy i zamawiającego oraz określenie formatu dowodu (raport SOC, protokół ćwiczeń, wyciąg z rejestru incydentów) i częstotliwości jego dostarczania.

W przypadku CRA — dla wyrobów z elementem cyfrowym — konieczne jest powiązanie oceny zgodności/CE z operacyjnym nadzorem nad cyklem życia produktu. W OPZ warto zdefiniować SBOM jako punkt wyjścia do przyrostowych skanów i przeglądów podatności, określić harmonogramy wdrożeń aktualizacji bezpieczeństwa zależne od wagi luk (np. według CVSS), wskazać zasady koordynowanego ujawniania podatności (CVD) oraz sposób i rytm raportowania do zamawiającego (miesięczne zestawienia statusu łatek i incydentów

produktowych, kwartalne podsumowania trendów). Obowiązki poproduktowe CRA — publikacja informacji o lukach, dostarczanie aktualizacji w minimalnym okresie wsparcia — powinny mieć w umowie jasne odpowiedniki: terminy, forma dowodu (np. biuletyn bezpieczeństwa, wpis w changelogu, potwierdzenie wdrożenia), progi eskalacji i CAP. Warto także przewidzieć powiązanie z procesem zmiany: każda zmiana wersji, komponentu lub jurysdykcji przetwarzania danych wymaga notyfikacji, oceny ryzyka i — gdy właściwe — testu regresji bezpieczeństwa.

Jeśli dla danej klasy istnieje program unijny (np. EUCS/EUCC), należy wskazać oczekiwany poziom pewności (np. Substantial/High) i powiązać go z wymaganymi dowodami w toku umowy, tak aby audyt mógł korzystać z jednego zestawu artefaktów. Gdy program na poziomie UE nie jest dostępny, można odwołać się do krajowych schematów certyfikacji (akredytacja PCA), opisując kryteria równoważności (zakres, poziom pewności, nadzór) oraz przewidując klauzulę migracji do programu UE po jego publikacji (okres przejściowy i plan dostosowania bez przerywania świadczenia). Spójność materiału dowodowego warto utrzymać przez stosowanie artefaktów z rodziny NIST jako nośników treści technicznej — planów bezpieczeństwa rozwiązania (SSP), rejestrów działań korygujących (POA&M/CAP), wykazów komponentów (SBOM) i metryk SOC — przy jednoczesnym oparciu kontroli na ISO/IEC 27001/27002 oraz kategoryzacji i baseline'ach ENISA. W efekcie audyt i nadzór posługują się jedną, uzgodnioną listą dowodów, bez dublowania obowiązków i bez „podwójnej księgowości" między regulacjami a standardami.

Aby harmonizacja była widoczna operacyjnie, warto dodać dwie praktyki. Po pierwsze, matrycę mapującą prawo → standard → wymaganie → dowód → próg → reakcja, utrzymywaną jako załącznik do OPZ i aktualizowaną przy zmianach ryzyka; ułatwia to przeglądy kwartalne i redukuje spory interpretacyjne. Po drugie, jednolity rytm sprawozdawczości: co miesiąc lekki pakiet operacyjny (KRI/KPI, status łatek, incydenty i CAP), co kwartał przegląd ryzyka (ISO/IEC 27005) i zgodności z obowiązkami regulacyjnymi (UKSC/NIS2, CRA), raz w roku audyt planowy z próbkowaniem dowodów. Tak ustawiony cykl sprawia, że zgodność nie jest jednorazowa, lecz stale potwierdzana, a odchylenia szybko przechodzą w decyzje i działania.

