

Mapa Ankiety Banku: Pytanie, Dokument, Dowód

40 typowych pytań z ankiet due diligence podmiotów finansowych i pytanie krajowe K1, z wzorem odpowiedzi, dokumentem, dowodem i statusem

Mapa pomaga przygotować odpowiedź na ankietę bezpieczeństwa lub due diligence banku, ubezpieczyciela albo instytucji płatniczej szybciej i spójnie z dokumentami. Każde pytanie ma wzór odpowiedzi, wskazanie dokumentu pakietu, dowód do dołączenia albo udostępnienia na żądanie oraz pole statusu.

WŁAŚCICIEL	ZATWIERDZA	PRZEGLĄD	CZAS CZYTANIA
KOORDYNATOR BEZPIECZEŃSTWA ICT	ZARZĄD	CO 12 MIESIĘCY I PO KAŻDEJ ANKIECIE Z NOWYMI PYTANIAM	≈ 25 MIN
ORGANIZACJA [NAZWA DOSTAWCY]			

1. Po co ta mapa

Przed zawarciem umowy klient finansowy musi ocenić Dostawcę i ryzyka usługi [§ DORA art. 28.4](#), może zawrzeć umowę tylko z dostawcą stosującym odpowiednie standardy bezpieczeństwa informacji, a dla funkcji krytycznych lub istotnych bierze pod uwagę standardy najwyższej jakości [§ DORA art. 28.5](#). W praktyce ocena przychodzi jako ankieta (od kilkudziesięciu do ponad 200 pytań) i prośba o dokumenty. Pytania różnią się brzmieniem, ale często powtarzają się co do treści: mapa zbiera 40 najczęstszych i jedno pytanie wynikające z prawa krajowego (K1).

ZASADA ODPOWIEDZI

Odpowiadamy faktami i dowodami, nie deklaracjami. Nie wysyłaj odpowiedzi bez potwierdzenia dowodem. Jeżeli czegoś nie ma, piszemy "w trakcie wdrożenia, termin [DATA]" i wskazujemy plan. Wiele klientów przyjmuje taką odpowiedź; decyzja o dalszej współpracy należy do klienta.

2. Jak odpowiadać na ankietę

2.1. Przebieg

- Opiekun Klienta przekazuje ankietę Koordynatorowi Bezpieczeństwa ICT w dniu otrzymania i ustala z klientem termin oraz to, czy usługa wspiera funkcję krytyczną lub istotną.
- Koordynator Bezpieczeństwa ICT przypisuje pytania анкеты do numerów z mapy (A1-J4, K1). Pytania bez odpowiednika trafiają do rozdziału 4.
- Odpowiedzi przygotowuje się z wzorów, uzupełniając dane z rejestrów ([→ A-DDS-06 · Rejestr Aktywów i Usług ICT](#), [→ A-DDS-08 · Rejestr Podwykonawców](#)); Kierownik Usługi sprawdza zgodność ze stanem faktycznym, a do każdej odpowiedzi ze statusem JEST przypisuje dowód.
- Koordynator Bezpieczeństwa ICT zatwierdza całość; Opiekun Klienta nie wysyła odpowiedzi bez tego zatwierdzenia.
- Wysłaną ankietę z dowodami archiwizuje się per klient; przy kolejnej ankiecie tego klienta odpowiedzi muszą być spójne z poprzednimi albo zmiana musi być wyjaśniona.

RODZAJ ANKIETY	TERMIN ODPOWIEDZI (DOMYŚLNIE, DO UZGODNIENIA Z KLIENTEM)
Krótką (wstępna kwalifikacja, do ok. 50 pytań)	do 5 dni roboczych
Pełna (z dokumentami i dowodami)	do 10 dni roboczych

2.2. Status pytania

STATUS	ZNACZENIE	JAK ODPOWIADAĆ
JEST	Kontrola działa i jest dowód.	Wzór odpowiedzi + dowód.
W BUDOWIE	Plan z właścicielem i terminem.	"W trakcie wdrożenia, termin [DATA]" + krótki opis planu i środków tymczasowych.
LUKA	Brak kontroli i planu.	Nie wysyłaj ankiet z LUKĄ bez decyzji Zarządu; wpisz ryzyko do → A-DDS-07 i ustal plan.

