SZKOLENIE • MATERIAŁ DLA PROWADZĄCEGO

Baza FAQ prowadzącego

Gotowe odpowiedzi • numery slajdów • podstawy prawne i normatywne

NIS2 / KSC	ISO/IEC 27001	RYZYKO / SZBI

Piotr Słupczyński, MBA
Audytor Wiodący ISO/IEC 27001:2022

Przygotowano na podstawie 160-slajdowej prezentacji szkoleniowej na 13 listopada 2026 r. Stan źródeł prawnych zweryfikowany na 10 listopada 2026 r.

Materiał do używania w widoku prezentera i podczas sesji pytań. Odpowiedzi są celowo krótsze niż komentarz prawniczy: najpierw odpowiadają na pytanie, następnie wskazują wyjątek lub przykład.

Jak korzystać z FAQ

Każde hasło ma ten sam układ: **pytanie → odpowiedź → slajdy → podstawa**. Numer slajdu odnosi się do finalnej prezentacji liczącej 160 stron. Skrót „PRAKTYKA” oznacza rozwiązanie rekomendowane, którego nie należy przedstawiać jako dosłownego obowiązku ustawowego.

Formuła bezpiecznej odpowiedzi: 1. Jednozdaniowy wniosek. 2. Najważniejszy wyjątek lub warunek. 3. Przykład biznesowy. 4. Wskazanie slajdu i podstawy. Jeśli brak danych o konkretnej organizacji — nie wydawaj kategorycznej kwalifikacji.

Spis treści

01. Podstawy prawne, NIS2 i normy . . . 3

02. Samoidentyfikacja i kwalifikacja podmiotów . . . 4

03. Terminy, Wykaz KSC, S46 i organizacja wdrożenia . . . 6

04. Prezes, zarząd i osobista odpowiedzialność . . . 8

05. Kary, nadzór i audyty . . . 10

06. SZBI, ISO 27001, zabezpieczenia i dowody . . . 12

07. Zarządzanie ryzykiem, ERM, RACI i raportowanie . . . 15

08. Dostawcy, umowy NDA, SLA i outsourcing . . . 19

09. Człowiek, socjotechnika i programy antyphishingowe . . . 21

10. Incydenty, zgłoszenia CSIRT, S46 oraz RODO . . . 22

11. Ciągłość działania, ISO 22301, BIA i blackouty . . . 25

12. Wdrożenie, koszty, plan i trudne pytania z sali . . . 27

Źródła i uwagi do aktualizacji . . . 31

Legenda źródeł

PRAWO – przepis obowiązujący lub jego oficjalne omówienie; **NORMA** – wymaganie albo wytyczna normatywna; **PRAKTYKA** – autorski model organizacyjny, przykład lub rekomendacja. Przy pytaniach o konkretny podmiot sprawdzaj aktualny tekst prawa i regulacje sektorowe.

01. Podstawy prawne, NIS2 i normy

Jak odróżnić obowiązek prawny od narzędzia zarządzania i uniknąć błędnych uproszczeń.

001. Czym w jednym zdaniu różnią się NIS2, KSC i ISO/IEC 27001?

NIS2 określa europejskie ramy bezpieczeństwa i obowiązki państw członkowskich, KSC konkretyzuje obowiązki podmiotów w Polsce, a ISO/IEC 27001 opisuje wymagania wobec systemu zarządzania bezpieczeństwem informacji. Organizacja powinna połączyć je w jeden system działania, ale nie utożsamiać normy z ustawą.

SLAJDY: 3–5, 18, 41 **ODNIESIENIE:** Dyrektywa (UE) 2022/2555; ustawa o KSC; ISO/IEC 27001:2022 **CHARAKTER:** PRAWO + NORMA

002. Czy NIS2 jest „normą ISO”?

Nie. NIS2 to dyrektywa Unii Europejskiej, a ISO/IEC 27001 to norma międzynarodowa. Nie należy mówić „dwie normy NIS2 i ISO”. W Polsce podstawą konkretnych obowiązków organizacji jest przede wszystkim ustawa o KSC wraz z właściwymi przepisami szczególnymi.

SLAJDY: 4–5, 18, 22 **ODNIESIENIE:** Dyrektywa (UE) 2022/2555; KSC **CHARAKTER:** PRAWO

003. Czy firma nieobjęta KSC może wdrożyć ISO 27001?

Tak. Norma może być stosowana niezależnie od ustawowego statusu podmiotu. Pomaga porządkować ryzyka, role, dokumentację, audyty i doskonalenie. Jest to często decyzja biznesowa wynikająca z wymagań klientów, kontraktów albo własnej oceny ryzyka.

SLAJDY: 18, 60–61, 77 **ODNIESIENIE:** ISO/IEC 27001:2022, klauzule 4–10 **CHARAKTER:** NORMA

004. Czy certyfikat ISO 27001 automatycznie potwierdza zgodność z KSC?

Nie. Certyfikat potwierdza wynik certyfikacji SZBI w określonym zakresie, a nie spełnienie wszystkich obowiązków ustawowych. Osobno sprawdza się np. kwalifikację, wpis do Wykazu KSC, S46, właściwe zgłoszenia incydentów, audyty ustawowe i obowiązki kierownictwa.

SLAJDY: 18, 41, 77 **ODNIESIENIE:** KSC art. 5, 8, 11–15; ISO/IEC 27001:2022 **CHARAKTER:** PRAWO + NORMA

005. Czy ISO 27001 trzeba koniecznie certyfikować, aby wdrożyć SZBI?

Nie. Należy odróżnić wdrożenie i utrzymywanie systemu od dobrowolnej certyfikacji. Jeżeli określony kontrakt lub przepis sektorowy nie wymaga certyfikatu, nie należy przedstawiać go jako automatycznego warunku zgodności z KSC. Wymagane jest faktyczne realizowanie obowiązków.

SLAJDY: 60–61, 68, 77 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001:2022 **CHARAKTER:** PRAWO + NORMA

006. Po co ISO/IEC 27005, skoro mamy ISO/IEC 27001?

ISO/IEC 27001 stawia wymagania wobec oceny i postępowania z ryzykiem. ISO/IEC 27005 rozwija metodyczne wskazówki, jak identyfikować scenariusze, oceniać skutki, wybierać działania i monitorować ryzyko. To przydatny przewodnik, nie osobny obowiązek certyfikacyjny wynikający z KSC.

SLAJDY: 5, 79–80, 94–95 **ODNIESIENIE:** ISO/IEC 27001:2022, 6.1.2–6.1.3; ISO/IEC 27005:2022 **CHARAKTER:** NORMA

007. Czym różni się ISO 31000 od ISO 27005?

ISO 31000 opisuje ogólne zasady zarządzania ryzykiem w całej organizacji. ISO/IEC 27005 koncentruje się na ryzyku bezpieczeństwa informacji. Wspólne definicje skutku i apetytu na ryzyko pozwalają połączyć ocenę SZBI z profilem ryzyka biznesowego.

SLAJDY: 5, 79–88 **ODNIESIENIE:** ISO 31000:2018; ISO/IEC 27005:2022 **CHARAKTER:** NORMA

008. Dlaczego w szkoleniu jest też ISO 22301?

Bo cyberbezpieczeństwo ma chronić zdolność świadczenia usług, nie tylko systemy informatyczne. PN-EN ISO 22301 wspiera analizę wpływu zakłóceń na działalność, planowanie ciągłości, odtwarzanie i testowanie gotowości. Uzupełnia podejście SZBI, ale nie zastępuje ISO 27001.

SLAJDY: 5, 129–136 **ODNIESIENIE:** PN-EN ISO 22301:2020-04/A1:2025-03; KSC art. 8 **CHARAKTER:** NORMA + PRAWO

009. Czy DORA zastępuje KSC w bankach?

Nie należy tego uogólniać. DORA jest regulacją szczególną dla podmiotów finansowych i ma pierwszeństwo w określonych, pokrywających się obszarach. Konkretną relację obowiązków i raportowania trzeba ustalić według rodzaju podmiotu oraz właściwych przepisów; nie oznacza to automatycznego wyłączenia całej KSC.

SLAJDY: 4, 23, 137 **ODNIESIENIE:** Rozporządzenie (UE) 2022/2554 (DORA); KSC; stanowiska KNF **CHARAKTER:** PRAWO

010. Czy rozporządzenie 2024/2690 dotyczy każdej firmy objętej KSC?

Nie. Doprecyzowuje wymogi i progi incydentów dla określonych kategorii usług cyfrowych, m.in. chmury, DNS, centrów danych, usług zarządzanych i niektórych platform. Najpierw ustala się, czy organizacja mieści się w zakresie aktu; dopiero później stosuje jego szczególne kryteria.

SLAJDY: 4, 23, 121–124 **ODNIESIENIE:** Rozporządzenie wykonawcze Komisji (UE) 2024/2690 **CHARAKTER:** PRAWO

011. Czy normy ISO można stosować bez kupowania ich pełnych tekstów?

Można znać ogólne założenia z opracowań, ale przy rzeczywistym wdrożeniu i audycie wymagane jest oparcie się na aktualnej, legalnie pozyskanej treści normy i jej zmian. Prezentacja szkoleniowa nie zastępuje dokumentu normatywnego.

SLAJDY: 5, 19, 61 **ODNIESIENIE:** ISO/IEC 27001:2022; ISO/IEC 27005:2022 **CHARAKTER:** NORMA

02. Samoidentyfikacja i kwalifikacja podmiotów

Najczęstsze pytania o sektory, status kluczowy/ważny, powiązania i dokumentowanie decyzji.

012. Od czego zacząć ocenę, czy firma podlega KSC?

Od rzeczywiście świadczonych usług, następnie właściwych pozycji załączników 1–2, rozmiaru przedsiębiorstwa i powiązań kapitałowych, a potem szczególnych przesłanek i wyjątków z art. 5. Wynik trzeba udokumentować wraz z uzasadnieniem; sam kod PKD nie wystarczy.

SLAJDY: 24–25, 31–33 **ODNIESIENIE:** KSC art. 5 i załączniki 1–2; MC FAQ, rozdz. 1 **CHARAKTER:** PRAWO

013. Czy każda firma zatrudniająca 50 osób automatycznie podlega KSC?

Nie. Wielkość jest tylko jednym z kryteriów. Konieczna jest jeszcze działalność mieszcząca się w odpowiedniej pozycji ustawowej i sprawdzenie wyjątków. W niektórych kategoriach znaczenie mają szczególne reguły niezależne od rozmiaru.

SLAJDY: 24–32 **ODNIESIENIE:** KSC art. 5; MC FAQ 1.1–1.11 **CHARAKTER:** PRAWO

014. Czy spółka zatrudniająca 250 osób zawsze jest podmiotem kluczowym?

Nie. Taką kwalifikację można rozważać dopiero po sprawdzeniu sektora, rodzaju usługi, przesłanek art. 5 oraz właściwego sposobu liczenia wielkości przedsiębiorstwa. Sama liczba pracowników nie przesądza o statusie.

SLAJDY: 29–32 **ODNIESIENIE:** KSC art. 5; załączniki 1–2 **CHARAKTER:** PRAWO

015. Czy trzeba uwzględniać spółki powiązane i partnerskie?

Tak, przy ustalaniu wielkości przedsiębiorstwa stosuje się właściwe zasady odnoszące się także do podmiotów partnerskich i powiązanych. Nie można automatycznie oceniać spółki w oderwaniu od grupy kapitałowej. Należy udokumentować sposób kalkulacji.

SLAJDY: 25, 31–32 **ODNIESIENIE:** KSC art. 5; zalecenie Komisji 2003/361/WE; MC FAQ 1.5–1.6 **CHARAKTER:** PRAWO

016. Czy wystarczy sprawdzić PKD?

Nie. PKD jest pomocną wskazówką, lecz rozstrzyga faktycznie wykonywana działalność i opis podmiotu lub usługi w ustawie. Spółka może podlegać KSC z tytułu działalności ubocznej nawet wtedy, gdy jej główny kod PKD sugeruje inny sektor.