### 5.4.3. Model „Cyber Supply Chain Assurance" dla administracji publicznej

Niniejszy punkt odnosi się do modelu „Cyber Supply Chain Assurance", rozumianego jako zorganizowany zestaw praktyk dających ciągłą i weryfikowalną pewność, że bezpieczeństwo w łańcuchu dostaw ICT jest utrzymywane na poziomie adekwatnym do ryzyka — od wszczęcia postępowania, przez realizację i zmiany, aż po wyjście z umowy. W praktyce łączy to trzy filary: jasne wymagania i dowody (normy, kontrolki, artefakty), stały pomiar i progi reakcji (KRI/KPI, eskalacje, CAP) oraz cykliczną weryfikację i uczenie się organizacyjne (przeglądy, audyty, aktualizacje wymagań). Innymi słowy, nie chodzi o jednorazową zgodność, lecz o ciągły reżim zapewniania bezpieczeństwa osadzony w dokumentacji postępowania o udzielenie zamówienia publicznego i nadzorze operacyjnym.

Na poziomie strategicznym warto utrzymywać zestaw profilów zakupowych (np. chmura IaaS/PaaS/SaaS, sieć i bezpieczeństwo brzegowe, endpoint/MDM, aplikacje rozwijane na zamówienie) wraz z gotowymi matrycami: właściwe normy i wytyczne (ISO/IEC 27001/27002/27036/28001, NIST CSF/800-161, podejście ENISA), dostępne programy certyfikacji (EUCS/EUCC oraz schematy krajowe) i obowiązki CRA, listy wymaganych dowodów (certyfikaty, konfiguracje, logi, skany, raporty testów, SBOM), a także zestaw metryk (KRI/KPI) i predefiniowane klauzule umowne dotyczące przenoszenia wymagań na podwykonawców, audytów planowych i doraźnych, ścieżek CAP oraz zasad „exit". Taki katalog powinien być aktualizowany po istotnych incydentach i zmianach regulacyjnych, tak aby „pewność" dostosowywała się do realiów.

Na poziomie taktycznym, czyli w ramach pojedynczego postępowania, najpierw wykonuje się krótką ocenę ryzyka zgodną z ISO/IEC 27005 i potwierdza właściwy profil. Następnie przygotowuje się OPZ i aneks bezpieczeństwa z baseline'em kontroli z ISO/IEC 27002, wymaganiami certyfikacyjnymi (unijnymi lub krajowymi) i obowiązkami wynikającymi z CRA, a w warunkach udziału wskazuje dojrzałość organizacyjną równoważną ISO/IEC 27001 z adekwatnym zakresem. Kryteria jakości różnicują oferty: poziomy certyfikacji, dojrzałość procesów reagowania (np. MTTD/MTTR), gotowość do przekazywania SBOM, telemetrii i raportów z testów odtworzeniowych oraz transparentność w zarządzaniu zmianą. Na etapie pytań/negocjacji doprecyzowuje się zakres certyfikacji, rytm dostarczania dowodów i harmonogram testów przyrostowych oraz definiuje zasady równoważności i ewentualnej migracji wymagań do programów unijnych.

Na poziomie operacyjnym nadzór powinien opierać się na przejrzystym panelu KRI/KPI (np. MTTD/MTTR, terminowość krytycznych łatek, liczba otwartych niezgodności, status certyfikacji), z progami uruchamiającymi eskalacje (audyt

incydentalny, zwiększenie gęstości testów, dodatkowe raporty) i działaniami korygującymi. Niezbędne jest repozytorium dowodów z kontrolą dostępu i wersjonowaniem (certyfikaty, raporty SOC, wybrane logi źródłowe, SBOM i jego zmiany, wyniki skanów, protokoły testów DR, raporty audytów) oraz uporządkowany proces zarządzania zmianą: modyfikacje wersji, lokalizacji, podwykonawców i uprawnień muszą wyzwalać notyfikację, ocenę ryzyka i — w razie potrzeby — test regresji bezpieczeństwa. Role powinny być klarownie zdefiniowane: zamawiający jako właściciel ryzyka akceptuje poziom resztkowy i uruchamia eskalacje; wykonawca jako właściciel zgodności utrzymuje certyfikacje i dostarcza dowody; jednostka audytowa weryfikuje równoważność i rekomenduje działania; CSIRT koordynuje obsługę incydentów, notyfikacje regulacyjne i odbudowę usług.

