

Przewodnik dla dostawcy ICT

Ankieta DORA od banku, aneks z art. 30 i wymagania łańcucha dostaw NIS2. Co przychodzi, skąd się bierze, co odpowiedzieć i jakie dokumenty musisz mieć.

Dla właściciela albo CTO firmy IT na 5 do 50 osób, która obsługuje bank, ubezpieczyciela, TFI albo podmiot kluczowy lub ważny z ustawy o krajowym systemie cyberbezpieczeństwa i właśnie dostała ankietę bezpieczeństwa z terminem dwóch tygodni.

- | | |
|---|---|
| 1 | Skąd biorą się wymagania klienta |
| 2 | Plan na dziesięć dni i statusy odpowiedzi |
| 3 | Dwanaście dokumentów, które pokrywają ankietę |
| 4 | Dwadzieścia pytań: dokument i dowód |
| 5 | Aneks z art. 30: co przyjąć, co negocjować |
| 6 | Incydenty i czerwone linie |
| 7 | Rejestr informacji, podwykonawcy i co wysłać |
| 8 | Klient objęty NIS2 |

Wersja 1.0, październik 2026. Stan prawny na 7 października 2026 r. realsec.pl/dla-dostawcow-ict

Materiał informacyjny RealSec. Nie stanowi porady prawnej, audytu ani oceny zgodności i nie gwarantuje pozytywnej oceny dostawcy przez klienta lub organ nadzoru. Brzmienie umowy uzgadnia prawnik. Za treść odpowiedzi udzielanych klientom odpowiada dostawca.

1 Skąd biorą się wymagania klienta

DORA (rozporządzenie (UE) 2022/2554) stosuje się od 17 stycznia 2025 r. i obowiązuje bank, nie dostawcę. Bank nie spełni jej jednak bez danych i zobowiązań dostawcy, więc przenosi wymagania na Ciebie przez ankietę i umowę.

Przed zawarciem umowy bank musi ocenić, czy usługa wspiera funkcję krytyczną lub istotną, i ocenić dostawcę (art. 28 ust. 4). Umowy może zawierać tylko z dostawcami, którzy stosują odpowiednie standardy bezpieczeństwa informacji (art. 28 ust. 5). Prowadzi rejestr informacji o wszystkich umowach ICT i co najmniej raz w roku raportuje do nadzoru (art. 28 ust. 3). Treść umowy wyznacza art. 30.

Przy usługach wspierających funkcje krytyczne lub istotne bank stosuje dodatkowo własną politykę z rozporządzenia delegowanego (UE) 2024/1773 i ocenia podwykonawstwo według rozporządzenia delegowanego (UE) 2025/532 (w mocy od 22 lipca 2025 r.).

CO PRZYCHODZI	PO CO BANKOWI ALBO KLIENTOWI	PODSTAWA
Ankieta due diligence	Ocena dostawcy i ryzyk usługi przed umową i cyklicznie potem.	DORA art. 28 ust. 4 i 5
Aneks do umowy	Minimalne klauzule każdej umowy ICT; rozszerzone przy funkcjach krytycznych lub istotnych.	DORA art. 30 ust. 2 i 3
Dane do rejestru informacji	Ewidencja wszystkich umów ICT i coroczne raportowanie do nadzoru.	DORA art. 28 ust. 3; ITS 2024/2956
Pytania o podwykonawców	Ocena łańcucha przy usługach wspierających funkcje krytyczne lub istotne.	DORA art. 29; RTS 2025/532
Wymagania klienta NIS2	Środki bezpieczeństwa łańcucha dostaw podmiotu kluczowego lub ważnego.	NIS2 art. 21 ust. 2 lit. d; ustawa o KSC

Co z tego wynika dla Ciebie. Formalnie DORA Cię nie dotyczy, praktycznie odpowiadasz na nią kontraktowo. Bank nie pyta o deklaracje, tylko o dowody: zatwierdzoną politykę, raport pokrycia MFA, protokół przeglądu uprawnień, raport z testu odtworzenia, listę podwykonawców z lokalizacjami.

Klienci objęci NIS2 działają tak samo. Podmiot kluczowy lub ważny musi objąć środkami bezpieczeństwa swój łańcuch dostaw (dyrektywa (UE) 2022/2555, art. 21 ust. 2 lit. d). W Polsce wdraża to nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa z 23 stycznia 2026 r. (Dz. U. 2026 poz. 252), obowiązująca od 3 kwietnia 2026 r. Szczegóły w rozdziale 8.

