Operacjonalizacja NIS2. Uzasadnienie procesów i ich zależności

Opracowanie do dyskusji · 19 listopada 2026 r. · na podstawie wersji 0.1 bazy NIS2 i KSC

Po awarii można przywrócić serwer, zalogować się do aplikacji i nadal nie móc obsłużyć użytkownika. Na przykład jego ostatni wniosek zniknął wraz z danymi z ostatnich kilkudziesięciu minut. Administrator potrafi powiedzieć, którą kopię odtworzył. Dopiero właściciel usługi może ocenić, czy odzyskany stan pozwala wznowić pracę i co zrobić z brakującymi wnioskami. Ta różnica wyjaśnia, po co w bazie rozdzielono ciągłość usługi, odtwarzanie i ocenę skuteczności.

Przy każdym z 18 procesów rozpatrujemy trzy pytania. **Jaką decyzję ktoś musi podjąć? Jakiego faktu mu do tego brakuje? Kto poniesie konsekwencje, jeśli wynik nie dotrze na czas?** Odpowiedzi wyjaśniają rolę wszystkich 97 kroków. Przykłady odnoszą się do funkcji usługi i jej odbiorców, dzięki czemu ten sam model można stosować w różnych branżach.

Podział na 18 procesów jest propozycją organizacji pracy. Dwa zespoły mogą prowadzić jedną wspólną sprawę, a mały podmiot może połączyć kilka funkcji w jednej procedurze, o ile zachowa wymagane uprawnienia, niezależność tam, gdzie jest wymagana, i możliwość sprawdzenia wyniku. Jeśli czynność wykonuje dostawca, warto już przy uzgadnianiu współpracy ustalić, jak właściciel usługi uzyska dane potrzebne do własnej decyzji.

Nawigacja

Zakres obowiązku 2
Warstwy operacjonalizacji 3
Nadzór i ryzyko 4
Cykl życia usługi 5
Incydent i komunikacja 6
Próba odtworzenia 7
Indeks 18 procesów 8
Teksty źródłowe 27

Kiedy proces jest niezbędny

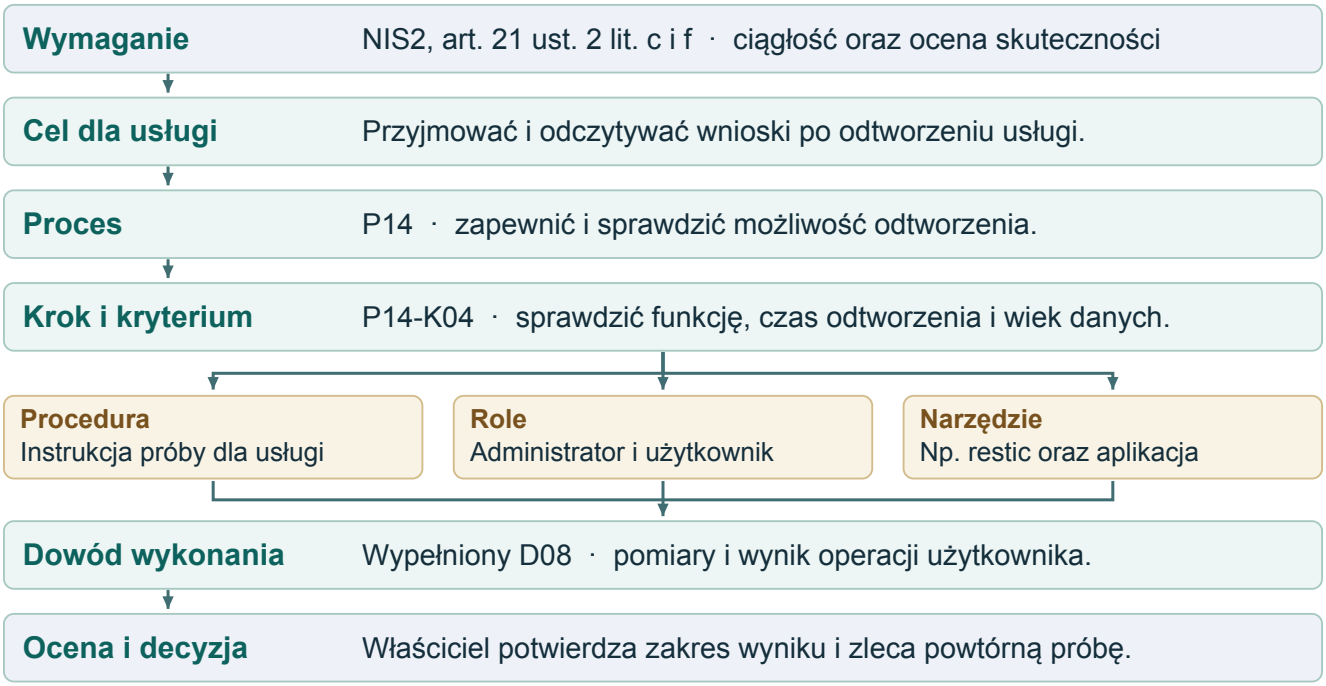
Z przepisu może wynikać konkretna czynność. Kierownictwo podmiotu objętego NIS2 ma zatwierdzać środki zarządzania ryzykiem i nadzorować ich wdrażanie. Można więc rozdzielić przygotowanie analizy i podjęcie decyzji. Właściciel ryzyka dostarcza warianty w P04, a organ zarządzający rozstrzyga je w P02. Przyjęty obieg dokumentów powinien pozwolić ustalić treść tej decyzji. NIS2, art. 20 ust. 1

Proces może być potrzebny do osiągnięcia wymaganego skutku. Art. 21 ust. 1–2 wiąże środki techniczne, operacyjne i organizacyjne z ryzykiem dla usług, ich użytkowników i innych usług. Wyznacza minimalny zakres tych środków. Organizacja dobiera sposób działania m.in. do narażenia, prawdopodobieństwa i dotkliwości incydentów. Jeśli jedno konto serwisowe obsługuje trzy usługi, P03 dostarcza tę informację P07 przed zmianą uprawnień. Przy prostszej usłudze wystarczy uzgodniony wykaz z właścicielem. W obu sytuacjach potrzebna jest wiedza o zależności. NIS2, art. 21 ust. 1–2

Niektóre kroki uruchamia dopiero przesłanka. Gotowość do klasyfikacji incydentu utrzymuje się wcześniej. Obowiązek zgłoszenia powstaje przy spełnieniu właściwych przesłanek. Podobnie procedura może przewidywać dostęp awaryjny, choć przez cały rok nikt z niego nie skorzysta. Można wówczas sprawdzić gotowość próbą i wskazać, czy w badanym okresie zaszło rzeczywiste zdarzenie. NIS2, art. 21 ust. 2 i art. 23

Polski profil ustala P01. NIS2 określa rezultaty, które mają zapewnić państwa członkowskie. Dla podmiotu działającego w Polsce trzeba ustalić właściwe przepisy KSC, reżim sektorowy i przepisy przejściowe. Przykładowo art. 8 ust. 3 KSC odsyła wskazane w nim podmioty do załącznika nr 4. Art. 4 NIS2 dotyczy równoważnych przepisów sektorowych UE, a rozporządzenie wykonawcze 2024/2690 doprecyzowuje wymagania i kryteria dla podmiotów wymienionych w jego art. 1. Wynik kwalifikacji wpływa na to, które kroki mają charakter obowiązkowy, kto jest adresatem zgłoszenia i jak ocenia się termin. NIS2, art. 2–4 · KSC, art. 8 i załącznik nr 4 · Rozporządzenie 2024/2690, art. 1–3

Warstwy operacjonalizacji



Wymaganie i cel. Wymaganie wyznacza adresata, warunki i obowiązek. Cel dla usługi przekłada go na stan, który można zaobserwować. W przykładzie celem jest wznowienie obsługi wniosków z dopuszczalnym ubytkiem danych. Docelowy czas i zakres utraty uzgadnia właściciel na podstawie wpływu przerwy, umów i właściwych przepisów.

Proces i krok. Proces zapewnia powtarzalny wynik i ma właściciela, np. sprawdzone odtworzenie. Krok służy jednej decyzji lub czynności. P14-K03 potwierdza wykonanie kopii, a P14-K04 sprawdza to, co można z niej odzyskać. Jeden wymóg angażuje tu P13, P14 i P16. Jeden krok P14-K04 dostarcza z kolei informacji zarówno o ciągłości, jak i o skuteczności środka.

Procedura, rola i narzędzie. Procedura mówi, jak wykonać krok w danej organizacji, jak postąpić z wyjątkiem i kto przejmuje sprawę. Rola wskazuje wykonawcę i osobę uprawnioną do decyzji. Narzędzie realizuje część czynności lub rejestruje jej przebieg. Administrator może użyć restic do odzyskania plików, a użytkownik testowy w aplikacji sprawdzić zapis i odczyt wniosku. Zmiana programu zwykle wymaga aktualizacji instrukcji i ponownej próby. Cel usługi może przy tym pozostać ten sam. Karta P14-K04 · Karta narzędzia restic

Dowód i ocena. Wzór D08 określa, co odnotować. Dowód powstaje po wykonaniu konkretnej próby. Łączy wersję kopii, pomiar, operację użytkownika i osobę potwierdzającą wynik. Dopiero odniesienie tych obserwacji do wcześniej zapisanego kryterium pozwala zdecydować o odbiorze lub korekcie. Wzór D08

Jak kierownictwo może ocenić skutek swojej decyzji

Strzałka na diagramach prowadzi od procesu wytwarzającego informację do procesu, który jej używa. Podpis określa przedmiot przekazania. Wiersze pokazują wybrane przepływy w tej samej organizacji. Ten sam proces może pojawić się kilkakrotnie, bo raz podejmuje decyzję, a innym razem dostarcza dane do jej sprawdzenia.