SLAJDY: 24–28, 33 **ODNIESIENIE:** KSC art. 5 i załączniki; MC FAQ 2.7–2.8 **CHARAKTER:** PRAWO

017. Jaka jest najważniejsza różnica między podmiotem kluczowym a ważnym?

Oba realizują istotne obowiązki zarządzania ryzykiem i incydentami. Różnią się szczegółową kwalifikacją, intensywnością nadzoru i niektórymi obowiązkami audytowymi oraz górnymi granicami kar. Nie należy traktować podmiotu ważnego jako „zwolnionego z cyberbezpieczeństwa".

SLAJDY: 29–30, 48–58 **ODNIESIENIE:** KSC art. 5, 8, 15 i przepisy nadzorcze **CHARAKTER:** PRAWO

018. Czy podmiot z załącznika nr 2 może zostać uznany za kluczowy?

Nie należy zakładać jednego prostego schematu. W pierwszej kolejności trzeba zastosować art. 5 i przepisy szczególne. Sam fakt ujęcia rodzaju działalności w załączniku nr 2 nie zastępuje całościowej analizy statusu.

SLAJDY: 26–32 **ODNIESIENIE:** KSC art. 5; załączniki 1–2 **CHARAKTER:** PRAWO

019. Czy dostawca usług ICT świadczący usługi wyłącznie dla własnej grupy kapitałowej może podlegać KSC?

Może, ale odpowiedź wymaga ustalenia charakteru usług, relacji między spółkami i właściwych definicji ustawowych. Nie wystarczy stwierdzenie, że klient jest „wewnętrzny". Warto przeanalizować model umowny i faktyczne świadczenie usług.

SLAJDY: 24–28, 32 **ODNIESIENIE:** KSC art. 5 i definicje; MC FAQ 1.21 **CHARAKTER:** PRAWO

020. Czy każda spółka produkcyjna jest podmiotem ważnym?

Nie. Załącznik nr 2 wymienia określone rodzaje produkcji, a nie całą produkcję jako taką. Trzeba dopasować realną działalność do pozycji ustawowej i sprawdzić wielkość oraz wyjątki.

SLAJDY: 26, 28, 31 **ODNIESIENIE:** KSC załącznik nr 2; MC FAQ 1.4 **CHARAKTER:** PRAWO

021. Czy małe podmioty mogą podlegać KSC?

Tak, w ustawowo określonych przypadkach. Dlatego reguła „poniżej 50 pracowników — nie podlegamy" jest niebezpieczna. Przykładowe wyjątki dla niektórych usług cyfrowych i publicznych trzeba analizować indywidualnie.

SLAJDY: 31–32 **ODNIESIENIE:** KSC art. 5; MC FAQ 1.7–1.9 **CHARAKTER:** PRAWO

022. Czy każda szkoła, urząd albo jednostka samorządowa automatycznie podlega KSC?

Nie. Dla podmiotów publicznych obowiązują szczególne definicje i wyjątki; sama nazwa instytucji nie przesądza o kwalifikacji. Należy ustalić formę prawną i odpowiednią pozycję ustawy.

SLAJDY: 26–28, 32 **ODNIESIENIE:** KSC art. 5 i załączniki; MC FAQ 1.8, 1.16, 2.6 **CHARAKTER:** PRAWO

023. Czy podmiot dostaje decyzję potwierdzającą, że jest kluczowy lub ważny?

Co do zasady samoidentyfikacja nie polega na oczekiwaniu na indywidualną decyzję, która „nada" status wszystkim podmiotom. Obowiązek sprawdzenia i dokonania wpisu wynika z przesłanek ustawowych. W szczególnych przypadkach możliwe są działania organu.

SLAJDY: 24–25, 33, 38 **ODNIESIENIE:** KSC art. 5; MC FAQ 1.12–1.13 **CHARAKTER:** PRAWO

024. Co jeśli spółka spełnia jednocześnie kryteria dla podmiotu kluczowego i ważnego?

Trzeba uwzględnić wszystkie podstawy kwalifikacji i zastosować ustawowe reguły kolizyjne, zamiast wybierać korzystniejszą kategorię. Wynik należy udokumentować wraz z dokładnymi podstawami prawnymi.

SLAJDY: 29–33 **ODNIESIENIE:** KSC art. 5; MC FAQ 1.10 **CHARAKTER:** PRAWO

025. Jakie dokumenty potwierdzą rzetelną samoidentyfikację?

Krótka notatka z opisem usług, mapowaniem do załączników, wyliczeniem wielkości i powiązań, analizą art. 5, wskazaniem decyzji, daty i osoby odpowiedzialnej. Dokument warto aktualizować przy zmianie usług, wielkości, grupy kapitałowej lub prawa.

SLAJDY: 25, 33, 140–141 **ODNIESIENIE:** KSC art. 5; praktyka dokumentowania zgodności **CHARAKTER:** PRAWO + PRAKTYKA

03. Terminy, Wykaz KSC, S46 i organizacja wdrożenia

Odpowiedzi wymagające precyzyjnego odróżnienia dat bazowych od terminów liczonych indywidualnie.

026. Kiedy weszła w życie nowelizacja KSC z 2026 roku?

Nowelizacja z 23 stycznia 2026 r., ogłoszona w Dz.U. 2026 poz. 252, weszła w życie 3 kwietnia 2026 r. To punkt startowy dla wielu przepisów przejściowych; część terminów liczy się jednak od późniejszego spełnienia przesłanek.

SLAJDY: 19, 21–23, 34–36 **ODNIESIENIE:** Dz.U. 2026 poz. 252; przepisy przejściowe **CHARAKTER:** PRAWO

027. Dlaczego w prezentacji pojawia się 3 października 2026 r.?

To bazowy termin samorejestracji dla podmiotów, które spełniały przesłanki już w dniu 3 kwietnia 2026 r. Podmiot, który uzyska status później, powinien ustalić własny termin zgodnie z ustawą.

SLAJDY: 34–38 **ODNIESIENIE:** KSC i przepisy przejściowe; MC FAQ 2.1, 3.1 **CHARAKTER:** PRAWO

028. Co jeśli firma nie złożyła wniosku do Wykazu KSC w terminie?

Nie należy czekać. Najpierw należy potwierdzić status i jego datę, następnie niezwłocznie podjąć czynności rejestracyjne, zabezpieczyć dowody oraz przygotować uzasadnienie przyczyn opóźnienia. Sposób oceny naruszenia należy odróżnić od automatycznego naliczenia kary.

SLAJDY: 33–38, 54 **ODNIESIENIE:** KSC przepisy o Wykazie i sankcjach; MC FAQ 2 **CHARAKTER:** PRAWO + PRAKTYKA

029. Czy wpis do Wykazu KSC i podłączenie do S46 to to samo?

Nie. Wpis dokumentuje status i dane podmiotu; operacyjne korzystanie z S46 służy m.in. komunikacji i zgłaszaniu incydentów. Są to powiązane, ale odrębne zadania organizacyjne, z różnymi czynnościami i terminami.

SLAJDY: 34–38, 126 **ODNIESIENIE:** KSC przepisy o Wykazie i S46; MC FAQ 2–3 **CHARAKTER:** PRAWO

030. Jaki jest główny termin wdrożenia SZBI dla nowych podmiotów z 2026 r.?

Dla podmiotów spełniających przesłanki od 3 kwietnia 2026 r. bazowy termin wynosi 3 kwietnia 2027 r. Przy późniejszym nabyciu statusu trzeba obliczyć termin indywidualnie. Warto budować plan wdrożenia od dowodów działania, a nie od daty podpisania polityki.

SLAJDY: 34–37, 140–147 **ODNIESIENIE:** KSC przepisy przejściowe; MC FAQ 3.1 **CHARAKTER:** PRAWO

031. Czy 3 kwietnia 2027 r. wszystkie firmy mają już posiadać certyfikat ISO 27001?

Nie. Chodzi o ustawowe obowiązki, a nie ogólny nakaz uzyskania certyfikatu ISO 27001. Organizacja musi zapewnić działania i dowody wymagane dla swojej kategorii; certyfikacja może być odrębną decyzją.

SLAJDY: 34–37, 60, 77 **ODNIESIENIE:** KSC art. 8 i przepisy przejściowe **CHARAKTER:** PRAWO

032. Kiedy przypada pierwszy audyt ustawowy?

Dla określonych nowych podmiotów kluczowych, które wcześniej nie były operatorami usług kluczowych, bazowa data to 3 kwietnia 2028 r. Nie wolno przenosić jej automatycznie na wszystkie podmioty ani mylić z audytem certyfikacyjnym ISO.

SLAJDY: 34–36, 57–58 **ODNIESIENIE:** KSC art. 15 i przepisy przejściowe; MC FAQ 3.1 **CHARAKTER:** PRAWO

033. Czy podmiot ważny ma obowiązek zewnętrznego audytu co trzy lata?

Nie należy mu automatycznie przypisywać tego samego cyklu co podmiotowi kluczowemu. Może jednak podlegać kontroli, żądaniu audytu lub innym środkom nadzorczym zgodnie z właściwymi przepisami. Audyt wewnętrzny SZBI to odrębny temat.

SLAJDY: 29–30, 55–58 **ODNIESIENIE:** KSC art. 15 i przepisy nadzorcze **CHARAKTER:** PRAWO

034. Czy wdrożenie możemy zakończyć w trzy miesiące?

W określonej organizacji bywa to możliwe dla części działań, ale nie ma uniwersalnego terminu projektu. Najpierw należy poznać zakres, liczbę zależności, luki i dostępne zasoby. Plan 30/90/180/365 dni z prezentacji jest przykładem organizacyjnym, nie terminem ustawowym.

SLAJDY: 140–147, 155 **ODNIESIENIE:** KSC terminy ustawowe; model planowania wdrożenia **CHARAKTER:** PRAKTYKA

035. Od czego liczyć termin po nabyciu statusu podmiotu?

Od właściwego momentu spełnienia przesłanek ustawowych, przy uwzględnieniu przepisów przejściowych i ewentualnych szczególnych reguł sektorowych. Dlatego w notatce samoidentyfikacji należy zapisać nie tylko status, ale również datę, od której on przysługuje.

SLAJDY: 25, 34–36 **ODNIESIENIE:** KSC art. 5 oraz przepisy przejściowe **CHARAKTER:** PRAWO

036. Kto powinien być właścicielem harmonogramu wdrożenia?

Najlepiej wskazać kierownika projektu lub koordynatora SZBI, ale sponsor i nadzór powinny pozostawać na odpowiednim poziomie kierownictwa. Każde działanie musi mieć osobę wykonującą, właściciela decyzji, termin i dowód zakończenia.

SLAJDY: 37, 44–47, 140–149 **ODNIESIENIE:** KSC art. 8c–8e; ISO/IEC 27001:2022, klauzula 5 **CHARAKTER:** PRAWO + NORMA

04. Prezes, zarząd i osobista odpowiedzialność

Odpowiedzi na pytania zadawane przez kierownictwo: co trzeba wiedzieć, zatwierdzić i nadzorować.

037. Czy prezes odpowiada za cyberbezpieczeństwo, jeśli zatrudnia dyrektora IT?

Odpowiedzialność za wykonanie obowiązków i nadzór nie znika przez delegowanie zadań. Specjaliści mogą prowadzić operacje i rekomendować rozwiązania, ale kierownictwo powinno otrzymywać informacje o ryzykach, decyzjach, środkach i skuteczności.

SLAJDY: 44–47 **ODNIESIENIE:** KSC art. 8c–8e; NIS2 art. 20 **CHARAKTER:** PRAWO

038. Czy prezes musi rozumieć konfigurację firewalli?

Nie musi osobiście konfigurować zabezpieczeń. Powinien jednak wiedzieć, które usługi są krytyczne, jakie ryzyka przekraczają tolerancję organizacji, ile kosztuje ich ograniczenie i jak sprawdzić skuteczność działań. To różnica między zadaniem technicznym a nadzorem zarządczym.

SLAJDY: 44–47, 99–101, 158 **ODNIESIENIE:** NIS2 art. 20; KSC art. 8d **CHARAKTER:** PRAWO + PRAKTYKA

039. Jakie decyzje powinien zatwierdzać zarząd w ramach SZBI?

Co najmniej kierunek i cele bezpieczeństwa, zakres odpowiedzialności, sposób nadzoru, zasoby oraz decyzje przekraczające delegowane limity akceptacji ryzyka. Konkretna matryca kompetencji musi być zgodna z organizacją i wewnętrznymi upoważnieniami.