3. Pytania i wzory odpowiedzi

PRZED WYSŁANIEM

Nie wysyłaj bez potwierdzenia dowodem. Wzór odpowiedzi jest punktem wyjścia, nie deklaracją; każda odpowiedź musi odpowiadać stanowi faktycznemu w dniu wysłania.

3.1. A. Profil dostawcy i ład

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
A1	Proszę podać dane rejestrowe, strukturę właścicielską i beneficjentów rzeczywistych (w tym spoza UE) oraz potwierdzić brak objęcia sankcjami.	[UZUPEŁNIJ] [NAZWA DOSTAWCY], KRS [KRS], NIP [NIP], [ADRES SIEDZIBY]. Beneficjenci rzeczywiście zgodnie z wpisem w CRBR; beneficjenci spoza UE: brak / wskazani w załączniku. Spółka, jej zarząd i beneficjenci nie figurują na listach sankcyjnych UE i krajowych (sprawdzenie z dnia [DATA]).	poza pakietem: [DOKUMENT FIRMY]	Odpis KRS, wydruk CRBR, wynik sprawdzenia list sankcyjnych	[STATUS]
A2	Kto odpowiada za bezpieczeństwo informacji? Czy macie CISO i zatwierdzone polityki?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Funkcję pełni Koordynator Bezpieczeństwa ICT, [IMIE I NAZWISKO], podległy Zarządowi. Polityka bezpieczeństwa ICT i procedury zatwierdzone przez Zarząd [DATA ZATWIERDZENIA], przegląd co 12 miesięcy i po istotnych zdarzeniach.	→ L1-DDS-01	Polityka (rozdział 3), spis dokumentów z datami zatwierdzenia	[STATUS]
A3	Jaka jest kondycja finansowa firmy? Proszę o sprawozdania finansowe.	[UZUPEŁNIJ] Sprawozdania finansowe za ostatnie 3 lata udostępniamy po podpisaniu NDA; brak	poza pakietem: [DOKUMENT FIRMY]	Sprawozdania finansowe, zaświadczenia o niezaleganiu	[STATUS]

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
		zaległości publicznoprawnych; udział największego klienta w przychodach: ...			
A4	Czy posiadacie certyfikat ISO 27001 lub raport SOC 2 / ISAE 3402?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Wariant 1: certyfikat nr ..., zakres obejmuje usługę [NAZWA USŁUGI], ważny do [DATA]. Wariant 2: nie posiadamy; stosujemy wymagania minimalne z polityki i udostępniamy rejestry i raporty z testów; certyfikację planujemy na [DATA] / nie planujemy.	→ L1-DDS-01	Certyfikat i zakres albo pakiet dowodów	[STATUS]

3.2. B. Ryzyko, aktywa i dane

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
B1	Jak identyfikujecie i oceniacie ryzyka ICT?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Ocena ryzyka co 12 miesięcy i doraźnie po istotnych zmianach, metoda 3x3; ryzyka wysokie mają plan przyjęty przez Zarząd w 20 dni roboczych.	→ A-DDS-07	Wyciąg z rejestru ryzyk (bez szczegółów podatności)	[STATUS]
B2	Czy prowadzicie inwentarz aktywów i usług?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Tak; rejestr usług i aktywów z właścicielami, lokalizacjami, klasą odtworzeniową; aktualizowany w dniu zmiany, przegląd co 12 miesięcy.	→ A-DDS-06	Wyciąg z rejestru dla usługi klienta	[STATUS]