Kierownik może zatwierdzić utrzymywanie zastępstwa dyżurnego, ale treść decyzji jeszcze nie pokazuje, czy zastępca otrzyma alarm i będzie mógł działać. P02 zapewnia zasoby i uprawnienia. P15 wykorzystuje aktualną instrukcję w ćwiczeniu. P16 ustala na udokumentowanej próbie, czy zastępca przejął sprawę. Jeżeli zabrakło dostępu do listy kontaktów, właściciel P08 poprawia sposób jej udostępniania. P04 ocenia ryzyko do czasu potwierdzenia poprawki, a P02 rozstrzyga potrzebę dodatkowych zasobów.

Dwie oceny służą różnym decyzjom. **P04** odpowiada na pytanie, jakie są możliwe skutki i jak z nimi postąpić. **P16** bada, jaki wynik dał przyjęty środek w określonych warunkach. Gdy wynik przeczy założeniu, zmienia się podstawa wcześniejszej decyzji kierownictwa. Upływ terminu zaplanowanego przeglądu nie jest warunkiem podjęcia koniecznych działań naprawczych. NIS2, art. 20 ust. 1 i art. 21 ust. 2 lit. f oraz ust. 4

Co trzeba przekazać od zakupu do utrzymania usługi

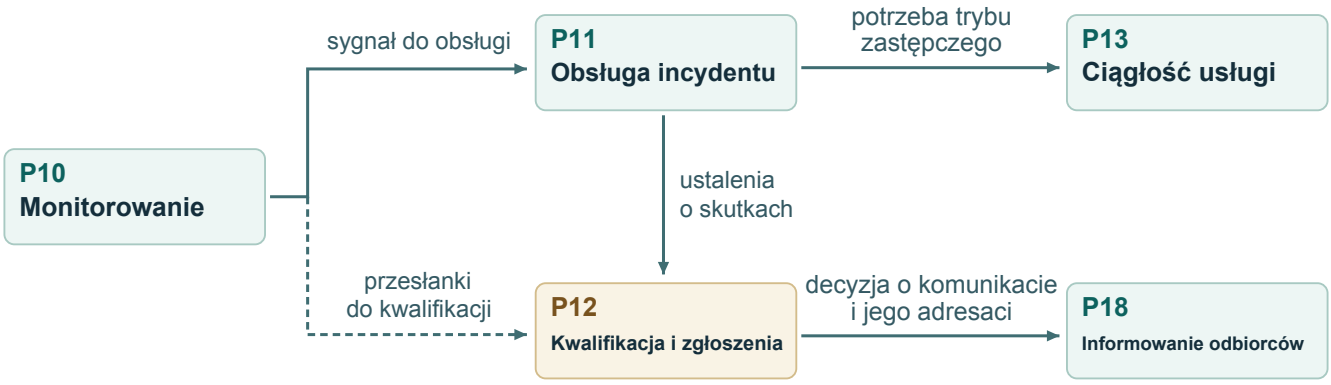


Warunki umowy i decyzja o odbiorze mają różnych adresatów. W P05 opiekun dostawcy uzgadnia, kto przekaże dane o awarii i na jaką pomoc można liczyć. W P06 właściciel projektu sprawdza, czy przekazywana wersja spełnia uzgodnione kryteria. Obietnica pomocy dostawcy jest ważna dla obydwu procesów. Dopiero próba odbiorowa pokazuje, czy przy danej konfiguracji odtworzenie rzeczywiście się uda. NIS2, art. 21 ust. 2 lit. c–e i ust. 3

Po odbiorze zmienia się odpowiedzialność za wersję. Zespół utrzymania korzysta z wersji i źródła wsparcia zapisanych w P03, żeby odnieść komunikat o podatności do własnej usługi. Po zmianie oddaje do ewidencji stan potwierdzony. Gdy poprawkę wdrożono tylko dla części zasobów, pozostałe nadal wymagają decyzji w P09. Dzięki temu kolejny komunikat można ocenić na podstawie rzeczywistych wersji.

Granica organizacji ma znaczenie także po zakupie. Zakończenie umowy uruchamia odebranie dostępu w P07. Jeżeli dostęp obejmował operacje kluczami, P08 rozstrzyga, które upoważnienia lub poświadczenia wymagają zmiany. Gdy usługę utrzymuje zewnętrzny gospodarz obiektu, P17 i P05 ustalają, kto odbierze alarm i przekaże go do P10. Wspólny identyfikator usługi pozwala dyżurnemu połączyć alarm z możliwym skutkiem dla odbiorcy.

Dlaczego reakcja i zgłoszenie biegną równolegle

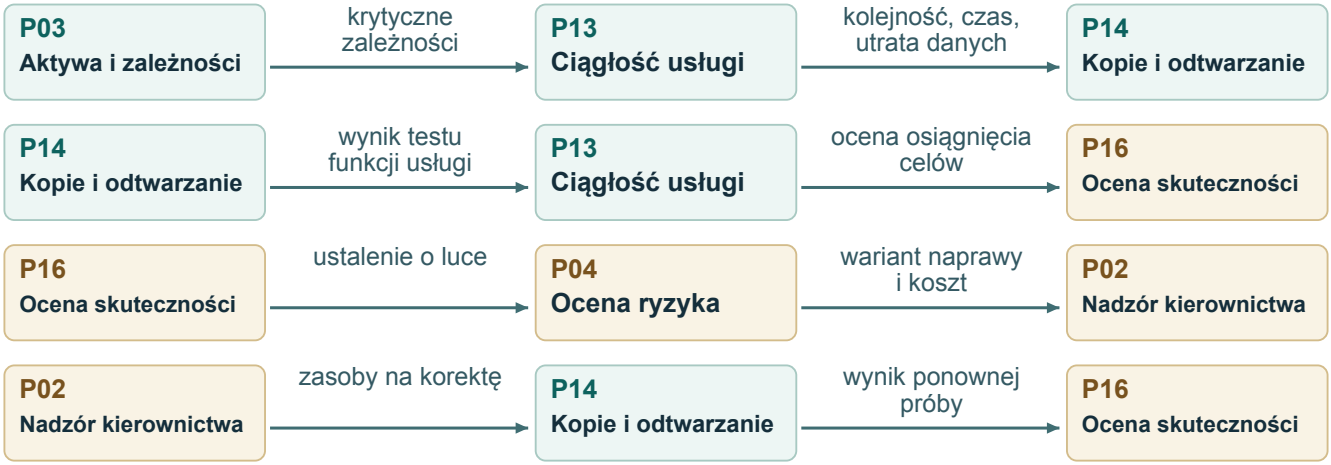


Przerywana strzałka pokazuje równoległe rozpoczęcie kwalifikacji, gdy sygnał daje podstawy do podejrzenia incydentu poważnego. Właściciel usługi w P11 ustala zakres niedostępnej funkcji, liczbę dotkniętych odbiorców i możliwe skutki. P12 stosuje właściwe przesłanki i terminy do aktualnie znanych faktów. Ustalenie przyczyny, przywrócenie usługi ani ukończenie raportu technicznego nie są warunkiem rozpoczęcia tej oceny. NIS2, art. 23 ust. 1 i 3–4 · KSC, art. 11–12c

Przykład. Zgłoszenia użytkowników wskazują, że nie otrzymują potwierdzenia przyjęcia sprawy. P10 potwierdza sygnał. P11 ustala, czy wnioski zapisują się mimo braku potwierdzenia. Różnica zmienia możliwe skutki i treść porady dla użytkowników. P12 od razu zapisuje znane fakty, źródła czasu i wynik klasyfikacji, a potem aktualizuje je po sprawdzeniu zapisów. Gdy przesłanki zgłoszenia są spełnione, osoba upoważniona działa w terminie właściwym dla profilu. Gdy danych brakuje, wskazuje, co i kiedy trzeba sprawdzić ponownie. Wzór wspólnej osi czasu D07

Jedna sprawa, odrębni odbiorcy. P18 potrzebuje od P11 informacji, czy użytkownik ma ponowić wniosek i czym grozi jego powtórzenie. P12 ustala podstawę i adresata wymaganej komunikacji. Potwierdzenie wysyłki do właściwego CSIRT i treść wiadomości do użytkowników to dwa odrębne zapisy. P18 może ruszyć również przy samym poważnym cyberzagrożeniu, gdy odbiorcy mogą zastosować środki ochronne. P13 uruchamia się, jeśli trzeba zapewnić pracę zastępczą. NIS2, art. 21 ust. 2 lit. b–c i art. 23 ust. 1–2

Jak wynik próby zmienia decyzję o ryzyku



W fikcyjnym przykładzie z D08 usługa powinna ponownie przyjmować i odczytywać wnioski w ciągu **120 minut**. Dopuszczalna utrata danych wyrażona w czasie to **15 minut**. W próbie operacja użytkownika udała się po **84 minutach**, lecz najnowszy odzyskany stan danych był starszy o **37 minut**. Pierwszy cel osiągnięto z zapasem 36 minut. Drugi przekroczono o 22 minuty. Są to parametry tej usługi. Wzór D08 z przykładem

Skutek dla decyzji. P14-K04 dostarcza wynik techniczny i wynik funkcji użytkownika. P13-K02 pozwala właścicielowi ocenić je względem dwóch wcześniej ustalonych celów. Przy rzeczywistym wznowieniu P11 potrzebowałby jeszcze decyzji o brakujących wnioskach. W próbie właściciel zleca sprawdzenie harmonogramu kopii i powtórzenie scenariusza. P16-K06 weryfikuje nowy wynik, a P04-K05 ponownie ocenia ryzyko. Jeśli korekta wymaga zakupu lub zmiany umowy, decyzja wraca odpowiednio do P02 lub P05. Karta próby P14-K04

Granica wniosku. Zaobserwowane 84 minuty dotyczą badanej funkcji i konfiguracji. Nieudany pomiar wieku danych uzasadnia konkretną naprawę. Inne usługi, awaria całej lokalizacji lub niedostępność dostawcy mogą wymagać oddzielnych prób. Właśnie dlatego dowód powinien identyfikować zakres, wersję, ocenione kryteria i ograniczenia pomiaru. Metryka dowodu D01

Indeks procesów

Każdy identyfikator kroku prowadzi w wersji Markdown do jego karty w bazie 0.1. Karta wskazuje pełną czynność, role, narzędzia i wzór dowodu. W opracowaniu ten sam identyfikator prowadzi czytelnika przez uzasadnienie i konsekwencje danego kroku.