2 Plan na dziesięć dni i statusy odpowiedzi

Krótką ankietę wstępną, do około 50 pytań, da się zwykle odesłać w 5 dni roboczych. Pełną, z dokumentami i dowodami, w 10. Kolejność ma znaczenie, bo rejestry z dni 2 i 3 zasilają odpowiedzi na większość pytań.

DZIEŃ	DZIAŁANIE	WYNIK
1	Ustal z klientem termin i to, czy usługa wspiera funkcję krytyczną lub istotną. Wyznacz osobę, która prowadzi ankietę.	Zakres: art. 30 ust. 2 czy także ust. 3
2 do 3	Spisz usługi dla klienta, systemy, lokalizacje danych i podwykonawców.	Rejestr usług, rejestr podwykonawców
4 do 7	Polityka i procedury: incydenty, ciągłość i kopie, dostęp, zmiana, wyjście. Wpisz realne terminy.	Dokumenty do zatwierdzenia
8	Wszystko, czego dziś nie spełniasz, wpisz jako ryzyko z planem i terminem.	Rejestr ryzyk, statusy W BUDOWIE
9 do 10	Odpowiedzi według mapy z dowodami, przegląd aneksu według checklisty, zatwierdzenie przez Zarząd.	Ankieta, komentarze do aneksu

Trzy statusy przy każdym pytaniu

Każdej odpowiedzi nadaj status, zanim wyjdzie do klienta. Status JEST bez aktualnego dowodu nie istnieje.

STATUS	KIEDY	JAK ODPOWIEDZIEĆ
JEST	Kontrola działa i jest dowód.	Fakt plus dowód (dokument, raport, protokół).
W BUDOWIE	Jest plan z właścicielem i terminem.	"W trakcie wdrożenia, termin [data]" plus krótki opis planu i środków tymczasowych.
LUKA	Brak kontroli i planu.	Nie wysyłaj bez decyzji Zarządu; wpisz ryzyko i ustal plan.

Zasada odpowiedzi. Odpowiadaj faktami i dowodami, nie zapewnieniami. Nie zmieniaj sensu pytania, żeby odpowiedzieć "tak". Każde "tak" w ankiecie staje się argumentem w umowie i przy audycie. Wysłaną ankietę archiwizuj per klient; za rok przyjdzie znowu i bank porówna odpowiedzi.

Pierwsze 48 godzin

Zapytaj na piśmie, czy usługa wspiera funkcję krytyczną lub istotną banku; od tego zależy, czy obowiązuje tylko art. 30 ust. 2, czy także ust. 3. Ustal format odpowiedzi (arkusz, portal, PDF) i to, czy dowody poufne mogą iść po podpisaniu NDA. Jeśli nie masz testu odtworzenia z ostatnich 12 miesięcy, zaplanuj go od razu: pytanie o RTO i RPO jest w każdej ankiecie.

3 Dwanaście dokumentów, które pokrywają ankietę

Nie potrzebujesz pełnego systemu zarządzania z certyfikacją. Potrzebujesz zestawu, który odpowiada na pytania banku i realnie działa w firmie na 5 do 50 osób. Tak wygląda pakiet Dostawca DORA Start.

KOD	DOKUMENT	NA CO ODPOWIADA
L1-DDS-01	Polityka bezpieczeństwa ICT dostawcy	Zasady, role i wymagania minimalne. Pierwszy dokument, o który prosi bank.
L3-DDS-02	Procedura incydentów i powiadamiania klienta	Klasyfikacja, termin powiadomienia klienta, raport przyczyn i rejestr incydentów.
L3-DDS-03	Plan ciągłości działania i kopii zapasowych	Klasy odtworzeniowe, RTO i RPO, kopie, scenariusze i testy.
L3-DDS-04	Procedura zarządzania dostępem	Nadawanie, przegląd i odbieranie dostępów, MFA, konta uprzywilejowane.
L3-DDS-05	Procedura zarządzania zmianą	Rejestr zmian, zatwierdzenie, wycofanie i notyfikacja zmian istotnych.
A-DDS-06	Rejestr aktywów i usług ICT	Usługi dla klientów, systemy i lokalizacje danych w jednym miejscu.
A-DDS-07	Rejestr ryzyk ICT	Metoda jednostronicowa 3×3, scenariusze bazowe i decyzje Zarządu.
A-DDS-08	Rejestr podwykonawców	Łańcuch podwykonawców z rangą i lokalizacjami; dane do rejestru informacji banku.
L3-DDS-09	Plan wsparcia wyjścia klienta	Okres przejściowy, eksport danych, usunięcie i potwierdzenie.
A-DDS-10	Mapa ankiety banku	40 pytań i pytanie krajowe K1: wzór odpowiedzi, dokument, dowód, status.
A-DDS-11	Checklista klauzul art. 30 do aneksu	Co przyjąć, co negocjować i czerwone linie, przed podpisaniem aneksu.
A-DDS-12	Rejestr szkoleń, testów i przeglądów	Dowód, że kontrole działają: szkolenia, testy odtworzenia, przeglądy dostępów.