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
B3	Gdzie przetwarzane i przechowywane są nasze dane, w tym kopie?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Usługa świadczona z: [LOKALIZACJA DANYCH]; dane i kopie: [LOKALIZACJA DANYCH]. O zmianie lokalizacji powiadamiamy z wyprzedzeniem uzgodnionym w umowie (domyślnie 90 dni).	→ A-DDS-06	Wyciąg z rejestru (pole U6)	[STATUS]
B4	Czy przetwarzacie dane osobowe w naszym imieniu? Proszę o umowę powierzenia i listę podmiotów przetwarzających.	[UZUPEŁNIJ] Tak / nie. Jeżeli tak: umowa powierzenia zgodna z art. 28 RODO; lista podmiotów dalej przetwarzających w rejestrze podwykonawców; zmiana podmiotu dalej przetwarzającego za zgodą lub z prawem sprzeciwu (art. 28 ust. 2 RODO).	→ A-DDS-08	Wzór umowy powierzenia, wyciąg z rejestru	[STATUS]

3.3. C. Kontrola dostępu logicznego i fizycznego

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
C1	Czy stosujecie uwierzytelnianie wieloskładnikowe (MFA)?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Tak, dla dostępu zdalnego, administracyjnego, do konsoli chmury, repozytoriów i poczty; pokrycie: ...%.	→ L3-DDS-04	Raport pokrycia MFA z [NAZWA SYSTEMU]	[STATUS]
C2	Jak zarządzacie kontami uprzywilejowanymi i jak często przeglądacie uprawnienia?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Oddzielne konta administracyjne lub podnoszenie	→ L3-DDS-04	Ewidencja kont uprzywilejowanych, protokół ostatniego przeglądu	[STATUS]

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
		uprawnień na czas zadania; ewidencja posiadaczy; przegląd uprawnień administracyjnych, dostępu do danych produkcyjnych i kont podwykonawców co kwartał, pozostałych co 6 miesięcy.			
C3	Jak zabezpieczacie fizycznie biuro, sprzęt i miejsca przetwarzania danych?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Systemy produkcyjne w centrach danych dostawcy chmury (zabezpieczenia fizyczne potwierdzone jego raportami niezależnymi); biuro: kontrola wejścia, brak serwerów z danymi klientów; stacje robocze szyfrowane, blokada ekranu.	→ A-DDS-08	Raport niezależny dostawcy chmury, opis zabezpieczeń biura	[STATUS]
C4	W jakim czasie odbieracie dostęp po odejściu pracownika?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). W ciągu 24 godzin od zakończenia współpracy, uprawnienia administracyjne natychmiast; dostępy w systemach klienta zgłaszamy klientowi tego samego dnia.	→ L3-DDS-04	Próbka odejść z datami blokady	[STATUS]

3.4. D. Bezpieczeństwo techniczne

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
D1	Jak szyfrujecie dane w spoczynku i w transmisji?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Transmisja: TLS 1.2 lub nowszy. Spoczynek: szyfrowanie dysków i baz danych mechanizmem [NARZĘDZIE] ; klucze zarządzane w usłudze zarządzania kluczami, sekrety poza kodem.	→ L1-DDS-01	Wynik skanu TLS, opis konfiguracji	[STATUS]
D2	Jak zarządzacie podatnościami? Jakie są terminy poprawek?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Skanowanie podatności i zależności; cel wewnętrzny: poprawki krytyczne dla systemów dostępnych z internetu do 72 godzin od publikacji poprawki, pozostałe do 7 dni; terminy umowne według umowy.	→ L1-DDS-01	Raport ze skanów, historia poprawek	[STATUS]
D3	Kiedy był ostatni test penetracyjny i jakie były wyniki?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Ostatni test: [DATA] , wykonawca niezależny; ustalenia krytyczne i wysokie usunięte / w trakcie usuwania do [DATA] . Streszczenie po podpisaniu NDA.	→ A-DDS-12	Streszczenie raportu, status ustaleń	[STATUS]
D4	Czy logujecie i monitorujecie zdarzenia bezpieczeństwa?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Tak; logi dostępu administracyjnego i zdarzeń bezpieczeństwa zbierane centralnie, chronione przed modyfikacją, przechowywane zgodnie z umową; alerty obsługiwane w oknie dyżuru [GODZINY DYŻURU] .	→ L1-DDS-01	Konfiguracja logowania, przykładowy alert	[STATUS]