P01	Kwalifikacja podmiotu, rejestracja i aktualizacja danych	9
P02	Nadzór kierownictwa, system zarządzania i dokumentacja	10
P03	Ewidencja aktywów, zależności i krytyczności	11
P04	Ocena ryzyka i postępowanie z ryzykiem	12
P05	Bezpieczeństwo i ciągłość łańcucha dostaw	13
P06	Bezpieczne nabywanie, rozwój i odbiór rozwiązania	14
P07	Zarządzanie tożsamościami i dostępem	15
P08	Zarządzanie kryptografią i bezpieczną łącznością	16
P09	Obsługa podatności, aktualizacji i zmian konfiguracji	17
P10	Monitorowanie i kwalifikacja zdarzeń	18
P11	Obsługa incydentu i przywrócenie usługi	19
P12	Kwalifikacja prawna, zgłaszanie i informowanie użytkowników	20
P13	Analiza wpływu, ciągłość usługi i zarządzanie kryzysowe	21
P14	Wykonywanie kopii i weryfikacja odtworzenia	22
P15	Rozwój kompetencji i cyberhigiena	23
P16	Ocena skuteczności, audyt i działania naprawcze	24
P17	Ochrona fizyczna i środowiskowa	25
P18	Informowanie użytkowników i współpraca przy cyberzagrożeniach	26

P01

Kwalifikacja podmiotu, rejestracja i aktualizacja danych

Przy grupie spółek jedna spółka może prowadzić działalność objętą regulacją, a inna dostarczać jej infrastrukturę. Ustalenie, kto świadczy usługę, przesądza o tym, kto podejmuje decyzje, dokonuje wpisu i zgłasza incydent. Art. 2–4 NIS2 i załączniki I–II wyznaczają zakres, kategorie podmiotów oraz relację do szczególnych regulacji UE. Art. 26 rozstrzyga właściwość państwa. Art. 3 ust. 3–4 rozdziela prowadzenie wykazu przez państwo i przekazywanie danych przez podmioty. Art. 27 ustanawia odrębny rejestr dla wymienionych w nim rodzajów podmiotów. Kwalifikację dla Polski, tryb wpisu i korzystanie z systemu S46 trzeba ustalić na podstawie KSC. NIS2 · KSC, art. 5–5a, 7–7m, 9 i 46

P01-K01 **Rozpoznanie działalności.** Opis działalności, odbiorców, wielkości i terytorium daje osobie oceniającej fakty, które może zestawić z definicją ustawową. Weryfikacja z właścicielem usługi wychwytuje działalność pominiętą w dokumentach rejestrowych.

P01-K02 **Decyzja o stosowalności.** Datowana decyzja o statusie wskazuje początek obowiązków, przepisy szczególne i właściwy organ. Zespół zgłoszeniowy może jej użyć także wtedy, gdy jedna organizacja prowadzi kilka rodzajów działalności.

P01-K03 **Wpis lub uzupełnienie danych.** Rozpoznanie, czy potrzebny jest wniosek, czy uzupełnienie danych po wpisie z urzędu, prowadzi do właściwej czynności. Potwierdzenie złożenia lub zawiadomienie pozwala sprawdzić, które działalności faktycznie ujęto.

P01-K04 **Kontakt i dostęp do S46.** Wyznaczenie kontaktu i sprawdzenie dostępu do S46 pokazuje, kto może odebrać korespondencję lub przekazać zgłoszenie. Pozwala ujawnić problem z uprawnieniami jeszcze przed incydentem.

P01-K05 **Aktualizacja wpisu.** Zapis daty zmiany pozwala obliczyć właściwy termin aktualizacji. Ponowna ocena po przejęciu, zmianie usługi lub zakończeniu działalności pozwala odpowiednio skorygować wpis i zakres nadzoru.

Przekazanie wyniku. Kierownictwo w P02 otrzymuje decyzję o stosowalności i terminach, właściciele usług w P03 granice ocenionej działalności, a zespół P12 właściwego adresata i sprawdzoną drogę kontaktu. Nowa usługa ujawniona w P03 może uruchomić ponowną kwalifikację w P01.

P02

Nadzór kierownictwa, system zarządzania i dokumentacja

Jeżeli próba odtworzenia wykazuje przerwę dłuższą niż dopuszcza właściciel usługi, administrator może opisać problem. Ktoś uprawniony musi jednak zdecydować o środkach, zasobach i terminie oraz sprawdzić wynik. Art. 20 ust. 1 NIS2 przypisuje zatwierdzanie środków i nadzór nad wdrażaniem organowi zarządzającemu, a ust. 2 przewiduje szkolenie jego członków. P02 organizuje obie funkcje. Sposób prowadzenia przeglądów można dopasować do organizacji. Polska ustawa określa m.in. odpowiedzialność kierownika, zasady dokumentacji i coroczne szkolenie wskazanych osób. NIS2, art. 20 i art. 21 ust. 2 lit. f oraz ust. 4 · KSC, art. 8c–8e i art. 10

P02-K01	**Zakres zarządzania i upoważnienia.** Określenie zakresu systemu zarządzania bezpieczeństwem informacji i granic upoważnień pozwala wskazać osobę uprawnioną do decyzji, także gdy zadanie wykonuje dostawca.
P02-K02	**Zatwierdzenie środków.** Decyzja kierownictwa wiąże scenariusz ryzyka z zatwierdzonym środkiem, zasobami i terminem. Dzięki temu właściciel usługi wie, co wdrożyć, a przełożony może zareagować na opóźnienie.
P02-K03	**Nadzór nad dokumentacją.** Kontrola wersji umożliwia wykonawcy odnalezienie obowiązującej instrukcji, a osobie oceniającej odtworzenie reguł z dnia zdarzenia. Chroni to przed rozliczaniem historycznego działania według późniejszej procedury.
P02-K04	**Szkolenie kierownictwa.** Szkolenie przygotowuje decydenta do oceny skutków ryzyka dla usług. W P15 można zorganizować szkolenie i zachować jeden wspólny zapis uczestnictwa, którym kierownik rozliczy obowiązek z art. 8e KSC.
P02-K05	**Przegląd decyzji.** Zestawienie dowodu skuteczności z wcześniejszą decyzją pozwala utrzymać środek, zmienić go albo nadać sprawie wyższy priorytet. Przegląd obejmuje również wcześniejsze decyzje, których nikt jeszcze nie wykonał.

Przekazanie wyniku. P04 przekazuje warianty postępowania i opis skutków, a P16 ustalenia oparte na próbach. P02 zwraca właścicielom decyzje, zasoby i warunki odbioru. P16 może później sprawdzić, czy usunięto przyczynę problemu wskazanego kierownictwu.

P03

Ewidencja aktywów, zależności i krytyczności

Dwie usługi mogą wyglądać na niezależne, a korzystać z tego samego mechanizmu uwierzytelniania. Dopiero powiązanie zasobu z usługami ujawnia łączny skutek jego awarii. Zarządzanie aktywami wynika wprost z art. 21 ust. 2 lit. i NIS2. Wiedza o zależnościach pozwala dodatkowo dobrać proporcjonalne środki i zaplanować ciągłość zgodnie z ust. 1 i ust. 2 lit. c. Postać ewidencji i skala krytyczności to wybory organizacji. W ogólnym profilu KSC zarządzanie aktywami i zawartość dokumentacji mają także krajową podstawę. NIS2, art. 21 · KSC, art. 8 ust. 1 pkt 2 lit. m i art. 10 ust. 3

P03-K01 **Usługa i jej właściciel.** Opis tego, czego odbiorca oczekuje od usługi, wyznacza granicę analizy. Właściciel usługi może wskazać, kiedy usterka pojedynczego zasobu staje się odczuwalnym zakłóceniem.

P03-K02 **Uzgodnienie ewidencji.** Porównanie danych od opiekunów, zakupów i administratorów ujawnia zasoby pominięte lub wykazane pod dwiema nazwami. Wspólny identyfikator pozwala później ustalić, których instalacji dotyczy komunikat o podatności.