SLAJDY: 44–47, 64, 76, 92–93 **ODNIESIENIE:** KSC art. 8c–8e; ISO/IEC 27001:2022, 5 i 6 **CHARAKTER:** PRAWO + NORMA

040. Czy członkowie zarządu muszą się szkolić?

Tak, w zakresie i częstotliwości wynikających z właściwych przepisów KSC; prezentacja omawia coroczne udokumentowane szkolenie kierownika. Warto zachować program, listę obecności oraz potwierdzenie, że szkolenie dotyczyło faktycznych ryzyk organizacji.

SLAJDY: 44, 46–47 **ODNIESIENIE:** KSC art. 8e; NIS2 art. 20 ust. 2 **CHARAKTER:** PRAWO

041. Czy w zarządzie wieloosobowym każdy odpowiada za wszystko?

Nie należy upraszczać tego do jednego zdania. Zakres odpowiedzialności kierowników wynika z ustawy i struktury danego podmiotu. W praktyce trzeba udokumentować podział zadań i raportowanie, ale wewnętrzny regulamin nie może znosić odpowiedzialności przewidzianej prawem.

SLAJDY: 44, 46–47 **ODNIESIENIE:** KSC art. 8c–8e; przepisy ustrojowe podmiotu **CHARAKTER:** PRAWO

042. Czy prezes może zaakceptować każde ryzyko, nawet skrajnie wysokie?

Sama akceptacja nie zwalnia z obowiązku zastosowania odpowiednich i proporcjonalnych środków wymaganych prawem. Ryzyko może być akceptowane tylko w ramach ustalonych kryteriów i uprawnień; nie może to być sposób na obejście wymogów ustawowych lub kontraktowych.

SLAJDY: 39–40, 44–47, 92–93 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001:2022, 6.1.3 **CHARAKTER:** PRAWO + NORMA

043. Czy każde ryzyko musi osobiście podpisywać prezes?

Nie. Właściwa matryca delegacji może przyznawać prawo akceptacji ryzyka właścicielom procesów albo odpowiednim dyrektorom. Prezes powinien otrzymywać ryzyka przekraczające zatwierdzone progi, ryzyka strategiczne i wymagające decyzji o zasobach.

SLAJDY: 81–83, 92–93 **ODNIESIENIE:** ISO/IEC 27001:2022, 6.1.3; praktyka ERM **CHARAKTER:** NORMA + PRAKTYKA

044. Jak często zarząd powinien otrzymywać raport o cyberbezpieczeństwie?

Prawo nie ustanawia uniwersalnego comiesięcznego dashboardu dla każdej firmy. Cykl należy ustalić według ryzyka, a incydenty i przekroczenia progów eskalować bez zwłoki. Dla wielu organizacji sensowny jest przegląd kwartalny plus raporty ad hoc.

SLAJDY: 76, 99–103, 138 **ODNIESIENIE:** KSC art. 8d; ISO/IEC 27001:2022, 9.3; dobra praktyka **CHARAKTER:** PRAWO + PRAKTYKA

045. Co powinno znaleźć się na jednej stronie raportu dla prezesa?

Najważniejsze zagrożone usługi, skutek biznesowy i trend ryzyka, ryzyka poza tolerancją, stan najważniejszych działań, zależności od dostawców, incydenty oraz decyzje wymagające zgody. Raport ma umożliwiać działanie, a nie prezentować katalog technicznych wykresów.

SLAJDY: 99–103, 138, 158 **ODNIESIENIE:** ISO/IEC 27001:2022, 9.1 i 9.3; praktyka ERM **CHARAKTER:** NORMA + PRAKTYKA

046. Jak zarząd ma ocenić, czy wydatek na bezpieczeństwo ma sens?

Nie przez liczbę zakupionych licencji, tylko przez zmianę ekspozycji na ryzyko. Należy porównać możliwy skutek przestoju lub naruszenia z kosztem i skutecznością działań, także z kosztami operacyjnymi, szkoleniami, testami i zależnościami od dostawców.

SLAJDY: 45, 90–93, 98–101 **ODNIESIENIE:** KSC art. 8; ISO 31000; praktyka oceny ryzyka **CHARAKTER:** PRAWO + PRAKTYKA

047. Jakie dowody nadzoru powinien przechowywać zarząd?

Decyzje i protokoły przeglądów, akceptacje ryzyka, zatwierdzone zasoby, raporty o przekroczeniach tolerancji, plany działań, dowody szkoleń i wyniki testów. Warto zapisywać także to, czego nie zaakceptowano, kto ma działać i do kiedy.

SLAJDY: 46–47, 64–68, 76, 151 **ODNIESIENIE:** KSC art. 8c–8e; ISO/IEC 27001:2022, 9.3 **CHARAKTER:** PRAWO + NORMA

048. Co powinien zrobić zarząd, gdy projekt wdrożenia KSC się opóźnia?

Zażądać mapy luk, konsekwencji biznesowych, nowego planu z terminami i osobami odpowiedzialnymi, decyzji o priorytetach oraz dowodów postępu. Nie należy ukrywać opóźnienia pod ogólnym statusem „w trakcie”; potrzebne jest udokumentowane zarządzanie odchyleniem.

SLAJDY: 37, 44–47, 140–151 **ODNIESIENIE:** KSC art. 8c–8e; praktyka nadzoru **CHARAKTER:** PRAWO + PRAKTYKA

049. Czy IOD, audytor lub pełnomocnik SZBI może przejąć odpowiedzialność zarządu?

Może doradzać, monitorować i wykonywać określone czynności zgodnie z mandatem, ale nie zastępuje kierownictwa w decyzjach biznesowych i ustawowej odpowiedzialności. Warto także ocenić niezależność audytora i ewentualny konflikt ról.

SLAJDY: 44–47, 57, 65, 81–83 **ODNIESIENIE:** KSC art. 8c–8e; ISO/IEC 27001:2022, 5 i 9.2 **CHARAKTER:** PRAWO + NORMA

05. Kary, nadzór i audyty

Jak mówić o konsekwencjach rzetelnie, bez przesadnego straszenia zarządu.

050. Jakie są górne pułapy kar dla podmiotów kluczowych i ważnych?

Dla podmiotu kluczowego zasadniczy próg to 10 mln EUR albo 2% właściwych przychodów; dla ważnego 7 mln EUR albo 1,4%. Mechanizm wyboru wartości i dokładny zakres naruszenia wynikają z ustawy. To limity, a nie automatyczna kara po incydencie.

SLAJDY: 48–51 **ODNIESIENIE:** KSC art. 73 i nast.; MC FAQ 12.4 **CHARAKTER:** PRAWO

051. Czy od razu po incydencie organ nałoży 10 mln EUR kary?

Nie. Sam incydent nie oznacza automatycznie maksymalnej sankcji. Znaczenie mają rodzaj naruszenia obowiązku, okoliczności, skutek, postawa podmiotu i ustawowa procedura. Trzeba odróżnić incydent od niewypełnienia obowiązków zarządzania bezpieczeństwem.

SLAJDY: 48–54, 121–124 **ODNIESIENIE:** KSC art. 73 i nast.; MC FAQ 12.3, 12.9–12.11 **CHARAKTER:** PRAWO

052. Czy kary pieniężne można nakładać już w listopadzie 2026 r.?

Zwykłe sankcje za określone naruszenia podlegają regule przejściowej przewidującej ich stosowanie od 3 kwietnia 2028 r. Wyjątkiem jest kara ekstraordynaryjna. Nie oznacza to odroczenia wszystkich obowiązków organizacji.

SLAJDY: 34–36, 48–54 **ODNIESIENIE:** KSC przepisy przejściowe; MC FAQ 12.1 **CHARAKTER:** PRAWO

053. Jaka może być kara pieniężna dla kierownika?

Według wyjaśnień Ministerstwa Cyfryzacji przewidziano odrębny mechanizm odpowiedzialności pieniężnej kierownika: do 300% wynagrodzenia w podmiocie prywatnym lub 100% w publicznym, przy spełnieniu ustawowych przesłanek. Nie jest to automatyczna sankcja za każdy błąd.

SLAJDY: 46–47, 50, 52 **ODNIESIENIE:** KSC przepisy o odpowiedzialności kierownika; MC FAQ 12.4 i 12.10 **CHARAKTER:** PRAWO

054. Czym jest kara okresowa?

To środek przymuszający do wykonania nałożonej decyzji, a nie zwykła kara za każdy dzień trwania incydentu. Ministerstwo wskazuje przedział od 500 zł do 100 000 zł za dzień opóźnienia w realizacji decyzji.

SLAJDY: 50–53 **ODNIESIENIE:** KSC przepisy sankcyjne; MC FAQ 12.5 **CHARAKTER:** PRAWO

055. Czym jest kara ekstraordynaryjna?

To wyjątkowa sankcja do 100 mln zł związana z poważnymi naruszeniami i szczególnymi przesłankami zagrożenia. Nie wolno przedstawiać jej jako zwykłej kary za brak jednego dokumentu. Należy przywołać konkretne ustawowe przesłanki.

SLAJDY: 50–53 **ODNIESIENIE:** KSC przepisy sankcyjne; MC FAQ 12.6 **CHARAKTER:** PRAWO

056. Czy organ ostrzega przed karą?

Przepisy przewidują określoną procedurę nadzorczą, w tym ostrzeżenie i informowanie o wstępnych ustaleniach w sytuacjach opisanych w ustawie. Nie oznacza to pełnej gwarancji dowolnego czasu na naprawę ani zwolnienia z bieżących obowiązków.

SLAJDY: 53–56 **ODNIESIENIE:** KSC przepisy nadzorcze; MC FAQ 12.3, 12.7–12.8 **CHARAKTER:** PRAWO

057. Co może kontrolować organ?

Nie tylko polityki. Może badać dokumentację, dowody operacyjne, decyzje, testy, wyniki audytów oraz faktyczne funkcjonowanie zabezpieczeń, zgodnie ze swoimi uprawnieniami. Deklaracja „mamy procedurę” nie jest wystarczającym dowodem skuteczności.

SLAJDY: 55–56, 66–68, 151 **ODNIESIENIE:** KSC rozdział dotyczący nadzoru; ISO/IEC 27001:2022, 9.1–9.2 **CHARAKTER:** PRAWO + NORMA

058. Czym różni się audyt pierwszej, drugiej i trzeciej strony?

Pierwsza strona to audyt wewnętrzny własnej organizacji. Druga strona to np. ocena dostawcy przez klienta. Trzecia strona to niezależna ocena zewnętrzna, np. certyfikacyjna. Audyt ustawowy KSC ma własną podstawę i wymagania — nie utożsamiaj go automatycznie z certyfikacją ISO.

SLAJDY: 57–58 **ODNIESIENIE:** ISO 19011:2026; KSC art. 15 **CHARAKTER:** NORMA + PRAWO

059. Czy audyt ISO 27001 może zastąpić audyt KSC?

Nie należy tego zakładać. Zakres, kryteria, kompetencje audytorów i wymagania formalne mogą być różne. Wyniki certyfikacji i audytów wewnętrznych mogą pomóc przygotować dowody, ale o spełnieniu obowiązku z art. 15 rozstrzygają jego własne przepisy.

SLAJDY: 57–58, 68 **ODNIESIENIE:** KSC art. 15; ISO/IEC 27001:2022, 9.2 **CHARAKTER:** PRAWO + NORMA

060. Czy audytor powinien być niezależny?

Tak w zakresie wymaganym przez konkretny rodzaj audytu. W audycie wewnętrznym ważna jest bezstronność i unikanie audytowania własnej pracy; w audycie ustawowym i certyfikacyjnym trzeba spełnić odrębne wymagania. Sam tytuł „audytor” nie zastępuje sprawdzenia kompetencji.

SLAJDY: 57–58 **ODNIESIENIE:** ISO 19011:2026; KSC art. 15; ISO/IEC 27001:2022, 9.2 **CHARAKTER:** NORMA + PRAWO

061. Jak przygotować organizację do kontroli lub audytu?

Zebrać mapę obowiązków, zakres systemu, rejestry ryzyk, plan działań, SoA, umowy z dostawcami, raporty z incydentów, testy odtwarzania, szkolenia i dowody przeglądów. Zespół powinien umieć pokazać nie tylko dokument, ale konkretną próbkę działania.