Dla przedsięwzięć o wysokiej krytyczności warto przewidzieć tryb wzmocniony: częstsze skany przyrostowe (np. tygodniowe dla komponentów wystawionych do Internetu), syntetyczne testy detekcji, niezależne testy konfiguracji według uznanych benchmarków, rozszerzoną telemetrię (EDR z udziałem zamawiającego) oraz gęstsze przeglądy KRI. Dzięki tak ułożonemu modelowi zapewnianie bezpieczeństwa w łańcuchu dostaw staje się procesem ciągłym, mierzalnym i możliwym do egzekwowania w całym cyklu życia umowy — dokładnie tym, co oznacza „Cyber Supply Chain Assurance".

### 5.4.4. Znaczenie szkoleń, certyfikacji i audytów dla profesjonalizacji zamawiających

Punktem wyjścia jest założenie, że wymagania bezpieczeństwa będą skuteczne tylko wtedy, gdy osoby po stronie zamawiającego potrafią je rzetelnie zaplanować, ocenić i egzekwować. Dlatego rozwój kompetencji powinien obejmować zarówno rozumienie przepisów, jak i umiejętność operacyjnej pracy z dowodami oraz znajomość standardów, które te dowody porządkują. Najpierw potrzebna jest pewność w obszarze regulacyjnym: należy sprawnie poruszać się po Pzp (proporcjonalność wymagań, zasady równoważności, jawność), UKSC/NIS2 (terminy notyfikacji, odpowiedzialności, zarządzanie ryzykiem łańcucha dostaw), CRA (ocena zgodności wyrobów z elementem cyfrowym, obowiązki po sprzedaży) i RODO (DPIA, powierzenia, transfery). Najlepsze efekty przynoszą szkolenia oparte na rzeczywistych przypadkach — z analizą stanowisk regulatorów i wniosków po incydentach — po których powstają gotowe do użycia zapisy do OPZ

i aneksów (np. progi eskalacji, wymagane typy dowodów, harmonogramy raportowania).

Równolegle warto budować biegłość w stosowaniu norm i wytycznych. Chodzi nie o „znajomość tytułów", ale o umiejętność przełożenia ich na język konkretnych wymagań i audytowalnych efektów. ISO/IEC 27001 oraz ISO/IEC 27002 porządkują system i kontrolki, ISO/IEC 27005 daje metodykę oceny ryzyka, ISO/IEC 27036 i ISO/IEC 28001 wskazują, jak wpisać bezpieczeństwo w relację kontraktową i przepływ towarów/usług. NIST (CSF i SP 800-161) dostarcza praktycznych artefaktów — planów bezpieczeństwa rozwiązania, rejestrów działań korygujących, wykazów komponentów (SBOM), metryk detekcji i reakcji — które świetnie nadają się na „nośniki dowodów" w umowie. ENISA pomaga dobrać rygor wymagań do kategorii dostawcy i utrzymać lekki, ale stały program monitoringu. Te kompetencje warto umacniać ścieżkami certyfikacyjnymi (np. audytor/implementer ISO/IEC 27001, menedżer ryzyka 27005) oraz krótkimi warsztatami „z dokumentu do OPZ", w których ćwiczy się mapowanie wymagań na dowody i pisanie precyzyjnych klauzul bezpieczeństwa.

Trzecia warstwa to praktyka operacyjna, czyli umiejętność pracy z danymi, które spływają w trakcie realizacji umowy. Przydaje się zdolność czytania raportów SOC i logów, rozumienia SBOM i wpływu zmian komponentów, znajomość podstaw testów (skany podatności, hardening, testy odtworzeniowe), a także nawyk pracy ze wskaźnikami KRI/KPI (np. MTTD/MTTR, terminowość łatek, liczba i kategorie incydentów). Kluczowe jest też sprawne domykanie planów działań korygujących: formułowanie działań, ustalanie terminów i odpowiedzialności, a później weryfikacja skutków i aktualizacja rejestru ryzyk. Dobre rezultaty dają ćwiczenia reagowania i odtwarzania z udziałem wykonawców, CSIRT i audytu, prowadzone na realnych narzędziach (SIEM, EDR, system zgłoszeń). Po każdym ćwiczeniu powinny powstać trwałe korekty wzorców OPZ i aneksów, tak aby lekcje nie znikały wraz z raportem z ćwiczeń.