P03-K03 **Mapa zależności.** Ustalenie, które zasoby, informacje, lokalizacje i dostawcy wspierają usługę, pozwala przejść od uszkodzonego elementu do dotkniętych odbiorców, a od usługi do warunków jej odtworzenia.

P03-K04 **Uzasadnienie krytyczności.** Właściciel uzasadnia krytyczność zasobu skutkiem dla usługi i zmianą tego skutku w czasie. W ten sposób planista ciągłości otrzymuje przesłankę do ustalenia kolejności odtwarzania.

P03-K05 **Aktualizacja stanu.** Porównanie ewidencji z wykonanymi zmianami i rzeczywistym stanem wykrywa przestarzałe zależności. Po wycofaniu zasobu opiekun potwierdza, kto lub co przejęło jego funkcję.

> **Przekazanie wyniku.** Mapa zależności daje P04 materiał do scenariuszy, P05 listę dostawców wpływających na usługę, P13 podstawę analizy wpływu, a P11 sposób ustalenia zasięgu zdarzenia. Przyjęcie nowej wersji w P06 lub wdrożenie zmiany w P09 powinno wrócić do P03 jako aktualizacja konkretnego rekordu.

P04

Ocena ryzyka i postępowanie z ryzykiem

Jeżeli ten sam zasób wspiera dwie usługi, awaria może powodować skutki o różnej wadze dla ich odbiorców. P04 pozwala zdecydować, gdzie zabezpieczenie jest pilniejsze, i uzasadnić tę decyzję. Art. 21 ust. 1 NIS2 wiąże dobór środków m.in. z narażeniem, prawdopodobieństwem, dotkliwością oraz kosztami wdrożenia. Ust. 2 lit. a i f obejmuje analizę ryzyka i ocenę skuteczności. Metoda porównywania scenariuszy może być prosta, o ile daje podstawę do decyzji. Kierownictwo może zaakceptować ryzyko pozostałe po wdrożeniu środka w granicach obowiązującego prawa. Stwierdzona niezgodność wymaga odpowiednich działań naprawczych bez zbędnej zwłoki zgodnie z ust. 4. NIS2, art. 21 · KSC, art. 8 ust. 1 pkt 1–2 i art. 8d

P04-K01 **Kryteria i uprawnienia decyzyjne.** Wspólne kryteria oceny i progi upoważnień pozwalają dwóm zespołom porównać podobne ryzyko oraz skierować sprawę do osoby uprawnionej do decyzji.

P04-K02 **Scenariusze zagrożeń.** Scenariusz łączy przyczynę z zależnością i skutkiem dla odbiorcy. Uwzględnienie awarii, błędu, incydentu u dostawcy czy utraty lokalizacji ujawnia działania, które zespół może rzeczywiście podjąć.

P04-K03 **Ocena przy istniejących środkach.** Uwzględnienie obecnych zabezpieczeń i jakości danych uzasadnia priorytet działania. Przy istotnej niepewności właściciel może najpierw zlecić próbę lub ustalenie brakującego faktu.

P04-K04 **Wybór postępowania.** Porównanie wariantów pokazuje kierownictwu koszt, spodziewaną poprawę i skutki uboczne. Wybrany wariant staje się zadaniem z wykonawcą, datą i warunkiem odbioru.

P04-K05 **Weryfikacja po wdrożeniu.** Próba po wdrożeniu dostarcza podstawy do ponownej oceny. Jeśli wynik rozmija się z założeniem, właściciel utrzymuje sprawę otwartą i przedstawia kolejną decyzję.

Przekazanie wyniku. P03 dostarcza mapę, P05 fakty o dostawcy, a P11 i P16 obserwacje z incydentów i prób. P04 przekazuje P02 propozycje wymagające decyzji, P05 warunki do uzgodnienia z dostawcą, a P06 kryteria dla konkretnej dostawy.

P05

Bezpieczeństwo i ciągłość łańcucha dostaw

Jeżeli dostawca jako pierwszy widzi zakłócenie, odbiorca może dowiedzieć się o zagrożeniu dopiero po przerwie w świadczeniu usługi. Żeby móc zareagować, musi znać tę zależność i mieć uzgodniony sposób wymiany informacji. Art. 21 ust. 2 lit. d i ust. 3 NIS2 obejmuje bezpieczeństwo relacji z bezpośrednimi dostawcami, właściwe im podatności, jakość produktów i praktyk oraz uwzględnienie wyników unijnych ocen określonych w art. 22 ust. 1. Znaczenie dostawy dla usługi uzasadnia głębokość oceny i dobór warunków współpracy. W Polsce uwzględnia się również wyniki właściwych postępowań z art. 67b KSC dotyczących uznania dostawcy za dostawcę wysokiego ryzyka. NIS2, art. 21–22 · KSC, art. 8 ust. 1 pkt 2 lit. e i ust. 2

P05-K01	**Zależność od dostawcy.** Rozpoznanie dostępu, możliwości zastąpienia dostawcy i skupienia kilku usług u jednej firmy pozwala wybrać relacje, których awaria dotknie najwięcej odbiorców.
P05-K02	**Ocena dostawcy.** Ocena dostawcy odniesiona do konkretnej dostawy wskazuje, które jego praktyki i słabości wpłyną na bezpieczeństwo usługi. Brak danych określa granice tego, co można uzasadnić przed zawarciem umowy.
P05-K03	**Uzgodnienie warunków.** Umowa zamienia rozpoznaną zależność w wykonalne uzgodnienie, np. wskazuje, kto po stronie dostawcy i w jakim terminie przekaże fakty potrzebne do oceny incydentu.
P05-K04	**Przegląd wykonania umowy.** Porównanie uzgodnionego czasu powiadomienia z rzeczywistą osią czasu zdarzenia pozwala stwierdzić, czy ustalenie działa. Wynik uzasadnia korektę, ponowną ocenę lub zmianę warunków przy odnowieniu.
P05-K05	**Zakończenie współpracy.** Przy zakończeniu współpracy odbiór użytecznych danych, potwierdzenie przejęcia funkcji i cofnięcie dostępu zmniejszają ryzyko przerwy w usłudze oraz dalszego dostępu byłego wykonawcy.

Przekazanie wyniku. P03 wskazuje zależność, a P04 jej wpływ. Uzgodnienia P05 dają P06 warunki odbioru konkretnego rozwiązania i P11 kontakt do dostawcy. Zakończenie umowy uruchamia cofnięcie dostępów w P07 oraz aktualizację zależności w P03.

P06

Bezpieczne nabywanie, rozwój i odbiór rozwiązania

Sprawdzony dostawca może przekazać wydanie, którego organizacja nie potrafi przywrócić po awarii. Rozwój własny niesie podobne ryzyko, nawet gdy nie występuje zewnętrzny dostawca. W obu przypadkach art. 21 ust. 2 lit. e NIS2 wymaga uwzględnienia bezpieczeństwa przy nabywaniu, rozwijaniu i utrzymywaniu systemów, łącznie z obsługą i ujawnianiem podatności. P06 rozstrzyga, czy konkretne rozwiązanie można przyjąć do eksploatacji i na jakich warunkach. Zakres prób oraz potrzeba pozyskania wykazu składników oprogramowania (SBOM) zależą od ryzyka, rodzaju dostawy i przepisów właściwych dla podmiotu. NIS2, art. 21 ust. 2 lit. d–f · KSC, art. 8 ust. 1 pkt 2 lit. b i h oraz pkt 5 lit. b

P06-K01	**Kryteria odbioru.** Ustalenie przed zamówieniem, jak sprawdzić istotne wymaganie i kto oceni wynik, umożliwia rozstrzygnięcie odbioru. Przykładowo warunek przywrócenia usługi wymaga uzgodnienia zakresu i kryterium udanej próby.
P06-K02	**Wybór rozwiązania.** Ocena źródła dostawy, wsparcia i sposobu aktualizacji przed wyborem rozwiązania ujawnia koszty lub ograniczenia, które po zawarciu umowy trudno będzie usunąć. Przy rozwoju własnym tę rolę pełni przegląd projektu i zasad wydawania zmian.
P06-K03	**Wersja i pochodzenie.** Przypisanie pochodzenia i dostępnych dowodów do wydania pozwala ustalić, co faktycznie przyjęto. Dla usługi zewnętrznej zakres i data potwierdzenia od dostawcy wskazują, do czego można odnieść jego oświadczenie.
P06-K04	**Sprawdzenie dostawy.** Wynik sprawdzenia każdego istotnego kryterium dotyczy konkretnej wersji. Ujawnienie punktu bez wyniku pozwala właścicielowi odroczyć odbiór lub rozważyć ograniczony zakres użycia.
P06-K05	**Decyzja o dopuszczeniu.** Decyzja o dopuszczeniu i przekazanie wiedzy osobie utrzymującej rozwiązanie zapewniają ciągłość odpowiedzialności. Opiekun dowiaduje się, jak przyjąć zgłoszenie o wadzie i które odstępstwa wymagają ponownej próby.

Przekazanie wyniku. P06 przejmuje kryteria ryzyka z P04 i warunki dostawy z P05. Po dopuszczeniu wersja trafia do ewidencji P03, warunki wsparcia i obsługi wad do P09, a ustalenia z odbioru do następnej oceny dostawcy w P05.