SLAJDY: 56–59, 66–69, 151 **ODNIESIENIE:** KSC art. 8 i 15; ISO/IEC 27001:2022, 9.1–9.3 **CHARAKTER:** PRAWO + NORMA

06. SZBI, ISO 27001, zabezpieczenia i dowody

Pytania o zakres, dokumentację, SoA i to, po czym poznajemy, że system działa.

062. Co oznacza SZBI w praktyce?

To uporządkowany sposób określania odpowiedzialności, identyfikowania ryzyk, wdrażania zabezpieczeń, sprawdzania ich skuteczności i doskonalenia. Dokumentacja jest ważna, ale nie zastępuje decyzji, działania i dowodów.

SLAJDY: 60–61, 64–68 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001:2022, klauzule 4–10 **CHARAKTER:** PRAWO + NORMA

063. Od czego zacząć określanie zakresu SZBI?

Od usług, procesów i danych, które trzeba chronić, a następnie zmapować systemy, ludzi, lokalizacje i dostawców, od których zależą te usługi. Zakres powinien być uzasadniony i spójny z obowiązkami prawnymi oraz realnymi zależnościami.

SLAJDY: 60–63 **ODNIESIENIE:** ISO/IEC 27001:2022, 4.1–4.4; KSC art. 8 **CHARAKTER:** NORMA + PRAWO

064. Czy można wyłączyć niewygodny system z zakresu SZBI?

Nie należy robić tego arbitralnie, aby uniknąć oceny ryzyka. Granice muszą mieć logiczne uzasadnienie i uwzględniać zależności z procesami krytycznymi oraz obowiązkami ustawowymi. Jeśli system wspiera usługę objętą zakresem, wyłączenie wymaga szczególnej analizy.

SLAJDY: 62–63, 77 **ODNIESIENIE:** ISO/IEC 27001:2022, 4.3; KSC art. 8 **CHARAKTER:** NORMA + PRAWO

065. Co jest ważniejsze: polityka bezpieczeństwa czy praktyka?

Obie rzeczy są potrzebne, ale polityka bez wdrożenia nie daje ochrony. Dobrze pokazać łańcuch: wymaganie → właściciel → działanie → test → wynik → decyzja korygująca. Audytor powinien poszukiwać dowodu, nie samej deklaracji.

SLAJDY: 64–68, 75 **ODNIESIENIE:** ISO/IEC 27001:2022, 7.5, 8–10 **CHARAKTER:** NORMA

066. Czym różni się dokumentacja normatywna od operacyjnej?

Normatywna określa, jak organizacja ma działać — polityki, zasady, procedury. Operacyjna potwierdza, co faktycznie zrobiono — logi, rejestry, protokoły testów, raporty, decyzje i działania po incydencie. Dwa rodzaje dokumentacji powinny być spójne.

SLAJDY: 66–68 **ODNIESIENIE:** KSC przepisy o dokumentacji; ISO/IEC 27001:2022, 7.5 **CHARAKTER:** PRAWO + NORMA

067. Czy trzeba tworzyć osobne procedury „pod KSC” i osobne „pod ISO”?

Nie ma sensu dublować dokumentów tylko dlatego, że pochodzą z dwóch źródeł wymagań. Warto stosować jedną procedurę i macierz mapowania, która pokazuje, jakie obowiązki prawne i wymagania normy realizuje oraz jakie dowody powstają.

SLAJDY: 41, 66–69, 77, 140 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001:2022 **CHARAKTER:** PRAWO + NORMA

068. Co to jest SoA?

Deklaracja Stosowania to uzasadniony wykaz niezbędnych zabezpieczeń oraz informacji o tym, dlaczego są przyjęte i czy zostały wdrożone, z uzasadnieniem wyłączeń z referencyjnego załącznika A. Nie jest to tabela, w której najlepiej zaznaczyć wszędzie „TAK".

SLAJDY: 69–70, 144 **ODNIESIENIE:** ISO/IEC 27001:2022, 6.1.3 d) **CHARAKTER:** NORMA

069. Czy ISO 27001 wymaga wdrożenia wszystkich 93 zabezpieczeń?

Nie. Załącznik A to zestaw referencyjny do porównania z potrzebnymi zabezpieczeniami. Dobór wynika z oceny i postępowania z ryzykiem oraz wymagań prawnych i umownych. Trzeba jednak uzasadnić, dlaczego poszczególne zabezpieczenia stosujemy lub wyłączamy.

SLAJDY: 69–70, 98 **ODNIESIENIE:** ISO/IEC 27001:2022, 6.1.3 i załącznik A **CHARAKTER:** NORMA

070. Czy zakup drogiego rozwiązania wystarczy, aby ograniczyć ryzyko?

Nie. Sam zakup nie dowodzi skuteczności. Potrzebne są wdrożenie, właściwe ustawienia, przydzielenie odpowiedzialności, szkolenia, monitoring i test. Mierzymy osiągnięty efekt, nie wysokość faktury.

SLAJDY: 42–43, 69–70, 75, 98 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001:2022, 9.1 **CHARAKTER:** PRAWO + NORMA

071. Czy firewall, MFA i szyfrowanie są zawsze obowiązkowe w identycznej konfiguracji?

Prawo co do zasady wymaga środków adekwatnych i proporcjonalnych do ryzyka oraz określa pewne obszary zabezpieczeń. Konkretną konfigurację dobiera się do usługi, ekspozycji i ewentualnych szczególnych przepisów. Nie można obiecywać zgodności przez zakup jednej technologii.

SLAJDY: 39–43, 70, 74 **ODNIESIENIE:** NIS2 art. 21; KSC art. 8; akty sektorowe **CHARAKTER:** PRAWO + PRAKTYKA

072. Jak ocenić skuteczność zabezpieczenia?

Ustalić cel, metodę testu, próg akceptacji, osobę odpowiedzialną i dowód. Przykładowo: backup jest skuteczny, jeśli da się odtworzyć krytyczną usługę w czasie wymaganym przez biznes, a nie tylko wtedy, gdy system pokazuje „OK".

SLAJDY: 68, 75, 129–131 **ODNIESIENIE:** ISO/IEC 27001:2022, 9.1; KSC art. 8 **CHARAKTER:** NORMA + PRAWO

073. Czym jest przegląd zarządzania?

To okresowa ocena, czy SZBI jest właściwy, skuteczny i adekwatny. Powinien obejmować wyniki pomiarów, audytów, zmiany ryzyk, incydenty, dostawców, zasoby oraz decyzje o doskonaleniu. Nie chodzi wyłącznie o prezentację statusu projektu.

SLAJDY: 76, 99–101 **ODNIESIENIE:** ISO/IEC 27001:2022, 9.3 **CHARAKTER:** NORMA

074. Czy brak incydentów oznacza skuteczny SZBI?

Nie. Może oznaczać dobrą ochronę, ale także słabe wykrywanie i brak zgłoszeń. Dlatego należy badać procesy, testy, niezależne audyty, podatności i wyniki ćwiczeń, zamiast opierać ocenę na samym liczniku incydentów.

SLAJDY: 68, 75–76, 102–103 **ODNIESIENIE:** ISO/IEC 27001:2022, 9.1–9.2 **CHARAKTER:** NORMA + PRAKTYKA

075. Czy polityka sprzed dwóch lat jest z automatu nieważna?

Nie. Istotna jest aktualność, adekwatność i stosowanie. Jeśli zmieniły się usługi, technologia, zagrożenia lub prawo, polityka wymaga przeglądu i ewentualnej aktualizacji. Data dokumentu jest sygnałem do weryfikacji, nie jedynym kryterium.

SLAJDY: 64, 66–68, 150 **ODNIESIENIE:** ISO/IEC 27001:2022, 7.5 i 10 **CHARAKTER:** NORMA

07. Zarządzanie ryzykiem, ERM, RACI i raportowanie

Najbardziej oczekiwany obszar szkolenia: wspólna logika ryzyka technologicznego i biznesowego.

076. Dlaczego ryzyko cyberbezpieczeństwa nie powinno być tylko „ryzykiem IT”?

Bo jego skutki dotyczą usług, klientów, przychodów, bezpieczeństwa ludzi i reputacji. Informatyk ocenia przyczyny i możliwe środki techniczne, ale właściciel procesu określa wpływ na działalność, a uprawnione kierownictwo podejmuje decyzje.

SLAJDY: 78–83, 90 **ODNIESIENIE:** ISO 31000:2018; ISO/IEC 27001:2022, 6.1.2 **CHARAKTER:** NORMA + PRAKTYKA

077. Co to jest ERM i jak łączy się z SZBI?

ERM to całościowe zarządzanie ryzykiem przedsiębiorstwa. SZBI dostarcza scenariusze ryzyka bezpieczeństwa informacji, ocenę zabezpieczeń, incydenty i wskaźniki. Oba systemy powinny korzystać ze wspólnych kategorii skutku oraz jednej ścieżki decyzji i eskalacji.

SLAJDY: 78–80, 84–89 **ODNIESIENIE:** ISO 31000:2018; ISO/IEC 27005:2022 **CHARAKTER:** NORMA

078. Czy firma może prowadzić dwa rejestry ryzyka?

Może, jeśli różne rejestry mają różną szczegółowość, ale muszą być powiązane identyfikatorami, właścicielami i wspólną oceną skutku. Nie powinny prowadzić do dwóch sprzecznych decyzji o tym samym ryzyku. Dobrym modelem jest jedna karta źródłowa i różne widoki raportowe.

SLAJDY: 79, 84, 87–89 **ODNIESIENIE:** ISO 31000; ISO/IEC 27005; model wdrożeniowy **CHARAKTER:** PRAKTYKA

079. Co jest dobrym opisem ryzyka?

Opis scenariuszowy: „Jeżeli dostawca ERP będzie niedostępny przez 24 godziny, nie zrealizujemy wysyłek i narazimy się na kary umowne”. Powinien zawierać przyczynę, zdarzenie, skutek biznesowy, proces i właściciela. Samo hasło „ransomware – 20 pkt” to za mało.

SLAJDY: 80, 84–85, 94–95 **ODNIESIENIE:** ISO/IEC 27005:2022; praktyka analizy ryzyka **CHARAKTER:** NORMA + PRAKTYKA

080. Kto jest właścicielem ryzyka: CISO, IT czy właściciel procesu?

Zasadniczo właściciel ryzyka powinien mieć mandat do decydowania o konsekwencjach biznesowych i działaniach. Komórka SZBI koordynuje metodykę, a IT dostarcza dane techniczne i realizuje środki. Przy ryzykach międzyprocesowych trzeba wyznaczyć właściciela przekrojowego.

SLAJDY: 81–83, 97 **ODNIESIENIE:** ISO/IEC 27001:2022, 6.1.2; praktyka RACI **CHARAKTER:** NORMA + PRAKTYKA

081. Czy komórka SZBI może sama akceptować ryzyka biznesowe?

Tylko w granicach formalnie nadanych uprawnień, co w przypadku ryzyk biznesowych zwykle jest niewłaściwe. Jej rolą jest analiza, rekomendacja i monitoring. Akceptacja skutków dla przychodów, usług lub zgodności powinna należeć do uprawnionego właściciela ryzyka.

SLAJDY: 81–83, 92–93 **ODNIESIENIE:** ISO/IEC 27001:2022, 6.1.3; praktyka ERM **CHARAKTER:** NORMA + PRAKTYKA

082. Co oznacza RACI i czy jest wymagane przez ISO 27001?

RACI to pomocnicza macierz: kto wykonuje, kto odpowiada za wynik, kogo konsultujemy i kogo informujemy. Sama macierz RACI nie jest jedynym obowiązkowym formularzem normy, ale bardzo pomaga wykazać jasny podział ról i uniknąć sytuacji „wszyscy odpowiadają, czyli nikt".