Odpowiednik dla klientów objętych NIS2 (pakiet Dostawca NIS2 Start): Polityka bezpieczeństwa informacji dostawcy, Analiza ryzyka i rejestr ryzyk, Procedura incydentów i powiadamiania klienta, Standard ciągłości działania i odtwarzania, Standard zarządzania dostępem, Standard bezpieczeństwa łańcucha dostaw, Standard kopii zapasowych i odtwarzania, Procedura aktualizacji i podatności, Standard szkoleń i świadomości, Rejestr aktywów i usług, Mapa wymagań klienta NIS2, Checklista umowna NIS2 dla dostawcy.

Dokument opisuje to, co robicie. Bank ma w aneksie prawo audytu. Procedura, której nikt nie stosuje, jest gorsza niż jej brak, bo dokumentuje niezgodność. Pola w nawiasach kwadratowych uzupełnij, przykłady, które Cię nie dotyczą, usuń, a terminy porównaj z umowami; obowiązuje termin z umowy.

4 Dwadzieścia pytań: dokument i dowód

Pytania brzmią w każdej ankiecie inaczej, ale treść się powtarza. Poniżej 14 z 40 pytań mapy ankiety banku i 6 z 30 pytań mapy wymagań klienta NIS2; pełne mapy z wzorami odpowiedzi są w bezpłatnej próbce.

NR	PYTANIE	DOKUMENT	DOWÓD
ANKIETA BANKU (DORA), MAPA A-DDS-10			
A2	Kto odpowiada za bezpieczeństwo informacji? Czy macie zatwierdzone polityki?	L1-DDS-01 Polityka bezpieczeństwa ICT	Polityka z datą zatwierdzenia przez Zarząd
A4	Czy posiadacie certyfikat ISO 27001 lub raport SOC 2 / ISAE 3402?	L1-DDS-01 Polityka bezpieczeństwa ICT	Certyfikat z zakresem albo pakiet dowodów
B3	Gdzie przetwarzane i przechowywane są nasze dane, w tym kopie?	A-DDS-06 Rejestr aktywów i usług ICT	Wyciąg z rejestru dla usługi klienta
C1	Czy stosujecie uwierzytelnianie wieloskładnikowe (MFA)?	L3-DDS-04 Procedura zarządzania dostępem	Raport pokrycia MFA
C2	Jak zarządzacie kontami uprzywilejowanymi i jak często przeglądacie uprawnienia?	L3-DDS-04 Procedura zarządzania dostępem	Ewidencja kont, protokół ostatniego przeglądu
D2	Jak zarządzacie podatnościami? Jakieką są terminy poprawek?	L1-DDS-01 Polityka bezpieczeństwa ICT	Raport ze skanów, historia poprawek
D3	Kiedy był ostatni test penetracyjny i jakie były wyniki?	A-DDS-12 Rejestr szkoleń, testów i przeglądów	Streszczenie raportu, status ustaleń
E3	Jak zarządzacie zmianami w środowisku produkcyjnym?	L3-DDS-05 Procedura zarządzania zmianą	Próbka z rejestru zmian
F1	W jakim czasie poinformujecie nas o incydencie?	L3-DDS-02 Procedura incydentów	Rejestr incydentów z czasami powiadomień
G1	Jakie są RTO i RPO usługi?	L3-DDS-03 Plan ciągłości i kopii	Raport z testu odtworzenia
G3	Czy macie plan ciągłości działania i kiedy był testowany?	L3-DDS-03 Plan ciągłości i kopii	Plan, raporty z testów
H1	Proszę o listę podwykonawców biorących udział w świadczeniu usługi i ich lokalizacje.	A-DDS-08 Rejestr podwykonawców	Wyciąg z rejestru podwykonawców
H4	Proszę o dane do naszego rejestru informacji (DORA).	A-DDS-08 Rejestr podwykonawców	Wyciąg w formacie klienta
J1	Jak wesprzecie nas przy zakończeniu umowy? Czy zapewnicie okres przejściowy?	L3-DDS-09 Plan wsparcia wyjścia klienta	Plan wsparcia wyjścia
WYMAGANIA KLIENTA NIS2, MAPA A-NISD-011			
1	Czy są Państwo podmiotem kluczowym lub ważnym w rozumieniu UKSC?	L1-NISD-001 Polityka bezpieczeństwa informacji	Notatka z oceny statusu z datą i uzasadnieniem
9	Czy dostarczą Państwo informacje potrzebne do naszego zgłoszenia w S46 (24h, 72h, 1 mies.)?	L3-NISD-003 Procedura incydentów	Wzór komunikatu, protokół ćwiczenia
19	W jakim czasie usuwają Państwo podatności krytyczne?	L3-NISD-008 Procedura aktualizacji i podatności	Zestawienie podatności, rejestr wyjątków
22	Czy pracownicy mają zobowiązania do poufności i jak są weryfikowani?	L2-NISD-009 Standard szkoleń i świadomości	Wzór zobowiązania, lista osób z datą informacji z KRK
24	Jak oceniają i nadzorują Państwo swoich podwykonawców?	L2-NISD-006 Standard łańcucha dostaw	Daty i wyniki ocen, wzór klauzul
30	Czy umożliwią Państwo audyt lub przekażą dowody zgodności?	T-NISD-012 Checklista umowna NIS2	Pakiet dowodów, klauzula audytu