3.5. E. Wytwarzanie, zmiany i ochrona środowisk

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
E1	Czy stosujecie bezpieczny cykl wytwarzania oprogramowania i rozdzielacie środowiska?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Przegląd kodu przez drugą osobę, skanowanie zależności i kodu w potoku wdrożeniowym, chroniona gałąź główna, sekrety poza repozytorium; środowiska rozdzielone, dane produkcyjne klienta nie trafiają do testów bez anonimizacji i zgody klienta.	→ L3-DDS-05	Konfiguracja repozytorium i potoku, opis środowisk	[STATUS]
E2	Jak chronicie się przed złośliwym oprogramowaniem i czy sieć jest segmentowana?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Ochrona przed złośliwym oprogramowaniem na stacjach i serwerach z centralnym raportowaniem; środowisko produkcyjne odseparowane sieciowo od biurowego i testowego; dostęp administracyjny tylko przez zabezpieczone połączenie z MFA.	poza pakietem: [DOKUMENT FIRMY]	Raport z narzędzia ochrony stacji, schemat segmentacji	[STATUS]
E3	Jak zarządzacie zmianami w środowisku produkcyjnym?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Każda zmiana w rejestrze, z oceną, testem, zatwierdzeniem drugiej osoby i planem wycofania; zmiany awaryjne dokumentowane w 5 dni roboczych; cel: 0 zmian poza rejestrem.	→ L3-DDS-05	Próbka z rejestru zmian	[STATUS]
E4	Czy informujecie o zmianach mających wpływ na usługę?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Tak; prace planowe domyślnie co	→ L3-DDS-05	Przykładowa notyfikacja	[STATUS]

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
		najmniej 3 dni robocze wcześniej; zmiany istotne (podwykonawca, lokalizacja, architektura) z wyprzedzeniem uzgodnionym w umowie (domyślnie 60-90 dni), wycofanie usługi domyślnie 12 miesięcy wcześniej.			

3.6. F. Incydenty

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
F1	W jakim czasie poinformujecie nas o incydencie?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Incydent krytyczny (S1): bez zbędnej zwłoki, nie później niż 2 godziny od wykrycia wpływu na usługę klienta, liczone w oknie dyżuru [GODZINY DYŻURU] ; dyżur 24/7 dostępny jako opcja płatna. Incydent istotny (S2): według umowy, nie później niż 24 godziny. Telefonicznie i pisemnie.	→ L3-DDS-02	Procedura, rejestr z czasami powiadomień	[STATUS]
F2	Jakie informacje przekażecie i jak często będziecie aktualizować status?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Powiadomienie zawiera m.in. czas wykrycia, usługę, charakter i zasięg zakłócenia, wpływ na dane, działania i szacowany czas przywrócenia; aktualizacje co 4 godziny (S1) lub co 24 godziny (S2).	→ L3-DDS-02	Wzór powiadomienia	[STATUS]

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
F3	Czy przekażecie raport z analizy przyczyn?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Tak, w ciągu 10 dni roboczych od przywrócenia usługi, w formie przydatnej do Państwa raportu końcowego.	→ L3-DDS-02	Przykładowy raport (zanonimizowany)	[STATUS]
F4	Czy w ostatnich 12 miesiącach mieliście istotne incydenty? Czy ćwiczyacie obsługę incydentów?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Liczba incydentów S1/S2 w 12 miesiącach: ...; szczegóły po NDA. Coroczne ćwiczenie łańcucha powiadomień, ostatnie: [DATA].	→ A-DDS-12	Statystyka z rejestru, raport z ćwiczenia	[STATUS]

3.7. G. Ciągłość działania

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
G1	Jakie są RTO i RPO usługi?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Usługa [NAZWA USŁUGI]: RTO ..., RPO ... (zgodnie z umową; domyślnie dla klasy A: RTO do 24 godzin, RPO do 24 godzin); ostatni test potwierdził RTO	→ L3-DDS-03	Raport z testu odtworzenia	[STATUS]
G2	Jak wykonujecie kopie zapasowe i czy są chronione przed ransomware?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Kopie co najmniej raz na dobę, retencja ... dni, co najmniej jedna kopia niezmiennalna w oddzielnym koncie lub lokalizacji, szyfrowana.	→ L3-DDS-03	Konfiguracja kopii	[STATUS]