SLAJDY: 65, 82–83 **ODNIESIENIE:** ISO/IEC 27001:2022, 5.3; dobra praktyka RACI **CHARAKTER:** NORMA + PRAKTYKA

083. Czy musimy stosować macierz 5 × 5?

Nie. Ani ISO 27001, ani KSC nie wymagają jednej uniwersalnej macierzy 5 × 5. Metodyka ma być powtarzalna, zrozumiała i adekwatna. W szkoleniu stosujemy przykłady skal, które organizacja musi skalibrować do własnych skutków i apetytu na ryzyko.

SLAJDY: 85–86, 94–95 **ODNIESIENIE:** ISO/IEC 27001:2022, 6.1.2; ISO/IEC 27005 **CHARAKTER:** NORMA

084. Jak ustalić prawdopodobieństwo, gdy nie mamy danych statystycznych?

Stosować uporządkowaną ocenę ekspercką na podstawie zagrożeń, ekspozycji, podatności, historii zdarzeń, skuteczności kontroli i zależności od dostawców. Trzeba zapisać założenia i poziom niepewności, a następnie aktualizować ocenę po testach i incydentach.

SLAJDY: 84–86, 91, 95 **ODNIESIENIE:** ISO/IEC 27005:2022; praktyka oceny scenariuszy **CHARAKTER:** NORMA + PRAKTYKA

085. Co jeśli biznes i IT zupełnie inaczej oceniają to samo ryzyko?

Najpierw porównajmy założenia: IT może oceniać szansę ataku, a biznes koszt niedostępności usługi. Uzgodnijmy jeden scenariusz, wspólną skalę skutku i źródła danych. Różnice należy udokumentować i rozstrzygnąć w procesie decyzyjnym, nie usuwać przez uśrednienie.

SLAJDY: 78–80, 85–89 **ODNIESIENIE:** ISO 31000; ISO/IEC 27005 **CHARAKTER:** NORMA + PRAKTYKA

086. Co to jest ryzyko inherentne, rezydualne i docelowe?

Inherentne opisuje ekspozycję przed uwzględnieniem analizowanych zabezpieczeń; rezydualne to ryzyko pozostające po obecnych środkach; docelowe to poziom, do którego chcemy dojść po planowanych działaniach. Trzeba jasno ustalić definicje w metodyce, aby nie mieszać liczb.

SLAJDY: 91, 94–95 **ODNIESIENIE:** ISO/IEC 27005:2022; praktyka metodyczna **CHARAKTER:** NORMA + PRAKTYKA

087. Co oznacza apetyt na ryzyko?

To poziom i rodzaj ryzyka, jakie organizacja jest gotowa podejmować w realizacji celów. W praktyce zarząd przekłada go na konkretne granice: np. dopuszczalny czas przestoju, kwotę straty albo maksymalny udział procesów bez sprawdzonych planów ciągłości.

SLAJDY: 86, 92–93 **ODNIESIENIE:** ISO 31000:2018; praktyka ERM **CHARAKTER:** NORMA + PRAKTYKA

088. Czy ryzyko wysokie zawsze trzeba natychmiast usunąć?

Nie każde można wyeliminować, ale nie wolno go ignorować. Powinno mieć właściciela, pilną decyzję, właściwe środki, termin i monitoring. Ryzyko poza tolerancją trzeba eskalować zgodnie z uprawnieniami, zwłaszcza gdy narusza wymagania prawne.

SLAJDY: 90–95, 98 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001:2022, 6.1.3 **CHARAKTER:** PRAWO + NORMA

089. Jak zagregować 80 ryzyk SZBI do jednego raportu ERM?

Nie sumować bezmyślnie punktów. Grupować ryzyka według wspólnych procesów, scenariuszy, zależności i konsekwencji, wskazać ryzyka przekraczające tolerancję oraz ekspozycję na pojedyncze punkty awarii. Do zarządu powinny trafić informacje o realnych decyzjach.

SLAJDY: 87–90, 99–101 **ODNIESIENIE:** ISO 31000; ISO/IEC 27005; praktyka raportowania **CHARAKTER:** PRAKTYKA

090. Jak nie liczyć dwa razy tej samej szkody?

Wskazać wspólną przyczynę i scenariusz. Jeżeli awaria jednego centrum danych zatrzymuje produkcję, magazyn i fakturowanie, nie należy mechanicznie sumować trzech pełnych strat bez ustalenia zależności. W raporcie pokazać łączny efekt oraz procesy składowe.

SLAJDY: 87–89, 96–97 **ODNIESIENIE:** ISO 31000; praktyka agregacji ryzyka **CHARAKTER:** PRAKTYKA

091. Co zrobić z ryzykiem, które dotyczy kilku działów?

Wyznaczyć jednego właściciela odpowiedzialnego za całość oraz osoby odpowiedzialne za działania w poszczególnych procesach. RACI pomoże rozstrzygnąć, kto decyduje o budżecie i kompromisach. Bez właściciela przekrojowego ryzyko może zniknąć między działami.

SLAJDY: 82–83, 96–97 **ODNIESIENIE:** ISO/IEC 27001:2022, 5.3; praktyka ERM **CHARAKTER:** NORMA + PRAKTYKA

092. Co musi zawierać dobra karta ryzyka?

Co najmniej: identyfikator, scenariusz, proces, przyczynę, skutek, właściciela, ocenę, istniejące zabezpieczenia, decyzję, plan działań, ryzyko rezydualne, termin przeglądu i wskaźnik monitorowania. Przykład 15 pól na slajdzie jest propozycją praktyczną, nie obowiązkowym wzorem ustawowym.

SLAJDY: 89, 94–95 **ODNIESIENIE:** ISO/IEC 27001:2022, 6.1.2–6.1.3; praktyka **CHARAKTER:** NORMA + PRAKTYKA

093. Czy prezes może zatwierdzić ryzyko bez żadnej analizy?

Nie jest to dobra praktyka ani rzetelna realizacja procesu zarządzania ryzykiem. Decyzja powinna opierać się na opisie scenariusza, konsekwencjach, zabezpieczeniach, alternatywach i poziomie ryzyka rezydualnego. Podpis nie zastępuje podstaw decyzyjnych.

SLAJDY: 92–95, 99 **ODNIESIENIE:** ISO/IEC 27001:2022, 6.1.2–6.1.3; KSC art. 8 **CHARAKTER:** PRAWO + NORMA

094. Czym różni się KPI od KRI?

KPI mierzy wykonanie i skuteczność działań, a KRI sygnalizuje zmianę ekspozycji na ryzyko. Liczba przeszkolonych osób jest raczej wskaźnikiem realizacji; rosnący udział nieodtworzonych kopii albo narastające przestoje dostawcy mogą być KRI.

SLAJDY: 99–103 **ODNIESIENIE:** ISO/IEC 27001:2022, 9.1; praktyka ERM **CHARAKTER:** NORMA + PRAKTYKA

095. Jak ustalić wartości progowe KRI?

Powiązać wskaźnik z konkretnym ryzykiem i apetytem na ryzyko. Ustalić, co oznacza poziom normalny, ostrzegawczy i krytyczny, kto reaguje oraz jakie decyzje są wymagane. Progi należy sprawdzić w praktyce; nie są uniwersalnymi wartościami ISO czy KSC.

SLAJDY: 92, 102–103 **ODNIESIENIE:** ISO 31000; ISO/IEC 27001:2022, 9.1; praktyka **CHARAKTER:** NORMA + PRAKTYKA

096. Czy jedno naruszenie bezpieczeństwa zawsze zmienia ocenę ryzyka?

Nie zawsze. Należy sprawdzić, czy incydent ujawnił błędne założenia o prawdopodobieństwie, skutkach lub zabezpieczeniach. Jeśli tak, rejestr ryzyk i plan postępowania należy zaktualizować. Ważniejsza od samego faktu incydentu jest zmiana wiedzy o ekspozycji.

SLAJDY: 104–107, 127–128 **ODNIESIENIE:** ISO/IEC 27001:2022, 8.2–8.3, 10; praktyka **CHARAKTER:** NORMA + PRAKTYKA

097. Kiedy incydent cyber powinien trafić również do ERM?

Gdy materializuje lub istotnie zmienia ryzyko biznesowe: zatrzymuje krytyczny proces, grozi stratą, odpowiedzialnością, naruszeniem umów lub reputacji. Warto ustalić z góry progi eskalacji, zamiast czekać, aż zdarzenie zostanie wyłącznie „zamknięte w systemie ticketowym".

SLAJDY: 104–107, 127–128 **ODNIESIENIE:** ISO 31000; ISO/IEC 27001:2022, 8–10; model wdrożeniowy **CHARAKTER:** PRAKTYKA

098. Co pokazać zarządowi zamiast stu technicznych wskaźników?

Pięć–sześć istotnych decyzji: jakie usługi i przychody są zagrożone, jakie ryzyka są poza tolerancją, gdzie brakuje dowodów skuteczności, jaki jest koszt przestoju, które działania wymagają zasobów i kto ma je zatwierdzić. Dane techniczne pozostają w załączniku.

SLAJDY: 90, 99–103, 138 **ODNIESIENIE:** ISO/IEC 27001:2022, 9.1 i 9.3; praktyka raportowania **CHARAKTER:** NORMA + PRAKTYKA

08. Dostawcy, umowy NDA, SLA i outsourcing

Zależność od dostawcy jest ryzykiem przedsiębiorstwa, nawet gdy systemy działają poza firmą.

099. Dlaczego dostawca ICT jest częścią naszego ryzyka?

Bo przeniesienie obsługi technologii nie przenosi całego skutku biznesowego awarii. Gdy dostawca zatrzyma ERP lub chmurę, to nasza organizacja traci zdolność świadczenia usługi. Dlatego ocenia się zależność, umowę, ciągłość i możliwość zastąpienia dostawcy.

SLAJDY: 109–113, 120 **ODNIESIENIE:** NIS2 art. 21; KSC art. 8; ISO/IEC 27001 A.5.19–A.5.23 **CHARAKTER:** PRAWO + NORMA

100. Czy każdy dostawca musi mieć ISO 27001?

Nie ma uniwersalnego ustawowego wymogu certyfikowania wszystkich dostawców. Należy dobrać wymagania proporcjonalnie do krytyczności usługi i ryzyka. Certyfikat może być jednym z dowodów, ale trzeba zweryfikować zakres, datę i to, czy obejmuje faktycznie kupowaną usługę.

SLAJDY: 110–113 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001 A.5.19–A.5.23 **CHARAKTER:** PRAWO + NORMA

101. Jak rozpoznać dostawcę krytycznego?

Zadać pytania: który proces zatrzyma jego niedostępność, jak szybko pojawi się szkoda, czy mamy alternatywę i dostęp do danych, czy dostawca ma dostęp uprzywilejowany oraz czy zależymy od jego podwykonawców. Klasyfikacja powinna wynikać z BIA i ryzyka.

SLAJDY: 109, 112–113, 119 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001 A.5.19–A.5.23; ISO 22301 **CHARAKTER:** PRAWO + NORMA

102. Czy ankieta bezpieczeństwa dostawcy wystarczy?

Nie. Sama deklaracja może być nieaktualna lub ogólna. W przypadku usług krytycznych warto badać konkretne dowody: testy odtwarzania, wyniki audytów, zakres certyfikatu, proces incydentowy i uprawnienia dostępu. Zakres dowodów powinien być proporcjonalny do ryzyka.

SLAJDY: 112–114 **ODNIESIENIE:** ISO/IEC 27001 A.5.19–A.5.22; praktyka due diligence **CHARAKTER:** NORMA + PRAKTYKA

103. Jakie klauzule bezpieczeństwa powinny być w umowie z dostawcą?

Minimum do rozważenia: zakres usług i danych, uprawnienia, wymagania zabezpieczeń, terminy powiadomień o incydentach, podwykonawcy, audyty lub dowody, parametry dostępności, odtwarzanie, zakończenie usługi i usunięcie danych. Nie każda klauzula ma tę samą wagę dla każdego dostawcy.

SLAJDY: 113–115, 119 **ODNIESIENIE:** ISO/IEC 27001 A.5.20–A.5.23; KSC art. 8 **CHARAKTER:** PRAWO + NORMA

104. Czy NDA wystarczy do ochrony informacji poufnych?

Nie. NDA tworzy zobowiązania umowne, ale nie zastępuje kontroli dostępu, klasyfikacji informacji, nadzoru nad udostępnianiem, monitoringu i odebrania uprawnień po zakończeniu współpracy. Ważna jest wykonalna treść umowy i praktyka jej stosowania.