P07

Zarządzanie tożsamościami i dostępem

Pracownik zmienia stanowisko, umowa serwisowa wygasa, a konto techniczne nadal działa. W każdym przypadku zmienia się podstawa dostępu, chociaż system może poprawnie potwierdzić tożsamość użytkownika. Dlatego właściciel usługi musi umieć rozstrzygnąć trzy pytania. Kto nadal potrzebuje dostępu? Do jakich czynności? Kto potwierdzi, że system wykonał decyzję? Art. 21 ust. 2 lit. i NIS2 obejmuje bezpieczeństwo personelu i politykę kontroli dostępu. Lit. j przewiduje w stosownych przypadkach uwierzytelnianie wieloskładnikowe lub ciągłe. Macierz ról i czasowy dostęp administracyjny są sposobami wykonania tych zadań. NIS2, art. 21

P07-K01 **Role i konflikty uprawnień.** Właściciel opisuje dozwolone czynności i konflikty uprawnień. Dzięki temu zatwierdzający potrafi rozpoznać wniosek pozwalający jednej osobie zarówno zlecić, jak i zatwierdzić operację.

P07-K02 **Dopuszczenie do określonych zadań.** Przed dopuszczeniem do zadań z art. 8 lub 11 KSC sprawdza się informację z Krajowego Rejestru Karnego o niekaralności za przestępstwa przeciwko ochronie informacji. Ustawa uznaje także ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji o klauzuli „poufne” lub wyższej. Uzasadnione podejrzenie skazania uruchamia ponowne wezwanie do przedstawienia informacji. Do dalszego obiegu operacyjnego wystarcza decyzja o dopuszczeniu i odsyłacz do chronionej dokumentacji. KSC, art. 8f

P07-K03 **Nadanie dostępu.** Zgoda właściciela wiąże zweryfikowaną osobę lub konto techniczne z zadaniem, zakresem i czasem dostępu. Administrator porównuje nadane prawa z decyzją i sprawdza wymagany mechanizm uwierzytelniania.

P07-K04 **Dostęp uprzywilejowany i awaryjny.** Czasowe nadanie uprawnień podwyższonych ogranicza okres, w którym można zmienić ustawienia całej usługi. Zapis użycia awaryjnego pozwala później ustalić, kto działał, dlaczego i kiedy zakończył pracę.

P07-K05 **Cofnięcie dostępu.** Zmiana funkcji lub odejście uruchamia cofnięcie uprawnień także poza głównym katalogiem kont. Sprawdzenie sesji, poświadczeń i właścicieli kont usługowych pozwala usunąć dostęp byłej osoby i zachować działanie samej usługi.

P07-K06 **Przegląd uprawnień.** Porównanie stanu rzeczywistego z aktualnymi obowiązkami ujawnia pominięte cofnięcia i uprawnienia nadane poza zwykłym obiegiem. Właściciel może zamknąć rozbieżność po sprawdzeniu korekty w systemie.

Przekazanie wyniku. P05 przekazuje warunki i datę zakończenia dostępu dostawcy. P07 zwraca do P05 potwierdzenie cofnięcia konta, które pozwala zamknąć współpracę. Ślady nieuprawnionego użycia trafiają do P11 wraz z informacją, czyj dostęp był dopuszczony w chwili zdarzenia.

P08

Zarządzanie kryptografią i bezpieczną łącznością

Usługa może stać się niedostępna mimo nienaruszonych danych, gdy wygaśnie używany przez nią certyfikat. Podczas awarii poczty dyżurni mogą utracić jednocześnie podstawowy kanał kontaktu i możliwość zalogowania się do kanału zapasowego. P08 łączy dwa zadania mające wspólną zależność od zaufanych poświadczeń. Art. 21 ust. 2 lit. h NIS2 wymaga polityk i procedur stosowania kryptografii oraz, w stosownych przypadkach, szyfrowania. Lit. j obejmuje bezpieczną komunikację i łączność wewnętrzną w sytuacjach nadzwyczajnych stosownie do okoliczności. Zakres rejestru kluczy i rozwiązanie łączności zależą od tego, co organizacja chroni i jaki rodzaj awarii musi przetrwać. NIS2, art. 21

P08-K01 **Zasady stosowania kryptografii.** Określenie, które dane i operacje wymagają ochrony kryptograficznej, pozwala projektantowi uzasadnić wybór zabezpieczenia, a właścicielowi ocenić skutki odstępstwa.

P08-K02 **Metadane i właściciele kluczy.** Powiązanie metadanych klucza lub certyfikatu z usługą, właścicielem i terminem pozwala wskazać, kto ma prawo odnowić poświadczenie i komu grozi przerwa. Rejestr można prowadzić bez ujawniania wartości kluczy prywatnych.

P08-K03 **Wymiana i unieważnienie.** Test po wydaniu, wymianie lub unieważnieniu pokazuje, czy usługa korzysta z właściwego poświadczenia. Sam zapis udanej operacji u wystawcy może współistnieć ze starą konfiguracją u odbiorcy.

P08-K04 **Kanał awaryjny.** Dobór kanału awaryjnego obejmuje sprawdzenie zależności od poczty, tożsamości i urządzeń oraz sposobu rozpoznania rozmówcy. W ten sposób koordynator może wydać wiarygodne polecenie po utracie typowej drogi kontaktu.

P08-K05 **Próba utraty łączności.** Próba kontaktu i wymiany poświadczenia ujawnia zależności przeoczone w projekcie, np. listę numerów dostępną wyłącznie po zalogowaniu do niedziałającej usługi.

Przekazanie wyniku. Właściciele i zakresy uprawnień z P07 wyznaczają osoby upoważnione do operacji kluczami. Zaplanowana wymiana może przejść przez P09. Sprawdzony kanał i lista dyżurnych służą P11 przy podejrzeniu kompromitacji podstawowego kanału oraz P13 przy zakłóceniu ciągłości.

P09

Obsługa podatności, aktualizacji i zmian konfiguracji

Komunikat o podatności staje się podstawą decyzji dopiero wtedy, gdy wiadomo, która usługa używa danego składnika, jakie są warunki narażenia i jaki wpływ będzie miała zmiana. Art. 21 ust. 2 lit. e NIS2 wiąże bezpieczeństwo utrzymania z postępowaniem z podatnościami i ich ujawnianiem. Ust. 1 uzasadnia dobór działań do ryzyka, a ust. 2 lit. f potrzebę sprawdzenia skuteczności naprawy. Rejestr zmian, sposób ustalania pilności i dobór próby technicznej są decyzjami wdrożeniowymi. NIS2, art. 21

P09-K01	**Wersje, wsparcie i odpowiedzialność.** Wskazanie usług korzystających z danej wersji oraz źródła aktualizacji wyznacza zakres sprawdzenia i osobę odpowiedzialną za zmianę.
P09-K02	**Ocena informacji o podatności.** Analityk konfrontuje komunikat z ewidencją wersji i warunkami użycia. Może ustalić zakres narażenia lub wskazać konkretną niewiadomą do wyjaśnienia ze zgłaszającym.
P09-K03	**Priorytet naprawy.** Właściciel porównuje przewidywaną szkodę ze zwłoki ze skutkami przerwy na zmianę. Gdy poprawki brak, wskazuje tymczasową ochronę i termin ponownej decyzji.
P09-K04	**Przygotowanie zmiany.** Sprawdzenie pochodzenia poprawki oraz uzgodnienie testu, okna zmiany i warunku wycofania umożliwiają podjęcie decyzji także wtedy, gdy działanie okaże się szkodliwe dla usługi.
P09-K05	**Wdrożenie i test.** Wynik wdrożenia dla każdego objętego składnika oraz test funkcji usługi rozstrzygają, czy utrzymać zmianę, wycofać ją, czy objąć część zasobów kolejną próbą.
P09-K06	**Potwierdzenie zamknięcia.** Ponowne odczytanie stanu końcowego pozwala zamknąć sprawę na podstawie obserwacji. W szczególnym krajowym trybie wezwania do usunięcia podatności informacja o usunięciu wraca również do właściwego organu. KSC, art. 11 ust. 1 pkt 6 i art. 32 ust. 2

Przekazanie wyniku. P03 dostarcza wykaz zasobów i otrzymuje wynik potwierdzający nowe wersje. Ryzyko pozostałe przy odroczeniu naprawy trafia do P04. Jeżeli pojawiają się ślady wykorzystania podatności, P11 otrzymuje ich opis jeszcze w czasie prac nad zmianą.

P10

Monitorowanie i kwalifikacja zdarzeń

Brak alarmu można zinterpretować dopiero wtedy, gdy wiadomo, co podlega obserwacji, czy napływają dane i kto odbierze sygnał. W NIS2 wykrywanie oraz analiza należą do obsługi incydentu (art. 6 pkt 8 i art. 21 ust. 2 lit. b). W powiązaniu z oceną skuteczności z lit. f uzasadnia to sprawdzenie całej drogi od zdarzenia do dyżurnego. W polskim profilu ogólnym art. 8 ust. 1 pkt 2 lit. g KSC wprost przewiduje monitorowanie w trybie ciągłym systemu informacyjnego służącego do świadczenia usługi. Dla profilu z art. 8 ust. 3 zakres środków wynika z załącznika nr 4. NIS2, art. 6 i 21 · KSC, art. 8 i załącznik nr 4

P10-K01 **Zakres obserwacji.** Zestawienie scenariuszy ryzyka ze źródłami informacji pokazuje, które zakłócenia może zauważyć dyżurny i gdzie pozostaje luka wymagająca decyzji.

P10-K02 **Ciągłość napływu danych.** Kontrola czasu zdarzeń i ciągłości napływu danych pozwala odróżnić spokojny okres od awarii obserwacji. Określenie retencji i praw dostępu wyznacza, kto i jak długo może później analizować materiał.