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
G3	Czy macie plan ciągłości działania i kiedy był testowany?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Plan ciągłości obejmujący scenariusze awarii, ransomware, utraty podwykonawcy i kluczowej osoby; test odtworzenia [DATA], ćwiczenie planu [DATA].	→ L3-DDS-03	Plan, raporty z testów	[STATUS]
G4	Czy weźmiecie udział w naszych testach ciągłości lub testach TLPT?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). W zakresie uzgodnionym w umowie i w sposób chroniący innych klientów; udział w TLPT na zasadach i kosztach ustalonych w umowie.	→ A-DDS-11	Postanowienie umowne	[STATUS]

3.8. H. Podwykonawcy

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
H1	Proszę o listę podwykonawców biorących udział w świadczeniu usługi i ich lokalizacje.	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Lista w załączeniu: nazwa, kraj, zakres, lokalizacje danych, ranga w łańcuchu.	→ A-DDS-08	Wyciąg z rejestru podwykonawców	[STATUS]
H2	Czy przenosicie nasze wymagania na podwykonawców?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Przy usługach wspierających funkcje krytyczne lub istotne przenosimy na podwykonawców istotnych wymagania dotyczące bezpieczeństwa, incydentów, zmian, audytu, ciągłości, wyjścia	→ A-DDS-08	Wynik weryfikacji umów	[STATUS]

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
		i współpracy z organami; dla dostawców chmury weryfikujemy ich warunki standardowe i dodatki DORA.			
H3	Czy poinformujecie nas o zmianie podwykonawcy?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Tak, z wyprzedzeniem uzgodnionym w umowie (domyślnie 90 dni dla usług wspierających funkcje krytyczne lub istotne, 30 dni dla pozostałych); mają Państwo prawo sprzeciwu.	→ L3-DDS-05	Procedura, przykładowa notyfikacja	[STATUS]
H4	Proszę o dane do naszego rejestru informacji (DORA).	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Przekazujemy: dane Dostawcy i identyfikator, opis usługi, lokalizację, łańcuch podwykonawców z rangą, identyfikatorami i krajami.	→ A-DDS-08	Wyciąg w formacie klienta	[STATUS]

3.9. I. Umowa, audyt i ubezpieczenie

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
I1	Czy zaakceptujecie nasz aneks DORA (art. 30)?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Akceptujemy postanowienia wymagane art. 30; uwagi do sposobu wykonania przekazujemy w komentarzach do aneksu.	→ A-DDS-11	Komentarze do aneksu	[STATUS]
I2	Czy zapewnicie prawo audytu i dostępu nam i	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Dostęp, inspekcje	→ A-DDS-11	Postanowienie umowne	[STATUS]

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
	organowi nadzoru oraz współpracę z KNF?	i audyt, także na miejscu, po uzgodnieniu terminu i w sposób chroniący dane innych klientów; w pierwszej kolejności udostępniamy dowody i raporty. Współpracujemy z organami nadzoru w pełnym zakresie, w koordynacji z Państwem.			
I3	Czy posiadacie ubezpieczenie OC zawodowe i ubezpieczenie od ryzyk cybernetycznych?	[UZUPEŁNIJ] OC zawodowe: ubezpieczyciel ..., suma gwarancyjna ..., ważne do [DATA] . Ubezpieczenie cyber: posiadamy / nie posiadamy / w trakcie zakupu, termin [DATA] .	poza pakietem: [DOKUMENT FIRMY]	Polisy lub certyfikaty ubezpieczenia	[STATUS]
I4	Czy pracownicy wezmą udział w naszych szkoleniach z bezpieczeństwa i odporności cyfrowej?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). W zakresie uzgodnionym w umowie; udział ewidencjonujemy.	→ A-DDS-12	Ewidencja szkoleń	[STATUS]