SLAJDY: 114–115 **ODNIESIENIE:** ISO/IEC 27001 A.6.6, A.5.20; prawo umów **CHARAKTER:** NORMA + PRAWO

105. Czym różni się NDA od umowy powierzenia danych?

NDA reguluje poufność informacji. Umowa powierzenia z art. 28 RODO dotyczy relacji administrator–podmiot przetwarzający dane osobowe i zawiera specyficzne wymogi. W jednej relacji obie umowy mogą być potrzebne, ale nie są zamienne.

SLAJDY: 114–115, 137 **ODNIESIENIE:** RODO art. 28; ISO/IEC 27001 A.6.6 **CHARAKTER:** PRAWO + NORMA

106. Czy SLA 99,9% oznacza, że firma ma zapewnioną ciągłość działania?

Nie. SLA opisuje uzgodniony parametr dostawcy, ale nie musi odpowiadać tolerowanemu czasowi przerwy procesu, RTO lub RPO. Trzeba też sprawdzić wyłączenia, sposób liczenia dostępności, reakcję na incydent i możliwość faktycznego odtworzenia usługi.

SLAJDY: 114, 119, 129–131 **ODNIESIENIE:** ISO 22301; ISO/IEC 27001 A.5.20–A.5.23 **CHARAKTER:** NORMA + PRAKTYKA

107. Kto odpowiada za bezpieczeństwo danych w chmurze?

Odpowiedzialność jest współdzielona zgodnie z modelem i umową. Dostawca może odpowiadać za część infrastruktury, lecz organizacja nadal odpowiada za konfigurację, uprawnienia, dane, kopie i decyzje w swoim zakresie. Należy sporządzić matrycę odpowiedzialności.

SLAJDY: 116–118 **ODNIESIENIE:** ISO/IEC 27001 A.5.23; KSC art. 8; umowa dostawcy **CHARAKTER:** PRAWO + NORMA

108. Czy możemy zlecić obsługę incydentów na zewnątrz?

Co do zasady można korzystać z usług zewnętrznych, ale trzeba ustalić odpowiedzialności, pełnomocnictwa, terminy raportowania i zapewnić dostępność zespołu. Outsourcing nie znosi własnych obowiązków podmiotu i nadzoru kierownictwa.

SLAJDY: 44–47, 109–114, 121–126 **ODNIESIENIE:** KSC art. 8, 8c, 11; MC FAQ 3.17 **CHARAKTER:** PRAWO

109. Jak traktować podwykonawców dostawcy?

Nie zatrzymywać oceny na pierwszym kontrahencie. Dla usług krytycznych trzeba rozumieć istotne zależności dalszych ogniw, lokalizacje przetwarzania, dostęp do danych, zasady zmian i sposoby informowania o incydentach. Warto powiązać je z planem wyjścia.

SLAJDY: 116–119 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001 A.5.21–A.5.23 **CHARAKTER:** PRAWO + NORMA

110. Czym różni się „dostawca krytyczny” od formalnego dostawcy wysokiego ryzyka?

„Krytyczny” to zwykle wewnętrzna ocena zależności biznesowej. Formalny status dostawcy wysokiego ryzyka może wynikać z odrębnego mechanizmu prawnego KSC. Nie wolno utożsamiać tych kategorii ani samodzielnie nadawać dostawcy skutków prawnych takiego statusu.

SLAJDY: 112, 117 **ODNIESIENIE:** KSC przepisy o dostawcach wysokiego ryzyka; praktyka klasyfikacji **CHARAKTER:** PRAWO + PRAKTYKA

111. Czym jest exit plan?

To plan zakończenia lub zastąpienia usługi bez utraty zdolności działania: eksport danych, przeniesienie konfiguracji, odzyskanie dostępu, test alternatywy, odbiór uprawnień i potwierdzenie usunięcia danych u starego dostawcy. Szczególnie ważny przy chmurze i ERP.

SLAJDY: 118–120 **ODNIESIENIE:** ISO/IEC 27001 A.5.22–A.5.23; ISO 22301 **CHARAKTER:** NORMA + PRAKTYKA

09. Człowiek, socjotechnika i programy antyphishingowe

Pytania z życia: Urząd Skarbowy, szkolenia personelu i budowanie odporności na manipulację.

112. Czy człowiek naprawdę jest „najsłabszym ogniwem”?

To przydatna metafora, ale zbyt uproszczona. Błędy ludzkie zależą od presji, projektu procesów i zabezpieczeń. Dojrzała organizacja ułatwia bezpieczne decyzje, tworzy kanały zgłaszania i projektuje kontrole tak, aby jedna pomyłka nie prowadziła do katastrofy.

SLAJDY: 71–74 **ODNIESIENIE:** ISO/IEC 27001 A.6.3 i A.6.8; praktyka ochrony warstwowej **CHARAKTER:** NORMA + PRAKTYKA

113. Dlaczego oszuści podszywają się pod Urząd Skarbowy?

Wykorzystują autorytet instytucji, presję czasu i obawę przed konsekwencjami. Celem jest nakłonienie odbiorcy do kliknięcia, podania danych lub wykonania płatności. Uczymy weryfikowania żądań niezależnym kanałem, a nie automatycznego zaufania do logotypu i nadawcy.

SLAJDY: 71–72 **ODNIESIENIE:** ISO/IEC 27001 A.6.3; dobre praktyki antyphishingowe **CHARAKTER:** PRAKTYKA

114. Co powinien zrobić pracownik po kliknięciu podejrzanego linku?

Nie ukrywać zdarzenia: jak najszybciej zgłosić je do właściwego kanału, nie kontynuować podawania danych, zastosować zalecenia zespołu bezpieczeństwa i zachować informacje o wiadomości. O szybkim ograniczeniu skutków decyduje procedura, nie szukanie winnego.

SLAJDY: 71–74, 121, 125 **ODNIESIENIE:** KSC art. 8 i obsługa incydentów; ISO/IEC 27001 A.6.8 **CHARAKTER:** PRAWO + PRAKTYKA

115. Czy symulacje phishingu są obowiązkowe dla każdej firmy?

Nie ma jednej uniwersalnej ustawowej formy symulacji dla wszystkich podmiotów. Należy zapewnić adekwatne szkolenia i działania budujące świadomość; symulacje są jednym ze sposobów sprawdzenia skuteczności, obok testów procesów, procedur i praktycznych ćwiczeń.

SLAJDY: 71–74 **ODNIESIENIE:** KSC art. 8; NIS2 art. 21; ISO/IEC 27001 A.6.3 **CHARAKTER:** PRAWO + NORMA

116. Jakie narzędzia pomagają walczyć z phishingiem?

Rozwiązania ochrony poczty, filtrowanie zagrożeń, MFA, SPF/DKIM/DMARC, zgłaszanie podejrzanych wiadomości i platformy szkoleniowe. Przykładowe produkty omawiane na slajdzie 73 nie zastępują procedur, szkoleń i monitorowania efektu.

SLAJDY: 73–74 **ODNIESIENIE:** ISO/IEC 27001 A.5, A.6, A.8; praktyka branżowa **CHARAKTER:** NORMA + PRAKTYKA

117. Czy MFA całkowicie eliminuje phishing?

Nie. Znacznie utrudnia część ataków, ale nie usuwa np. oszustw płatniczych, manipulacji telefonicznej czy prób przejęcia sesji. Potrzebne są warstwy ochrony i bezpieczne procesy weryfikacji wrażliwych decyzji.

SLAJDY: 72–74 **ODNIESIENIE:** NIS2 art. 21; KSC art. 8; dobra praktyka **CHARAKTER:** PRAWO + PRAKTYKA

118. Czy pracownik, który dał się oszukać, powinien być ukarany?

Najpierw trzeba ustalić fakty, wpływ organizacji na warunki pracy i skuteczność kontroli. Automatyczna kultura karania może zniechęcić do szybkiego zgłaszania incydentów. Ewentualna odpowiedzialność pracownicza wymaga odrębnej oceny prawnej i konkretnych okoliczności.

SLAJDY: 71–74, 125 **ODNIESIENIE:** Praktyka zarządzania incydentami; właściwe przepisy prawa pracy **CHARAKTER:** PRAKTYKA

119. Jak sprawdzać skuteczność szkoleń antyphishingowych?

Nie tylko liczbą uczestników. Warto mierzyć odsetek zgłoszeń podejrzanych wiadomości, czas zgłoszenia, efekty symulacji, powtarzalność błędów i gotowość przełożonych do reakcji. Wynik należy analizować z uwzględnieniem kontekstu, nie jako wyścig do zera kliknięć.

SLAJDY: 73–75, 102–103 **ODNIESIENIE:** ISO/IEC 27001:2022, 9.1; A.6.3 **CHARAKTER:** NORMA + PRAKTYKA

120. Czy zabezpieczenia techniczne są ważniejsze od szkoleń?

To fałszywa alternatywa. System jest skuteczny, gdy technologia, proces i zachowania personelu wzajemnie się uzupełniają. Przykład: pracownik może rozpoznać oszustwo, ale organizacja i tak powinna mieć niezależny proces potwierdzania zmian rachunków bankowych.

SLAJDY: 71–75 **ODNIESIENIE:** ISO/IEC 27001:2022, klauzule 7–8 i załącznik A **CHARAKTER:** NORMA

10. Incydenty, zgłoszenia CSIRT, S46 oraz RODO

Co robić pod presją czasu, jak klasyfikować zdarzenia i nie przegapić terminów.

121. Czym różni się zdarzenie od incydentu?

Zdarzenie to obserwowany sygnał, który wymaga oceny; incydent dotyczy naruszenia lub zagrożenia bezpieczeństwa systemu/usługi w rozumieniu właściwych definicji. Nie każdy alarm z monitoringu staje się incydentem, a nie każdy incydent jest „poważny”.

SLAJDY: 121, 125 **ODNIESIENIE:** KSC definicje ustawowe; ISO/IEC 27001 A.5.24–A.5.28 **CHARAKTER:** PRAWO + NORMA

122. Czy każdy incydent trzeba zgłaszać do CSIRT?

Nie każdemu incydentowi odpowiada ten sam obowiązek raportowy. W KSC kluczowa jest prawidłowa kwalifikacja incydentu poważnego zgodnie z właściwymi kryteriami; określone informacje można również przekazywać dobrowolnie w przewidzianych trybach.

SLAJDY: 121–124 **ODNIESIENIE:** KSC art. 11 i nast.; MC FAQ 6.1–6.10 **CHARAKTER:** PRAWO

123. Kiedy zaczyna się termin 24 godzin?

Co do zasady od wykrycia incydentu poważnego w rozumieniu właściwych przepisów. Procedura powinna jasno określać rejestrowanie momentu wykrycia i kwalifikacji; nie wolno czekać na pełną analizę przyczyn, jeśli obowiązek wczesnego ostrzeżenia już powstał.

SLAJDY: 122–126 **ODNIESIENIE:** KSC art. 11 i nast.; S46 „Zgłoszenie incydentu" **CHARAKTER:** PRAWO

124. Co należy wysłać w 24 godziny?

Wczesne ostrzeżenie: podstawowe dostępne fakty o incydencie i możliwych skutkach, w tym informacje o potencjalnym działaniu bezprawnym lub wpływie transgranicznym, jeżeli są znane. Nie musi być jeszcze kompletne śledztwo techniczne.

SLAJDY: 122–124 **ODNIESIENIE:** KSC art. 11 i nast.; NIS2 art. 23 **CHARAKTER:** PRAWO

125. Co należy przekazać do 72 godzin?

Uzupełnione zgłoszenie z dokładniejszą oceną dotkliwości, wpływu na usługi, prawdopodobnych przyczyn, wskaźników kompromitacji i podjętych działań, w zakresie danych dostępnych w danym momencie. Obowiązuje właściwy tryb dla kategorii podmiotu.