P10-K03 **Sprawdzenie reguł.** Test na danych o znanym przebiegu sprawdza, czy reguła dostarczy osobie dyżurnej użytecznej informacji. Zapis wersji reguły wyjaśnia, dlaczego to samo zdarzenie mogło zostać ocenione inaczej przed zmianą.

P10-K04 **Wstępna ocena sygnału.** Uzgodnienie czasu, źródła i możliwego wpływu łączy powielone alarmy w jedną sprawę. Analityk wskazuje odbiorcy, które ustalenia mają potwierdzenie, a co trzeba jeszcze sprawdzić.

P10-K05 **Przekazanie sprawy.** Potwierdzenie przejęcia sprawy kończy przekazanie. Oddzielne czasy pierwszego sygnału, wykrycia i eskalacji pozwalają zbadać opóźnienie oraz ustalić początek właściwego terminu prawnego.

Przekazanie wyniku. P03 wskazuje zależności usługi, P04 scenariusze do obserwacji. P10 przekazuje podejrzenie z osią czasu do P11, a przy możliwym incydencie poważnym równolegle uruchamia kwalifikację w P12. Wykryta przerwa w monitorowaniu kieruje do P09 zadanie naprawcze, a do P04 informację, przez jaki czas i w jakim zakresie obserwacja była ograniczona.

P11

Obsługa incydentu i przywrócenie usługi

W trakcie incydentu decyzja chroniąca jeden składnik może przerwać inną potrzebną funkcję. Kto może ją podjąć, jakie skutki dopuszcza właściciel i po czym pozna bezpieczny powrót do pracy? Art. 21 ust. 2 lit. b NIS2 obejmuje obsługę incydentu, a lit. c łączy ją z ciągłością. Definicja z art. 6 pkt 8 sięga do przywrócenia normalnego działania. Koordynator i wspólna karta sprawy są sposobem uzgodnienia decyzji między ludźmi, którzy obserwują różne skutki tego samego zdarzenia. NIS2, art. 6 i 21

P11-K01 **Rozpoczęcie obsługi.** Wskazanie koordynatora i zastępstwa daje zgłaszającemu oraz zespołowi jedno miejsce na decyzje. Odrębne wpisanie czasu wystąpienia, jeśli jest znany, i wykrycia zachowuje chronologię przy zmianie dyżuru.

P11-K02 **Ocena wpływu na usługę.** Właściciel przekłada objawy techniczne na konsekwencje dla funkcji i odbiorców. Z tej samej datowanej oceny zespół wyprowadza priorytet reakcji, a P12 przesłanki do kwalifikacji prawnej.

P11-K03 **Zabezpieczenie materiału.** Utrwalenie materiałów przed ich utratą wraz z pochodzeniem i historią przekazania pozwala zweryfikować ustalenia oraz odpowiedzieć na właściwie umocowane pytanie CSIRT.

P11-K04 **Ograniczenie skutków.** Porównanie możliwych działań z potrzebami usługi pozwala wybrać sposób ograniczenia skutków, upoważnić wykonawcę i wskazać moment przejścia na tryb ciągłości.

P11-K05 **Przywrócenie funkcji.** Test uzgodnionej funkcji i decyzja właściciela określają warunki przywrócenia usługi. Wykaz ograniczeń i okres obserwacji pomagają wykryć nawrót problemu po wznowieniu pracy.

P11-K06 **Zakończenie obsługi.** Zapis daty zakończenia obsługi i uzgodnionych wniosków pozwala P12 ustalić odpowiedni termin raportu. Działania pozostające po przywróceniu usługi otrzymują wykonawcę i sposób sprawdzenia.

> **Przekazanie wyniku.** P11 korzysta z kanału awaryjnego P08, z planu ciągłości P13 i w razie potrzeby z odtworzenia w P14. Przekazuje do P12 kolejne wersje oceny wpływu podczas obsługi, do P09 potwierdzoną potrzebę zmiany, a do P04 dane o faktycznym rozmiarze szkody.

P12

Kwalifikacja prawna, zgłaszanie i informowanie użytkowników

Właściciel usługi podejmuje działania ratunkowe, nawet gdy zna jedynie część przyczyny. Ten sam brak pełnych ustaleń występuje przy pierwszym zgłoszeniu. Art. 23 ust. 1 i 3–4 NIS2 wiąże obowiązek zgłoszenia z poważnym incydentem i przewiduje kolejne przekazania w miarę przyrostu wiedzy. Ocena obejmuje również możliwe dotkliwe zakłócenie usług, straty finansowe podmiotu lub znaczne szkody dla innych osób, zgodnie z właściwą przesłanką. Z kolei ostrzeżenie użytkowników o środkach, które mogą sami zastosować, może być potrzebne już na etapie poważnego cyberzagrożenia (ust. 2). Dlatego organizacja potrzebuje dwóch niezależnych decyzji o adresacie i treści oraz jednej uzgodnionej chronologii. NIS2, art. 23

P12-K01 **Tryb, adresat i kanał.** Ustalenie z wyprzedzeniem właściwego trybu, progów, adresata i kanału daje dyżurnemu możliwość działania poza godzinami pracy. W Polsce trzeba uwzględnić przepisy przejściowe i stan gotowości właściwego CSIRT, a dla podmiotów objętych rozporządzeniem 2024/2690 także kryteria właściwe dla danej usługi. Nowela KSC, art. 32, 33 i 44 · Rozporządzenie wykonawcze 2024/2690

P12-K02 **Kwalifikacja i początek terminu.** Koordynator wiąże znane lub możliwe skutki z właściwymi przesłankami, zapisuje podstawę i wraca do oceny po nowych ustaleniach. Dla terminów NIS2 istotne jest powzięcie wiedzy o poważnym incydencie, a dla KSC wykrycie incydentu poważnego. Późniejsza akceptacja wewnętrzna nie rozpoczyna biegu terminu od nowa. NIS2, art. 23 ust. 3–4 · KSC, art. 11

P12-K03 **Wczesne ostrzeżenie.** Wczesne ostrzeżenie w trybie podstawowym daje CSIRT sygnał do działania jeszcze w trakcie oceny rozmiaru szkody. Wysyła się je niezwłocznie, najpóźniej w ciągu 24 godzin według właściwego początku terminu.

P12-K04 **Zgłoszenie incydentu.** Zgłoszenie dostarcza wstępnej oceny skutków. W trybie podstawowym należy je przekazać niezwłocznie, maksymalnie w ciągu 72 godzin od tego samego zdarzenia rozpoczynającego bieg terminu. NIS2 skraca ten limit do 24 godzin przy incydencie poważnym wpływającym na usługi zaufania. Dla polskiego dostawcy usług zaufania szczególny termin wynika z art. 11 ust. 1a KSC. NIS2, art. 23 ust. 4 · KSC, art. 11

P12-K05 **Aktualizacje w toku obsługi.** Kontrola wersji pozwala wskazać, które ustalenia zespołu zastąpiły wcześniejsze szacunki. Sprawozdanie okresowe składa się na wniosek. Odrębną czynnością pozostaje uzupełnianie danych zgłoszenia.

P12-K06 **Decyzja o informacji dla użytkowników.** Zgłoszenie do CSIRT i komunikat do użytkownika mają innych odbiorców i inne cele. KSC przewiduje informację o incydencie poważnym przy niekorzystnym wpływie na świadczenie usług. Przy poważnym cyberzagrożeniu narażeni użytkownicy powinni otrzymać wskazówki ochronne, a wiadomość o samym zagrożeniu przekazuje się, jeżeli nie zwiększy to ryzyka dla bezpieczeństwa systemów. P18 realizuje uzgodnioną wysyłkę. KSC, art. 11 ust. 2a–2b

P12-K07 **Sprawozdanie z postępu lub końcowe.** W trybie podstawowym termin sprawozdania końcowego wynosi miesiąc od zgłoszenia. Jeżeli obsługa nadal trwa, w tym terminie przekazuje się sprawozdanie z postępu, a końcowe w ciągu miesiąca od zakończenia obsługi. Daty z P11 pozwalają rozpoznać właściwy wariant. NIS2, art. 23 ust. 4 lit. d–e · KSC, art. 11 i 12b

> **Przekazanie wyniku.** P01 określa obowiązujący reżim prawny. Przykładowo art. 12c KSC zwalnia podmiot ważny będący podmiotem publicznym z wczesnego ostrzeżenia i trzech rodzajów sprawozdań, zachowując obowiązek samego zgłoszenia. P11 dostarcza skutki i chronologię, P18 otrzymuje decyzję i zakres komunikatu, a P16 może porównać moment wykrycia, właściwy termin i potwierdzenie wysyłki w wybranej sprawie. KSC, art. 12c

P13

Analiza wpływu, ciągłość usługi i zarządzanie kryzysowe

Gdy jednocześnie przestają działać dwie funkcje usługi, zespół techniczny może wiedzieć, jak przywrócić każdą z nich, a mimo to w pierwszej kolejności uruchomić mniej pilną. Właściciel usługi musi wcześniej rozpoznać, jak rosną skutki przerwy, co można przez pewien czas wykonywać zastępczo i kto podejmie decyzję w razie konfliktu priorytetów. Art. 21 ust. 2 lit. c NIS2 obejmuje ciągłość działania i zarządzanie kryzysowe. Proporcjonalność z ust. 1 pozwala dobrać szczegółowość planu do skutków przerwy. Cele RTO i RPO są sposobem wyrażenia tolerancji danej usługi. Właściciel uzgadnia wartości liczbowe dla ocenianej funkcji. NIS2, art. 21

P13-K01 **Skutki przerwy.** Analiza wpływu w kolejnych przedziałach czasu pokazuje, kiedy opóźnienie staje się niedopuszczalne i które osoby, dane lub usługi zewnętrzne będą wtedy potrzebne. To podstawa wyboru minimalnego poziomu obsługi.