3.10. J. Wyjście i ludzie

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
J1	Jak wesprzecie nas przy zakończeniu umowy? Czy zapewnicie okres przejściowy?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Zwrot danych bezwarunkowy; plan wsparcia w ciągu 15 dni roboczych; usługa bez pogorszenia SLA w okresie przejściowym określonym w umowie, usługi przejściowe według cennika uzgodnionego w umowie; przekazanie wiedzy i dokumentacji.	→ L3-DDS-09	Plan wsparcia wyjścia	[STATUS]

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
J2	W jakim formacie oddacie nasze dane?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). W otwartych, udokumentowanych formatach (CSV, JSON, zrzut SQL, pliki oryginalne) z opisem struktury i sumami kontrolnymi.	→ L3-DDS-09	Katalog eksportu, raport z próbnego eksportu	[STATUS]
J3	Czy potwierdzicie usunięcie danych?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Pisemne potwierdzenie obejmujące produkcję, środowiska testowe, kopie i podwykonawców, w ciągu 30 dni od końca retencji kopii.	→ L3-DDS-09	Wzór potwierdzenia	[STATUS]
J4	Jak szkolicie pracowników i weryfikujecie ich przed zatrudnieniem?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Szkolenie wstępne w pierwszym tygodniu i coroczne z testem; cel wewnętrzny: ukończenie przez co najmniej 98% osób; zobowiązanie do poufności przed dostępem; weryfikacja w granicach prawa pracy.	→ A-DDS-12	Statystyka szkoleń	[STATUS]

3.11. K. Pytanie krajowe

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
K1	Jak zapewnacie ochronę tajemnicy bankowej (lub ubezpieczeniowej) i jakie obowiązki mają osoby z dostępem?	[JEST / W BUDOWIE] (przy W BUDOWIE termin: [DATA]). Osoby z dostępem do informacji objętych tajemnicą bankową mogą być nią związane z mocy ustawy (art. 104 ust. 1 Prawa bankowego) lub zobowiązane umownie;	→ L3-DDS-04	Zobowiązanie do poufności podpisywane przy nadaniu dostępu (→ L3-DDS-04) albo [DOKUMENT FIRMY] ; lista osób z dostępem	[STATUS]

NR	TYPOWE PYTANIE	WZÓR ODPOWIEDZI	DOKUMENT	DOWÓD	STATUS
		analogicznie tajemnica ubezpieczeniowa (art. 35 ustawy o działalności ubezpieczeniowej i reasekuracyjnej). Osoby te podpisują przed nadaniem dostępu imienne zobowiązanie do zachowania tajemnicy; dostęp ograniczamy do niezbędnych osób (lista na żądanie); obowiązek trwa po zakończeniu współpracy.			

4. Pytania spoza mapy

- Pytanie, które nie pasuje do żadnego z numerów mapy, Koordynator Bezpieczeństwa ICT opracowuje sam lub z Kierownikiem Usługi i dopisuje do mapy po wysłaniu ankiety.
- Pytanie o wymaganie, którego Dostawca nie spełnia: odpowiedź "nie / w trakcie wdrożenia" z planem; nie zmieniaj sensu pytania, żeby odpowiedzieć "tak".
- Pytanie o dane poufne innych klientów lub szczegóły podatności: odpowiedź ogólna, szczegóły po NDA lub w trakcie audytu.
- Pytanie o outsourcing czynności bankowych lub wymagania chmurowe: zob.
→ A-DDS-11 · Checklista Klauzul Art. 30 DORA do Aneksu, rozdział 6.
- Pytanie dotyczące NIS2 / ustawy o krajowym systemie cyberbezpieczeństwa: ten pakiet go nie obejmuje; odpowiedz zgodnie ze swoim statusem i dokumentacją w tym zakresie.

5. Folder dowodów

Dowody przechowuj w jednym folderze w [MIEJSCE PRZECHOWYWANIA] z podziałem na obszary A-K, z datą każdego pliku. Dowód starszy niż 12 miesięcy odśwież przed wysłaniem.