Całość domyka program audytów, rozumiany jako pętla doskonalenia. Audyty wewnętrzne pozwalają sprawdzić spójność dokumentacji, próbkować dowody i zweryfikować skuteczność kontrolek (np. czy deklarowane RTO/RPO potwierdzają się w testach). Audyty zewnętrzne służą weryfikacji certyfikatów i praktyk dostawcy, ocenie równoważności rozwiązań oraz kontroli nadzoru w reakcji na

progi KRI; w razie potrzeby mogą przybierać formę audytów doraźnych. Po każdym incydencie lub istotnym odchyleniu warto przeprowadzić przegląd po-zdarzeniowy: zidentyfikować przyczyny, ocenić luki kontrolne i zaproponować zmiany. Wnioski powinny zasilać wspólne repozytorium wzorców: doprecyzowane baseline'y ISO/IEC 27002, wyraźniej opisane metryki (w tym progi i konsekwencje), mocniejsze klauzule „down-flow" dla podwykonawców, realistycznie zweryfikowane parametry ciągłości, zaktualizowane matryce dowodów wraz z częstotliwościami i kryteriami akceptacji. Dzięki temu szkolenia, certyfikacje i audyty nie działają w izolacji, tylko składają się na jeden spójny mechanizm profesjonalizacji, który bezpośrednio podnosi jakość dokumentacji postępowania o udzielenie zamówienia publicznego i skuteczność nadzoru nad bezpieczeństwem w całym cyklu życia umowy.

## 6. Przykłady złych i dobrych praktyk

Zestawienia dobrych i złych praktyk pojawiają się w trakcie debat dotyczących budowania cyberodporności. Prosto i trafnie zestawiła je brytyjska agencja National Cyber Security Center[135]. Opierając się na brytyjskim zestawieniu można zaproponować lekko zmodyfikowany pod kątem zamówień publicznych wzór dobrych i złych praktyk.

### Zestawienie dobrych i złych praktyk w zakresie cyberbezpieczeństwa łańcucha dostaw

| Dobre praktyki | Złe praktyki |
|---|---|
| Uzyskanie świadomości w organizacji, że dostawcy mogą stanowić ryzyko zarówno dla zamawiających świadczone przez nich usługi publiczne, jak i dla wykonawców oraz oferowanych przez nich dostaw lub usług. | Brak wystarczającej wiedzy w organizacji na temat ryzyk wynikających z działalności dostawców oraz oferowanych przez nich produktów lub usług. |
| Uzyskanie możliwie najdokładniejszej wiedzy o tym, jak rozbudowany i złożony jest łańcuch dostaw w organizacji, z uwzględnieniem podwykonawców. | Znajomość wyłącznie najbliższych wykonawców lub dostawców, bez analizy, z jakimi podwykonawcami współpracują i w jaki sposób. |
| Poznanie zasad zarządzania informacją i ryzykiem w obszarze | Brak rozeznania w standardach cyberbezpieczeństwa obowiązujących u |