P13-K02 **Cele odtworzenia.** Właściciel usługi uzgadnia kolejność wznowienia, docelowy czas odtworzenia (RTO) i dopuszczalną utratę danych wyrażoną w czasie (RPO). Jeżeli dostawca potrzebuje więcej czasu, różnicę trzeba rozstrzygnąć już przy wyborze strategii.

P13-K03 **Aktywacja i zastępstwo.** Przesłanki aktywacji, zastępstwo i instrukcja dostępna podczas awarii pozwalają dyżurnemu uruchomić pracę zastępczą także wtedy, gdy niedostępne są zwykłe narzędzia albo osoba kierująca.

P13-K04 **Próba planu lub uruchomienie.** Próba utraty konkretnej zależności ujawnia, jaki poziom obsługi zespół rzeczywiście utrzyma. Przy zdarzeniu rzeczywistym dziennik decyzji daje zespołowi incydentowemu czas i uzasadnienie przejścia na tryb zastępczy.

P13-K05 **Powrót i rozliczenie zaległości.** Uruchomienie systemu może pozostawić zaległe zlecenia lub rozbieżne dane. Właściciel przed powrotem uzgadnia sposób ich rozliczenia, sprawdza działanie usługi i zleca poprawę niesprawdzonych założeń planu.

Przekazanie wyniku. P03 dostarcza mapę zależności, P04 ocenę ryzyka, a P05 sprawdza możliwości dostawcy. P14 otrzymuje z P13 cele odtworzenia i oddaje wyniki próby. Podczas zakłócenia P11 i P13 mogą działać równolegle. Pierwszy ustala stan incydentu, drugi podtrzymuje obsługę użytkowników. P16 dostaje zapis ćwiczenia z osiągniętym poziomem usługi.

P14

Wykonywanie kopii i weryfikacja odtworzenia

Kopia może się zapisać poprawnie, choć brakuje klucza, konfiguracji lub zależnej bazy potrzebnej do otwarcia danych. Dlatego pytanie o wykonanie kopii i pytanie o odzyskanie funkcji usługi wymagają różnych dowodów. Art. 21 ust. 2 lit. c NIS2 wymienia zarządzanie kopiami i odtwarzanie jako przykłady działań zapewniających ciągłość, a lit. f wymaga procedur oceny skuteczności środków. Wybór technologii i zakres próby zależą od usługi. Przykładowo przy usłudze zewnętrznej znaczenie mają zapewnienia dostawcy oraz możliwość sprawdzenia, co użytkownik rzeczywiście odzyska. NIS2, art. 21

P14-K01 **Zakres kopii.** Planista wiąże cele P13 z konkretnymi danymi, konfiguracją, zależnościami i dostępem do kluczy. Tak powstaje wykaz elementów, których pominięcie uniemożliwiłoby odtworzenie usługi w potrzebnym stanie.

P14-K02 **Ochrona repozytorium.** Sposób przechowywania i ograniczenia dostępu mają zapewnić, że awaria źródła albo utrata zwykłego konta administratora pozostawi wykonalną drogę odzyskania. Sprawdzenie dostępu awaryjnego weryfikuje to założenie.

P14-K03 **Wykonanie i aktualność kopii.** Historia wykonania pozwala ustalić wiek ostatniej dostępnej kopii. Brak zadania lub narastające opóźnienie dają podstawę do interwencji, zanim luka w danych ujawni się podczas awarii.

P14-K04 **Próba odtworzenia.** Odtworzenie próbki i wykonanie uzgodnionej operacji użytkownika sprawdzają razem czas, punkt odzyskania i przydatność wyniku. Zakres próbki wyznacza granice wniosku o skuteczności.

P14-K05 **Korekta i powtórzenie próby.** Powtórzenie nieudanego scenariusza pozwala ocenić, czy poprawka usunęła przyczynę. W rzeczywistej awarii właściciel potrzebuje potwierdzonego punktu odzyskania i informacji o brakujących danych do decyzji o wznowieniu obsługi.

> **Przekazanie wyniku.** P13 podaje cele, P03 wykaz zależności, a P08 dostarcza ustalenia dotyczące kluczy. P14 przekazuje do P13 i P16 protokół z wynikiem operacji użytkownika. Jeżeli test ujawni pominięty komponent, P03 uzupełnia ewidencję, a P04 ponownie ocenia ryzyko przerwy.

P15

Rozwój kompetencji i cyberhigiena

Decyzję o ryzyku podejmuje kierownictwo, pierwsze oznaki zdarzenia może zaś dostrzec pracownik obsługujący użytkowników. Każdy potrzebuje umiejętności odpowiadających temu, co faktycznie ma zrobić. Art. 20 ust. 2 NIS2 przewiduje regularne szkolenia członków organu zarządzającego i zachęcanie do oferowania podobnych szkoleń pracownikom. Art. 21 ust. 2 lit. g włącza cyberhigienę i szkolenia do wymaganych środków. W Polsce art. 8e KSC określa osobno adresatów, zakres oraz udokumentowane szkolenie raz w roku kalendarzowym dla kierownika i osoby, której powierzono jego obowiązki w zakresie cyberbezpieczeństwa. Dobór ćwiczeń do ról jest decyzją organizacji. NIS2, art. 20–21 · KSC, art. 8e

P15-K01 **Zadania wymagające umiejętności.** Powiązanie ról z zadaniami pozwala dobrać właściwych uczestników i ustalić, po czym przełożony pozna gotowość do pracy. Przy zmianie stanowiska wiadomo, które umiejętności wymagają uzupełnienia.

P15-K02 **Szkolenie kierownictwa.** Scenariusz decyzji kierowniczej, na przykład wybór sposobu utrzymania usługi podczas awarii, pozwala przećwiczyć ocenę konsekwencji. Data, uczestnicy i zakres dokumentują realizację szkolenia osób objętych obowiązkiem.

P15-K03 **Praktyka personelu.** Personel przechodzi przez zadanie ze swojego stanowiska, na przykład zgłoszenie zaobserwowanego zdarzenia. W ten sposób poznaje właściwy kanał, potrzebne fakty i dalszy przebieg sprawy.

P15-K04 **Sprawdzenie umiejętności.** Samodzielne wykonanie zadania przez uczestnika pozwala rozpoznać konkretną trudność. Jeżeli kilka osób zatrzymuje się w tym samym miejscu, sprawdzenia może wymagać również instrukcja lub dostęp do kanału zgłoszeń.

P15-K05 **Uzupełnienie braków.** Właściciel usuwa ujawnioną przeszkodę, aktualizuje materiał i zleca ponowne wykonanie zadania. Kolejny wynik pozwala przełożonemu ustalić, czy uczestnik wykonuje już zadanie samodzielnie.

Przekazanie wyniku. P07, P11 i P18 dostarczają aktualne zasady dostępu, obsługi incydentu i komunikacji. Wyniki ćwiczeń wracają do właścicieli tych procedur. P02 wykorzystuje informacje o lukach do decyzji o zasobach lub zastępstwach, a P16 dobiera próbkę do oceny skuteczności szkolenia.

P16

Ocena skuteczności, audyt i działania naprawcze

Właściciel zabezpieczenia potrafi przedstawić jego konfigurację. Osoba oceniająca musi jeszcze ustalić, w jakich warunkach zabezpieczenie spełniło cel i jakiego zakresu dotyczy wniosek. Art. 21 ust. 2 lit. f NIS2 wymaga polityk i procedur oceny skuteczności. Ust. 4 wiąże stwierdzenie niespełnienia wymaganych środków z podjęciem odpowiednich działań naprawczych bez zbędnej zwłoki. Audyty w ramach nadzoru mają odrębną podstawę w art. 32–33 dyrektywy. W polskim modelu art. 15 KSC reguluje cykliczny audyt podmiotu kluczowego oraz audyt zewnętrzny nakazywany decyzją organu na ustawowych przesłankach. Profil podmiotu rozstrzyga, które z tych czynności stosuje się obok własnych testów. NIS2, art. 21 i 32–33 · KSC, art. 15

P16-K01 **Tryb i termin oceny.** Ustalenie rodzaju oceny i zdarzenia, od którego biegnie termin, pozwala zarezerwować właściwych wykonawców. Pomylenie przeglądu wewnętrznego z audytem ustawowym grozi uchybieniem terminowi pomimo wykonania pracy technicznej.

P16-K02 **Projekt próby.** Pytanie testowe, kryterium odbioru i sposób doboru przypadków ustala się przed poznaniem wyników. Dzięki temu wiadomo, czy próba odpowie na pytanie o jedną usługę, grupę użytkowników czy szerszy zbiór.

P16-K03 **Weryfikacja dowodów.** Weryfikator porównuje zapis z obserwacją lub powtórzeniem czynności. Brak materiału uzasadnia wniosek o luce dowodowej, a zaobserwowana usterka pozwala już zlecić naprawę konkretnego mechanizmu.

P16-K04 **Wykonawca audytu.** Dla audytu podlegającego wymogom ustawowym sprawdza się kwalifikacje i niezależność wykonawcy oraz zapewnia mu dostęp do materiału. Te ustalenia warunkują możliwość wykorzystania wyniku w danej ścieżce.