OBSZAR	TYPOWE DOWODY
A	Odpis KRS, wydruk CRBR, sprawdzenie list sankcyjnych, polityka z datą zatwierdzenia, sprawozdania finansowe, certyfikaty
B	Wyciągi z rejestrów aktywów i ryzyk
C	Raport MFA, protokoły przeglądów dostępów, próbka odejść, opis zabezpieczeń fizycznych
D	Wynik skanu TLS, raporty ze skanów podatności, streszczenie testu penetracyjnego
E	Konfiguracja repozytorium, raport ochrony przed złośliwym oprogramowaniem, schemat segmentacji, próbka rejestru zmian
F	Statystyka z rejestru incydentów, raport z ćwiczenia, wzór powiadomienia
G	Raporty z testów odtworzenia i ćwiczeń planu ciągłości
H	Wyciąg z rejestru podwykonawców
I	Komentarze do aneksów, postanowienia umowne, polisy ubezpieczeniowe
J	Raport z próbnego eksportu, wzór potwierdzenia usunięcia, statystyka szkoleń
K	Wzór zobowiązania do zachowania tajemnicy, lista osób z dostępem

6. Dostosowanie i zatwierdzenie

Dokument jest wzorem. Przed zatwierdzeniem uzupełnij pola oznaczone nawiasem kwadratowym, usuń przykłady, które nie dotyczą Twojej organizacji, i sprawdź, czy wartości (terminy, częstotliwości) są zgodne z umowami zawartymi z klientami. Gdy umowa z klientem przewiduje termin ostrzejszy niż ten dokument, obowiązuje termin z umowy.

- Kolumnę "Status" wypełnij dla każdego pytania przed pierwszą ankietą: JEST, W BUDOWIE (z terminem) albo LUKA; pytania ze statusem LUKA wpisz do [→ A-DDS-07 · Rejestr Ryzyk ICT z Metodą Jednostronicową](#) z planem.
- Wzory odpowiedzi zaczynają się od pola [JEST / W BUDOWIE] (zostaw właściwy wariant, przy W BUDOWIE wpisz termin w polu [DATA]) albo, przy odpowiedziach czysto faktograficznych (A1, A3, B4, I3), od pola [UZUPEŁNIJ]. Wpis "poza pakietem" w kolumnie "Dokument" oznacza, że odpowiedź opiera się na dokumencie firmy spoza pakietu. Po uzupełnieniu sprawdź odpowiedź ze stanem faktycznym.
- Folder dowodów (rozdział 5) załóż w [MIEJSCE PRZECHOWYWANIA]; dowody poufne udostępniaj po podpisaniu umowy o zachowaniu poufności.

CZYNNOŚĆ	IMIĘ I NAZWISKO	DATA	PODPIS
Opracował	[IMIĘ I NAZWISKO]	[DATA]	
Zatwierdził (Zarząd)	[IMIĘ I NAZWISKO]	[DATA ZATWIERDZENIA]	

CHARAKTER DOKUMENTU

Wzór dokumentacji opracowany przez RealSec dla dostawców usług ICT obsługujących podmioty finansowe. Nie stanowi porady prawnej, audytu ani oceny zgodności i nie gwarantuje pozytywnego wyniku oceny dostawcy przez klienta ani organ nadzoru. Za dostosowanie, wdrożenie i stosowanie dokumentu odpowiada organizacja, która go przyjmuje.

7. Historia zmian

WERSJA	DATA	AUTOR	OPIS ZMIANY
v1.0	2026-10-02	RealSec (wzór)	Wydanie wzoru w pakiecie Dostawca DORA Start.
[WERSJA]	[DATA]	[IMIĘ I NAZWISKO]	Dostosowanie do [NAZWA DOSTAWCY] i zatwierdzenie przez Zarząd.

RealSec · pakiet Dostawca DORA Start v1.0 · A-DDS-10 · wzór do dostosowania; nie stanowi porady prawnej

PRÓBKA