[135] https://www.ncsc.gov.uk/collection/supply-chain-security/assessing-supply-chain-security

| | |
|---|---|
| cyberbezpieczeństwa, stosowanych przez zamawiających, wykonawców i podwykonawców. | współpracujących dostawców oraz założenie – bez jakiejkolwiek weryfikacji – że kwestie bezpieczeństwa traktują oni z należytą powagą. |
| Kontrolowanie bezpieczeństwa łańcucha dostaw poprzez wprowadzenie wymogów (np. w opisie przedmiotu zamówienia lub w umowie) dotyczących udostępniania wyników audytów bezpieczeństwa przeprowadzanych u wykonawców i podwykonawców. | Brak kontroli nad bezpieczeństwem łańcucha dostaw; brak zainteresowania tym, czy wykonawcy i podwykonawcy przeprowadzają audyty bezpieczeństwa oraz jak reagują na cyberincydenty. |
| Stawianie dostawcom przez zamawiających lub wykonawców adekwatnych i proporcjonalnych wymagań w obszarze cyberbezpieczeństwa, wraz z jednoznacznym określeniem minimalnych wymagań. | Brak jasno określonych, adekwatnych i proporcjonalnych wymagań w obszarze cyberbezpieczeństwa; brak wyraźnego zakomunikowania wymagań dostawcom. |
| Stosowanie podejścia opartego na analizie ryzyka, odzwierciedlonego w klauzulach umownych dotyczących odpowiedzialności i zarządzania cyberincydentami. | Pomijanie w organizacji oceny ryzyka; nieuwzględnianie w umowach kwestii zarządzania cyberincydentami oraz odpowiedzialności za ich skutki. |
| Stosowanie zasady proporcjonalności wobec różnego rodzaju usług, produktów i procesów ICT w celu dostosowania wymagań do potrzeb organizacji oraz realiów rynkowych. | Stosowanie nieproporcjonalnych, powtarzalnych i niedostosowanych do rynku wymagań wobec usług, produktów lub procesów ICT, co utrudnia dostęp do zamówienia lub nieuzasadnione eliminuje potencjalnych dostawców. |
| Konsekwentne egzekwowanie wymagań w całym łańcuchu dostaw. | Ograniczanie realizacji wymagań wyłącznie do dostawców, bez nadzoru nad ich wdrożeniem. |
| Dokonywanie samooceny w zakresie bezpieczeństwa – niezależnie od tego, czy organizacja pełni rolę zamawiającego, wykonawcy, czy obu – z uwzględnieniem swojej roli w łańcuchu dostaw i obowiązku przekazywania dalej wymagań otrzymanych od podmiotów nadzorujących lub nadzorowanych (np. | Zaniedbywanie diagnozy własnej roli jako ogniwa mogącego stanowić ryzyko dla bezpieczeństwa oraz zaniechanie przekazywania wymagań otrzymanych od podmiotów nadzorujących lub nadzorowanych. |

| | |
|---|---|
| związków gmin, spółek zależnych, jednostek budżetowych). | |
| Wspieranie wykonawców przez zamawiających poprzez jasne wytyczne dotyczące zarządzania cyberincydentami oraz prowadzenie komunikacji zachęcającej do poszerzania wiedzy w zakresie cyberbezpieczeństwa. | Brak komunikacji pomiędzy zamawiającym a wykonawcami; brak transferu wiedzy o ryzykach dla łańcucha dostaw. |
| Stosowanie kryteriów oceny ofert promujących produkty i usługi gwarantujące wysoki poziom cyberbezpieczeństwa. | Stosowanie wyłącznie kryterium ceny, bez uwzględnienia innych kryteriów jakościowych związanych z cyberbezpieczeństwem. |
| Monitorowanie efektywności wymagań w zakresie cyberbezpieczeństwa poprzez odpowiednio dobrane klauzule umowne, zapewniające ciągłość kontroli i wsparcia w przypadku wystąpienia cyberincydentu. | Nieuwzględnianie w umowach wymagań dotyczących reagowania na cyberincydenty oraz opieranie się na założeniu, że wykonawca, producent lub dostawca samodzielnie udzieli niezbędnej pomocy. |
| Tworzenie warunków postępowania o udzielenie zamówienia publicznego, które premiują wykonawców skutecznie zarządzających ryzykiem w obszarze cyberbezpieczeństwa. | Brak jakichkolwiek warunków dotyczących cyberbezpieczeństwa w postępowaniach o udzielenie zamówienia; ignorowanie ryzyk mogących wynikać z cyberincydentów. |

Literatura:

Clark, S., Dahl, J. „Huawei's solar tech sparks fears of Europe's next dependency crisis", POLITICO, online: https://www.politico.eu/article/europe-solar-industry-having-huawei-moment/ [dostęp: 12.11.2025].
ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, "Threat Landscape for Supply Chain Attacks", 29 lipca 2021, s. 6–7, online: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks oraz https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf [dostęp: 12.11.2025].