P16-K05 **Sprawozdanie i przekazanie.** Podpisane sprawozdanie, data odbioru i potwierdzenie przekazania pozwalają oddzielnie ocenić wynik audytu i dotrzymanie obowiązku wobec organu, zgodnie z właściwą ścieżką.

P16-K06 **Naprawa i ponowny test.** Przypisanie właściciela i terminu uruchamia naprawę. Dopiero powtórna ocena pokazuje, czy środek działa, oraz które otwarte ryzyka wymagają jeszcze zasobów lub decyzji kierownictwa.

Przekazanie wyniku. P01 wskazuje właściwy tryb, a P04 pomaga wybrać zagadnienia o największych skutkach. Na przykład nieudana próba z P14 skutkuje zleceniem poprawki właścicielowi odtwarzania. P16 weryfikuje wynik powtórzenia, P04 aktualizuje ocenę pozostałego ryzyka, a P02 otrzymuje ustalenia wymagające decyzji kierownictwa.

P17

Ochrona fizyczna i środowiskowa

Awaria zasilania może przerwać usługę tak samo skutecznie jak awaria jej oprogramowania. Art. 21 ust. 2 zdanie wprowadzające NIS2 wprost obejmuje środowisko fizyczne w podejściu uwzględniającym wszystkie zagrożenia. Z ust. 1 wynika proporcjonalny dobór środków. Organizacja mająca własny obiekt może sprawdzić stan zabezpieczeń na miejscu. Przy infrastrukturze zewnętrznej potrzebuje wiedzy o granicy odpowiedzialności, możliwości odzyskania usługi oraz wiarygodnego potwierdzenia od gospodarza obiektu. W obu przypadkach można ustalić, kto zareaguje na utratę istotnej zależności. NIS2, art. 21

P17-K01 **Lokalizacje i gospodarze.** Przyporządkowanie usługi do lokalizacji, mediów i gospodarza ujawnia wspólne punkty zależności. Pozwala też wskazać osobę, która sprawdzi stan obiektu w czasie awarii.

P17-K02 **Zagrożenia fizyczne.** Ocena następstw utraty zasilania, dostępu osób nieuprawnionych czy przekroczenia dopuszczalnej temperatury daje podstawę do wyboru zabezpieczeń oraz określenia, kiedy dyżurny powinien zareagować.

P17-K03 **Dostęp do obiektu.** Powiązanie klucza, identyfikatora lub wizyty serwisowej z osobą i zatwierdzoną potrzebą pozwala wygasić dostęp po zakończeniu prac albo ustalić, co trzeba zabezpieczyć po utracie klucza.

P17-K04 **Próba zabezpieczeń i alarmu.** Próba alarmu obejmuje odbiór sygnału i czynność dyżurnego. Sprawny czujnik może sygnalizować awarię w pustym pomieszczeniu, podczas gdy osoba odpowiedzialna za interwencję niczego się nie dowie.

P17-K05 **Usterki i zmiany lokalizacji.** Zmiana lokalizacji, przeterminowane uprawnienie lub usterka otwierają sprawę z opisem skutku dla usługi. Aktualizacja dokumentacji i ponowne sprawdzenie pozwalają zamknąć sprawę lub przekazać utrzymujące się ryzyko właścicielowi.

Przekazanie wyniku. P17 aktualizuje mapę zależności P03 i scenariusze ryzyka P04. P05 otrzymuje wymagania wobec zewnętrznego gospodarza, P11 informację o zakłóceniu, a P13 dane o zagrożonym poziomie świadczenia usługi potrzebne do decyzji o pracy zastępczej.

P18

Informowanie użytkowników i współpraca przy cyberzagrożeniach

Przy tym samym zdarzeniu zespół reagowania potrzebuje danych do koordynacji, a użytkownik potrzebuje odpowiedzi, czy może korzystać z usługi i jak ograniczyć szkody. Art. 23 ust. 1–2 NIS2 przewiduje powiadamianie odbiorców bez zbędnej zwłoki w stosownych przypadkach. Rozróżnia poważny incydent mogący niekorzystnie wpłynąć na świadczenie usług i poważne cyberzagrożenie, wobec którego odbiorca może podjąć środki ochronne. W polskiej ustawie art. 11 ust. 2b wiąże informację o incydencie poważnym z jego niekorzystnym wpływem na świadczenie usługi. Art. 9 ust. 1 pkt 2–3 określa stały dostęp do wiedzy i możliwość zgłaszania problemów przez użytkownika. Przesłanki rozpatruje się dla profilu z P01. NIS2, art. 23 · KSC, art. 9 i 11

P18-K01 **Wiedza i kanał zgłoszeń.** Wskazówki powiązane z usługą i przetestowany kontakt skracają drogę od obserwacji przez użytkownika do osoby, która może podjąć sprawę. Zgłoszenie próbne ujawnia na przykład formularz, którego nikt już nie obsługuje.

P18-K02 **Dobór odbiorców.** Ustalenie dotkniętej grupy, znanych faktów i możliwego działania odbiorców pozwala zdecydować o pouczeniu ochronnym, informacji o zagrożeniu lub komunikacie o incydencie.

P18-K03 **Wskazówki przy zagrożeniu.** Użytkownik potencjalnie dotknięty poważnym cyberzagrożeniem otrzymuje wskazówki, które może zastosować. Dla informacji o samym zagrożeniu art. 11 ust. 2a KSC przewiduje dodatkową ocenę, czy ujawnienie zwiększy ryzyko dla bezpieczeństwa systemów informacyjnych. KSC, art. 11 ust. 2a

P18-K04 **Informacja o incydencie.** Przy spełnieniu przesłanek komunikat o skutkach incydentu pomaga odbiorcy zaplanować dalszą pracę. Wspólny identyfikator wysyłki umożliwia P12 potwierdzenie poinformowania użytkowników, podczas gdy zgłoszenie do CSIRT ma własnego adresata i potwierdzenie.

P18-K05 **Dobrowolna wymiana.** Uczestnictwo w wymianie informacji jest dobrowolne. Po wyborze tej drogi trzeba ustalić dopuszczalny kanał, adresatów i warunki dalszego przekazywania. Art. 29 ust. 4 NIS2 przewiduje powiadamianie właściwego organu o przystąpieniu, a stosownie do sytuacji także o wystąpieniu z mechanizmu. W Polsce zawarcie porozumienia z art. 8h ust. 6 KSC jest daną w wykazie. P18 przekazuje datę zmiany do P01-K05, żeby podmiot mógł złożyć wniosek o zmianę wpisu w ciągu 14 dni. KSC, art. 7 ust. 2 pkt 18 i art. 7c ust. 3 · NIS2, art. 29 · KSC, art. 8h

P18-K06 **Korekta i dotarcie do odbiorców.** Zmiana rozpoznania sytuacji może wymagać odwołania wcześniejszej porady. Historia wersji, niedoręczenia i pytania do obsługi pozwalają wskazać grupę, która powinna dostać korektę innym kanałem.

Przekazanie wyniku. P11 dostarcza potwierdzone fakty i informację o skutkach dla usługi. P12 prowadzi równolegle zgłoszenie urzędowe, a od P18 otrzymuje zapis komunikacji z użytkownikami. W drugą stronę zgłoszenia od użytkowników mogą uruchomić ocenę zdarzenia w P11 lub postępowanie z podatnością w P09. P16 ocenia dotarcie do właściwych odbiorców i przydatność wskazówek.

Źródła i zakres interpretacji

Opracowanie objaśnia wersję 0.1 bazy z 18 listopada 2026 r. Opisuje zależności między procesami organizacji. Przyjęcie rozwiązania dla konkretnej usługi wymaga ustalenia jej zakresu, właściwego reżimu prawnego i warunków technicznych. Podane role, nazwy procesów, przykładowe narzędzia, przebieg prób oraz nazwy dowodów są elementami modelu organizacyjnego.

• **Dyrektywa (UE) 2022/2555.** Art. 2–4 i 26–27 dotyczą zakresu, jurysdykcji i rejestrów. Art. 20–21 stanowią podstawę nadzoru kierownictwa i środków zarządzania ryzykiem. Art. 23 dotyczy zgłaszania i informowania, art. 29 wymiany informacji, a art. 32–33 uprawnień nadzorczych. Tekst polski w EUR-Lex

• **Ustawa o krajowym systemie cyberbezpieczeństwa.** Wykorzystano tekst ujednolicony Kancelarii Sejmu z datą redakcji 9 listopada 2026 r. Przy określaniu początku stosowania krajowych obowiązków znaczenie mają również przepisy przejściowe ustawy zmieniającej z 23 stycznia 2026 r. KSC w ELI · Ustawa zmieniająca, Dz.U. 2026 poz. 252

• **Rozporządzenie wykonawcze (UE) 2024/2690.** Art. 1 określa podmioty objęte rozporządzeniem. Przy kwalifikacji należy ustalić właściwe dla nich szczegółowe wymogi i przypadki uznania incydentu za poważny. Tekst polski w EUR-Lex

• **Materiały robocze.** Identyfikatory procesów, kroków i wzorów pochodzą z międzysektorowej bazy odniesienia. Diagramy przedstawiają wybrane przepływy na podstawie kart procesów. Fikcyjny przykład z wnioskami rozwija próbę opisaną we wzorze D08. Indeks bazy · Mapa wymagań i wyjątków · Narzędzia · Wzory dowodów