SLAJDY: 122–124 **ODNIESIENIE:** KSC art. 11 i nast.; NIS2 art. 23; S46 **CHARAKTER:** PRAWO

126. Kiedy jest raport końcowy?

Co do zasady do miesiąca od zgłoszenia incydentu, zgodnie z właściwym reżimem. Jeżeli obsługa nadal trwa, przepisy mogą przewidywać raport postępu. Harmonogram należy mieć w procedurze i od razu przypisać osoby odpowiedzialne za kolejne terminy.

SLAJDY: 122–124 **ODNIESIENIE:** KSC art. 11 i nast.; NIS2 art. 23; S46 **CHARAKTER:** PRAWO

127. Co jeśli nie mamy wszystkich informacji do zgłoszenia?

Zgłaszamy dostępne, rzetelnie potwierdzone dane w terminie i później je uzupełniamy. Brak pełnej wiedzy o ataku nie jest argumentem za automatycznym odkładaniem wczesnego ostrzeżenia. Trzeba wyraźnie odróżniać fakty od hipotez.

SLAJDY: 122–125 **ODNIESIENIE:** KSC art. 11 i nast.; MC FAQ 6.15 **CHARAKTER:** PRAWO

128. Do którego CSIRT należy zgłosić incydent?

Do właściwego CSIRT sektorowego, a jeśli nie został wyznaczony dla danego podmiotu — według właściwości do zespołu poziomu krajowego. S46 wspiera wyznaczanie adresatów, ale organizacja powinna wcześniej ustalić własną ścieżkę i kanał awaryjny.

SLAJDY: 124–126 **ODNIESIENIE:** KSC i system S46; gov.pl „Zgłoszenie incydentu" **CHARAKTER:** PRAWO

129. Co jeśli S46 jest niedostępny podczas incydentu?

Należy skorzystać ze wskazanego przez właściwy CSIRT sposobu komunikacji zastępczej i zachować dowód czasu oraz treści zgłoszenia. Warto przetestować tę ścieżkę zawczasu, aby awaria narzędzia raportowego nie zatrzymała wykonania obowiązku.

SLAJDY: 125–126 **ODNIESIENIE:** KSC; gov.pl „Zgłoszenie incydentu" **CHARAKTER:** PRAWO + PRAKTYKA

130. Czy dostawca usług zaufania ma identyczne terminy co inni?

Nie we wszystkich etapach. Dla wybranych usług i kategorii podmiotów istnieją szczególne reguły, także w rozporządzeniach unijnych. Trzeba sprawdzić dokładną kategorię i jej przepisy, zamiast powtarzać jedną tabelę dla wszystkich.

SLAJDY: 121–124 **ODNIESIENIE:** KSC; NIS2 art. 23; rozporządzenie (UE) 2024/2690 **CHARAKTER:** PRAWO

131. Czy awaria ERP na 30 minut zawsze oznacza incydent poważny?

Nie. Należy przeanalizować rodzaj usługi, skutki, zakres i właściwe progi. Dla niektórych dostawców usług cyfrowych istnieją szczególne kryteria, ale nie wolno ich automatycznie przenosić na każdą wewnętrzną instalację ERP.

SLAJDY: 121–124, 129 **ODNIESIENIE:** KSC kryteria incydentów; rozporządzenie (UE) 2024/2690 w zakresie zastosowania **CHARAKTER:** PRAWO

132. Czy incydent związany z automatyką przemysłową (OT) podlega KSC?

Może podlegać, jeśli dotyczy systemów informacyjnych i usług objętych ustawą oraz spełnia kryteria raportowania. Nie ograniczamy cyberbezpieczeństwa do komputerów biurowych; skutkiem incydentu OT może być zatrzymanie produkcji lub zagrożenie dla ludzi.

SLAJDY: 121–126, 129 **ODNIESIENIE:** KSC definicje i art. 11; MC FAQ 6.6 **CHARAKTER:** PRAWO

133. Kiedy jednocześnie stosować KSC i RODO?

Gdy incydent spełnia właściwe przesłanki obu reżimów, np. narusza bezpieczeństwo usług i dane osobowe. Zgłoszenie CSIRT nie zastępuje automatycznie zgłoszenia organowi ochrony danych. Trzeba prowadzić odrębne kwalifikacje i terminy, koordynując jeden stan faktyczny.

SLAJDY: 121–124, 137 **ODNIESIENIE:** KSC art. 11 i nast.; RODO art. 33–34 **CHARAKTER:** PRAWO

134. Czy termin RODO 72 godziny jest tym samym co termin KSC 72 godziny?

Nie. Są to różne obowiązki, różni adresaci i odmienne punkty odniesienia. W RODO termin zgłoszenia naruszenia ochrony danych liczony jest od stwierdzenia naruszenia, z własnymi przesłankami; w KSC obowiązuje kwalifikacja incydentu poważnego.

SLAJDY: 122–124, 137 **ODNIESIENIE:** RODO art. 33; KSC art. 11 i nast. **CHARAKTER:** PRAWO

135. Kiedy poinformować zarząd o incydencie?

Nie czekać automatycznie na 72-godzinne zgłoszenie. Wewnętrzny próg eskalacji powinien zależeć od potencjalnego skutku dla usług, ludzi, finansów, zgodności i reputacji. Zarząd musi znać sytuację wtedy, gdy potrzebna jest jego decyzja.

SLAJDY: 104–107, 125, 127–128, 138 **ODNIESIENIE:** KSC art. 8c–8d; ISO/IEC 27001 A.5.24–A.5.28 **CHARAKTER:** PRAWO + NORMA

136. Jakie dowody należy zachować po incydencie?

Oś czasu, decyzje, logi i artefakty techniczne, kanały zgłoszeń, osoby odpowiedzialne, komunikaty, działania ograniczające skutki, wynik odtworzenia i wnioski po incydencie. Dowody muszą być zabezpieczone w sposób uwzględniający poufność i integralność.

SLAJDY: 125–128, 138–139 **ODNIESIENIE:** KSC art. 8 i 11; ISO/IEC 27001 A.5.24–A.5.28 **CHARAKTER:** PRAWO + NORMA

11. Ciągłość działania, ISO 22301, BIA i blackouty

Pytania o realną odporność organizacji na brak zasilania, danych, dostawcy i personelu.

137. Czym różni się backup od ciągłości działania?

Backup to sposób ochrony i odtworzenia danych. Ciągłość działania obejmuje zdolność utrzymania kluczowej usługi: ludzi, alternatywne procesy, zasilanie, łączność, lokalizację, dostawców i decyzje. Można mieć poprawną kopię, a mimo to nie potrafić obsłużyć klienta.

SLAJDY: 129–132 **ODNIESIENIE:** PN-EN ISO 22301; KSC art. 8; ISO/IEC 27001 A.5.29–A.5.30 **CHARAKTER:** NORMA + PRAWO

138. Co oznacza BIA?

Business Impact Analysis — analiza wpływu zakłócenia na działalność. Pomaga ustalić, które procesy trzeba przywrócić, jak szybko rośnie szkoda oraz jakie zasoby i zależności są niezbędne. BIA jest punktem wyjścia do celów odtworzenia, nie samą tabelą aktywów IT.

SLAJDY: 129–131 **ODNIESIENIE:** PN-EN ISO 22301; praktyka BCM **CHARAKTER:** NORMA

139. Czym różnią się RTO i RPO?

RTO opisuje docelowy czas przywrócenia usługi po zakłóceniu. RPO określa akceptowalną utratę danych wyrażoną w czasie. Przykładowo RTO cztery godziny i RPO piętnaście minut oznaczają dwa różne cele, które trzeba zweryfikować testami.

SLAJDY: 129–131 **ODNIESIENIE:** PN-EN ISO 22301; praktyka DR **CHARAKTER:** NORMA + PRAKTYKA

140. Czy ustawa narzuca każdemu przedsiębiorstwu RTO równe cztery godziny?

Nie. Takie parametry wyznacza się na podstawie BIA, umów, wymagań usług i szczególnych regulacji. Prezentacyjne liczby są przykładami, a nie uniwersalnym terminem KSC lub ISO 22301.

SLAJDY: 129–131 **ODNIESIENIE:** KSC art. 8; PN-EN ISO 22301 **CHARAKTER:** PRAWO + NORMA

141. Co jest ważniejsze: system dostępny czy proces działający?

Celem jest utrzymanie zdolności biznesowej na uzgodnionym poziomie. System informatyczny może działać, ale bez energii, personelu, łączności lub dostawcy usługa nadal będzie niedostępna. Dlatego testujemy nie tylko przywrócenie serwera, lecz cały proces.

SLAJDY: 129–132 **ODNIESIENIE:** PN-EN ISO 22301; ISO/IEC 27001 A.5.29–A.5.30 **CHARAKTER:** NORMA

142. Czy UPS zabezpiecza organizację przed blackoutem?

UPS pomaga przetrwać krótki brak zasilania lub bezpiecznie wyłączyć urządzenia. Nie gwarantuje ciągłości produkcji, dostaw, łączności i pracy ludzi podczas wielogodzinnego blackoutu. Potrzebna jest analiza zależności oraz realistyczne alternatywy.

SLAJDY: 132–136 **ODNIESIENIE:** PN-EN ISO 22301; praktyka odporności **CHARAKTER:** NORMA + PRAKTYKA

143. Czy blackout jest cyberatakiem?

Nie z definicji. Może wynikać z awarii sieci elektroenergetycznej, pogody, błędów operacyjnych lub innych przyczyn. W ćwiczeniu blackout jest przykładem zakłócenia biznesowego. Nie należy przypisywać ataku cybernetycznego konkretnemu wydarzeniu bez potwierdzonych ustaleń.

SLAJDY: 132–136 **ODNIESIENIE:** PN-EN ISO 22301; raporty operatorów energii **CHARAKTER:** PRAKTYKA

144. Jakie światowe blackouty można przywołać w szkoleniu?

Przykłady omawiane w prezentacji to Indie 2012, USA i Kanada 2003, Teksas 2021, Włochy 2003 oraz Hiszpania i Portugalia 2025. Warto przedstawiać ich przyczyny i skalę oddzielnie, bez sztucznego rankingu opartego na nieporównywalnych danych.

SLAJDY: 133–135 **ODNIESIENIE:** Raporty operatorów i instytucji publicznych; studia przypadków **CHARAKTER:** PRAKTYKA

145. Jakie przykłady z Polski ilustrują zagrożenia ciągłości?

Awaria związana z zasilaniem Szczecina w 2008 r. oraz rozległe zakłócenia po nawałnicach w 2017 r. pokazują zależność usług od energii i łączności. Są użyteczne do rozmowy o planach awaryjnych, ale nie są automatycznie przykładami cyberataków.

SLAJDY: 132–136 **ODNIESIENIE:** Studia przypadków z prezentacji; materiały operatorów **CHARAKTER:** PRAKTYKA

146. Jak często trzeba testować odtwarzanie z backupu?

Nie ma jednego uniwersalnego ustawowego interwału dla wszystkich systemów. Częstotliwość powinna wynikać z krytyczności procesu, zmian technologicznych i ryzyka. Dla najważniejszych usług test warto przeprowadzać tak, aby mieć wiarygodny dowód osiągania RTO/RPO.

SLAJDY: 68, 75, 129–131 **ODNIESIENIE:** KSC art. 8; PN-EN ISO 22301; ISO/IEC 27001, 9.1 **CHARAKTER:** PRAWO + NORMA

147. Czy plan BCP ma sens, jeżeli znajduje się na tym samym serwerze co ERP?

To częsty błąd projektowy. Plan awaryjny musi być osiągalny także w scenariuszu zakłócenia, dla którego go przygotowano. Warto zapewnić kontrolowane kopie offline, kontakty awaryjne i przetestować dostęp do instrukcji bez normalnej infrastruktury.

SLAJDY: 129–132, 145 **ODNIESIENIE:** PN-EN ISO 22301; dobre praktyki BCM **CHARAKTER:** NORMA + PRAKTYKA

148. Co zrobić, gdy nie da się osiągnąć wymaganego RTO?

Powiadomić właściciela procesu, przeanalizować różnicę między celem a zdolnością, wskazać potrzebne środki, alternatywny tryb działania i koszt. Brak zdolności odtworzenia powinien być widoczny jako ryzyko, a nie ukryty w dokumentacji IT.