Europol. International investigation disrupts phishing-as-a-service platform LabHost, 18 kwietnia 2024, online: https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost.
Fertsch, M. „Podstawy logistyki", Wydawnictwo Instytut Logistyki i Magazynowania, Poznań 2008, s. 175.
Gawrońska-Baran, A. [w:] E. Wiktorowska, A. Wiktorowski, P. Wójcik, A. Gawrońska-Baran, „Prawo zamówień publicznych. Komentarz aktualizowany", LEX/el. 2024, art. 116.
Kwaśniewska, D. „Zhakowani mimo wydania 500 mln na IT. Clorox pozywa Cognizant", CyberDefence24, 24.07.2025, online: https://cyberdefence24.pl/cyberbezpieczenstwo/zhakowani-mimo-wydania-500-mln-na-it-clorox-pozywa-cognizant [dostęp: 12.11.2025].
Liderman, K., Księżopolski, A. „Cyberbezpieczeństwo łańcuchów dostaw / Supply chain cybersecurity", Cybersecurity & Cybercrime, t. 1, nr 8, rocznik 2025, online dostęp: 12.11.2025.
Maciąg, A., Tarnowski, I. „Atak teleinformatyczny na polski sektor finansowy", Rządowe Centrum Bezpieczeństwa, online: https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [dostęp: 12.11.2025].
McFarlane, S. „Rogue communication devices found in Chinese solar power inverters", Reuters, 14 maja 2025, online: https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/ [dostęp: 12.11.2025].
MITRE. "ATT&CK Matrix for Enterprise", online: https://attack.mitre.org/ [dostęp: 12.11.2025].
National Cyber Security Centre, „Supply chain security guidance", on line https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security/ii-establish-control
Nowak, H. (red.), Winiarz, M. „Prawo zamówień publicznych. Komentarz", wyd. II, online: https://www.gov.pl/web/uzp/komentarz-do-prawa-zamowien-publicznych [dostęp: 12.11.2025], s. 83.
NIST. Special Publication 800-160, Volume 2: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, on line: https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final (dostęp 12.11.2025 r.
Orzecznictwo – zamówienia publiczne. „Wybrane Orzeczenia Krajowej Izby Odwoławczej i Sądów Okręgowych", nr 7 (2), Warszawa 2024.
Rynek zamówień publicznych. „Orzecznictwo Trybunału Sprawiedliwości dotyczące zamówień publicznych w II półroczu 2024 r.", online: https://www.gov.pl/web/uzp/orzecznictwo-tsue-w-ii-polroczu-2024-roku [dostęp: 12.11.2025].

Śledziewska, M. (red.), Adamiec, K., Jędrzejczyk, A., Matuszewska, A., Tarnowska, B. „Proces udzielania zamówień publicznych na podstawie nowego Prawa zamówień publicznych. Komentarz praktyczny z orzecznictwem", Wydawnictwo C.H. Beck, Warszawa, s. 289.
World Economic Forum. "Global Cybersecurity Outlook 2025. Insight Report", January 2025, s. 8, online: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ oraz PDF: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf s.12[dostęp: 12.11.2025].
Wskazówki w przedmiocie analizy potrzeb i wymagań, online: https://www.gov.pl/web/uzp/wskazowki-dla-zamawiajacych-publicznych-do-opracowania-analizy-potrzeb-i-wymagan [dostęp: 12.11.2025].