SLAJDY: 91–95, 129–131, 138 **ODNIESIENIE:** ISO 31000; PN-EN ISO 22301; KSC art. 8 **CHARAKTER:** NORMA + PRAKTYKA

149. Kto odpowiada za decyzję o uruchomieniu planu awaryjnego?

Osoba wskazana w planie zarządzania kryzysowego lub ciągłości, mająca odpowiedni mandat. IT może wykonać odtworzenie, ale decyzje o priorytetach usług, komunikacji z klientami, kosztach i przerwaniu produkcji wymagają udziału biznesu i kierownictwa.

SLAJDY: 81–83, 125, 129–132 **ODNIESIENIE:** PN-EN ISO 22301; KSC art. 8c–8d **CHARAKTER:** NORMA + PRAWO

12. Wdrożenie, koszty, plan i trudne pytania z sali

Pytania kończące szkolenie: od czego zacząć, jak udowodnić gotowość i co powiedzieć, gdy brakuje danych.

150. Jakie są pierwsze trzy kroki wdrożenia KSC?

Po pierwsze udokumentować samoidentyfikację i terminy; po drugie określić kluczowe usługi, właścicieli i zakres; po trzecie przeprowadzić ocenę ryzyka i planować wymagane działania. Równolegle trzeba zadbać o formalności Wykazu KSC i gotowość do komunikacji z właściwymi podmiotami.

SLAJDY: 24–38, 140–143, 155–157 **ODNIESIENIE:** KSC art. 5 i 8; MC FAQ 3.2 **CHARAKTER:** PRAWO + PRAKTYKA

151. Czy istnieje jedna oficjalna lista dokumentów, która zapewnia zgodność z NIS2?

Nie ma uniwersalnego pakietu papierów, który zastępuje obowiązki. Dokumenty muszą wynikać z profilu organizacji, wymagań prawnych i przyjętych procesów. Ważne są dowody działania: wyniki testów, decyzje, pomiary, rejestry i zamknięte działania korygujące.

SLAJDY: 66–68, 140–151, 156–157 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001:2022, 7.5–10 **CHARAKTER:** PRAWO + NORMA

152. Czy można kupić gotową dokumentację i uznać wdrożenie za zakończone?

Nie. Szablony mogą przyspieszyć opracowanie dokumentów, ale bez rzeczywistej mapy usług, analizy ryzyka, ról, wdrożenia zabezpieczeń i testów nie dowodzą zgodności. Organizacja odpowiada za to, czy procesy działają.

SLAJDY: 66–68, 77, 140–151 **ODNIESIENIE:** KSC art. 8; MC FAQ 3.7 **CHARAKTER:** PRAWO + PRAKTYKA

153. Czy małej firmie wystarczy jeden informatyk do realizacji wszystkich obowiązków?

Nie można odpowiedzieć bez analizy zakresu i ryzyka. Jedna osoba może wykonywać wiele czynności, ale potrzebne są odpowiednie kompetencje, zastępowalność, decyzje biznesowe, nadzór i osoby kontaktowe zgodnie z przepisami. Część zadań można powierzyć dostawcom.

SLAJDY: 38, 44–47, 65, 140–145 **ODNIESIENIE:** KSC art. 8 i przepisy dotyczące kontaktów; MC FAQ 3.15–3.17 **CHARAKTER:** PRAWO + PRAKTYKA

154. Czy firma musi mieć własny SOC?

Nie ma jednego narzuconego modelu organizacyjnego dla wszystkich. Podmiot musi zapewnić skuteczne środki odpowiednie do ryzyka, co może realizować własnymi zasobami lub usługą zewnętrzną. Kluczowe są odpowiedzialność, reakcja, dostępność i dowody skuteczności.

SLAJDY: 42–43, 65, 73, 109 **ODNIESIENIE:** KSC art. 8; MC FAQ 3.14 **CHARAKTER:** PRAWO

155. Czy wdrożenie ISO 27001 i KSC można zrealizować wspólnym zespołem?

Tak, a często jest to optymalne. Wspólne powinny być mapa wymagań, ocena ryzyka, dokumentacja, role i dowody, z zachowaniem odrębności obowiązków ustawowych. Jeden zespół nie oznacza, że wszystkie decyzje może podejmować dział IT.

SLAJDY: 41, 60–69, 78–83, 140 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001:2022 **CHARAKTER:** PRAWO + NORMA

156. Ile kosztuje wdrożenie NIS2/KSC?

Bez informacji o wielkości, usługach krytycznych, stanie zabezpieczeń, liczbie dostawców i lukach nie da się rzetelnie podać kwoty. Koszt trzeba rozbić na diagnozę, organizację, technologie, szkolenia, testy, audyty oraz utrzymanie, a następnie nadać priorytety według ryzyka.

SLAJDY: 45, 90–93, 140–150 **ODNIESIENIE:** KSC art. 8; praktyka budżetowania wg ryzyka **CHARAKTER:** PRAKTYKA

157. Co zrobić, jeśli zarząd nie ma budżetu na wszystkie zabezpieczenia?

Zidentyfikować obowiązki bezwzględne, ryzyka poza tolerancją i działania o największym wpływie. Przygotować warianty kosztowe z opisem skutków odroczenia, przypisać decyzje i terminy. Brak budżetu nie zwalnia z obowiązków prawnych; wymaga świadomego zarządzania priorytetami.

SLAJDY: 44–47, 90–93, 147–151 **ODNIESIENIE:** KSC art. 8 i 8c–8e; ISO 31000 **CHARAKTER:** PRAWO + PRAKTYKA

158. Kto powinien prowadzić projekt wdrożenia: IT, compliance czy zarząd?

Najczęściej potrzebny jest sponsor z kierownictwa, koordynator SZBI i współpraca IT, biznesu, prawników, HR, zakupów i właścicieli procesów. Jeden dział nie ma pełnego obrazu skutków. Właściciel każdego zadania i decyzji musi być jasno wskazany.

SLAJDY: 44–47, 65, 81–83, 140–149 **ODNIESIENIE:** KSC art. 8c–8d; ISO/IEC 27001:2022, 5.3 **CHARAKTER:** PRAWO + NORMA

159. Co zrobić najpierw: audyt GAP czy zakup nowych narzędzi?

Najpierw ustalić obowiązki, usługi, ryzyka i faktyczne luki. GAP pomaga odróżnić brak dokumentu od braku skutecznego działania. Dopiero na tej podstawie warto wybierać środki, budżet i kolejność wdrożenia. Zakupy bez diagnozy często nie rozwiązują najważniejszych problemów.

SLAJDY: 98, 140–150 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001:2022, 6.1.3; praktyka GAP **CHARAKTER:** PRAKTYKA

160. Jak odpowiedzieć prezesowi: „Po czym poznam, że jesteśmy gotowi?”

Pokaż stan prawnych obowiązków i Wykazu, aktualną ocenę ryzyka, decyzje właścicieli, wykonanie planu, testy odtworzenia, obsługę incydentów, nadzór nad dostawcami i wyniki audytów. Gotowość to dowody działania, nie samo podpisanie polityki.

SLAJDY: 140–151, 155–159 **ODNIESIENIE:** KSC art. 5, 8, 11, 15; ISO/IEC 27001:2022, 9–10 **CHARAKTER:** PRAWO + NORMA

161. Czy po wdrożeniu możemy „zamknąć projekt” i nie wracać do tematu?

Można zamknąć etap wdrożeniowy, ale SZBI wymaga monitorowania, przeglądów, audytów, aktualizacji ryzyka oraz reakcji na nowe zagrożenia i zmiany w działalności. Największym błędem jest potraktowanie zgodności jak jednorazowego odbioru dokumentacji.

SLAJDY: 60–61, 75–76, 140–159 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001:2022, 9–10 **CHARAKTER:** PRAWO + NORMA

162. Co powiedzieć, gdy uczestnik pyta o konkretną firmę, a nie znamy jej wszystkich danych?

Nie wydawać kategorycznej kwalifikacji. Powiedzieć, jakie dane są potrzebne: usługi, załącznik, wielkość i powiązania, art. 5, data uzyskania statusu i przepisy sektorowe. Można wskazać metodę, ale końcowy wniosek wymaga udokumentowanej analizy.

SLAJDY: 24–33, 140–141 **ODNIESIENIE:** KSC art. 5; MC FAQ 1 **CHARAKTER:** PRAWO + PRAKTYKA

163. Czy audytor zewnętrzny może wesprzeć zarząd przed kontrolą?

Tak. Niezależny przegląd może wykazać luki, zweryfikować mapę ryzyk i dowody skuteczności oraz wskazać plan naprawczy. Należy zadbać o niezależność i zakres usługi. Wynik konsultacji nie przenosi ustawowej odpowiedzialności podmiotu na audytora.

SLAJDY: 55–58, 68, 150–151, 158 **ODNIESIENIE:** KSC art. 8c, 15; ISO 19011:2026 **CHARAKTER:** PRAWO + NORMA

164. Jak zamknąć szkolenie jednym praktycznym wnioskiem?

Poprosić uczestników, by po powrocie ustalili trzy rzeczy: co jest krytyczną usługą, kto akceptuje jej ryzyko i jaki dowód potwierdza skuteczność zabezpieczeń. To prosty most między przepisami, ISO 27001 i rzeczywistą odpowiedzialnością.

SLAJDY: 155–160 **ODNIESIENIE:** KSC art. 8; ISO/IEC 27001:2022; wniosek szkoleniowy **CHARAKTER:** PRAKTYKA

Źródła i uwagi do aktualizacji

Źródła pierwotne są ważniejsze niż prezentacje handlowe i opracowania internetowe. Użyte w FAQ skróty odpowiedzi stanowią parafrazę, a nie reprodukcję pełnych treści norm lub ustaw.

Zastrzeżenie metodyczne: Właściwość organów, wyłączenia sektorowe, nowe akty wykonawcze, przepisy przejściowe oraz terminy zależą od statusu konkretnego podmiotu. W przypadku pytania o konkretną organizację należy sprawdzić jej działalność, wielkość, powiązania i datę uzyskania statusu. Źródła zostały sprawdzone na 10 listopada 2026 r., lecz przed późniejszym wykorzystaniem dokumentu wymagają aktualizacji.

01. Ustawa o krajowym systemie cyberbezpieczeństwa — tekst jednolity, Dz.U. 2026 poz. 20; stosować ze zmianami
https://eli.gov.pl/eli/DU/2026/20/ogl

02. Nowelizacja KSC z 23 stycznia 2026 r., Dz.U. 2026 poz. 252
https://eli.gov.pl/eli/DU/2026/252/ogl

03. Dyrektywa (UE) 2022/2555 — NIS2, EUR-Lex
https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=pl

04. Ministerstwo Cyfryzacji — oficjalny FAQ KSC (materiał objaśniający, niewiążący)
https://cyber.gov.pl/assets/pdf/faq-ksc.pdf

05. Ministerstwo Cyfryzacji — obowiązki podmiotów kluczowych i ważnych, 5 czerwca 2026 r.
https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc---obowiazki-podmiotow-kluczowych-i-waznych

06. S46 Cyber Hub — zgłaszanie incydentów
https://www.gov.pl/web/system-s46/zgloszenie-incydentu

07. Rozporządzenie wykonawcze Komisji (UE) 2024/2690
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R2690

08. ISO/IEC 27001:2022 — ISMS requirements, oficjalny katalog ISO
https://www.iso.org/standard/27001

09. ISO/IEC 27005:2022 — zarządzanie ryzykiem bezpieczeństwa informacji
https://www.iso.org/standard/80585.html

10. ISO 31000:2018 — wytyczne zarządzania ryzykiem
https://www.iso.org/standard/31000

11. ISO 19011:2026 — wytyczne audytowania systemów zarządzania
https://www.iso.org/standard/19011

12. PN-EN ISO 22301:2020-04/A1:2025-03 — katalog PKN
https://sklep.pkn.pl/normy/pn-en-iso-22301-2020-04-a1-2025-03e.html

13. RODO — rozporządzenie (UE) 2016/679
https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pl

14. DORA — rozporządzenie (UE) 2022/2554
https://eur-lex.europa.eu/eli/reg/2022/2554/oj?locale=pl