5 Aneks z art. 30: co przyjąć, co negocjować

Art. 30 ust. 1 wymaga formy pisemnej i jednego dokumentu. Postanowień z art. 30 bank nie może pominąć, więc ich odrzucenie co do zasady kończy się utratą klienta. Negocjujesz sposób wykonania: terminy, tryb audytu, koszty ustalone z góry.

LIT.	ART. 30 UST. 2: KAŻDA UMOWA ICT	STANOWISKO
a	Opis funkcji i usług; czy i na jakich warunkach dopuszczalne jest podwykonawstwo.	AKCEPTUJ; zaproponuj zamkniętą listę podwykonawców zamiast zakazu.
b	Lokalizacje świadczenia usług i przetwarzania danych; uprzednie powiadomienie o zmianie.	NEGOCJUJ termin powiadomienia (30 do 90 dni).
c	Dostępność, autentyczność, integralność i poufność danych, w tym osobowych.	AKCEPTUJ; dla danych osobowych umowa powierzenia.
d	Dostęp do danych, odzyskanie i zwrot przy niewypłacalności lub zakończeniu umowy.	AKCEPTUJ; katalog eksportu w planie wyjścia.
e	Opisy poziomu usług, ich aktualizacji i zmian.	AKCEPTUJ; zmiana SLA tylko za zgodą stron.
f	Pomoc przy incydencie bez dodatkowych kosztów albo po koszcie ustalonym z góry.	NEGOCJUJ; incydenty z Twojej przyczyny bez dopłaty, pozostałe z cennika.
g	Pełna współpraca z właściwymi organami.	AKCEPTUJ; współpraca koordynowana z klientem.
h	Prawa wypowiedzenia i minimalne okresy wypowiedzenia.	NEGOCJUJ okresy powiązane z okresem przejściowym.
i	Udział w programach świadomości i szkoleniach klienta.	NEGOCJUJ udział zdalny z limitem godzin.

LIT.	ART. 30 UST. 3: FUNKCJE KRYTYCZNE LUB ISTOTNE	STANOWISKO
a	Pełny opis poziomów usług z mierzalnymi celami.	AKCEPTUJ; kary za naruszenie SLA, nie za samo zdarzenie.
b	Okresy powiadomień i obowiązki sprawozdawcze.	AKCEPTUJ; katalog notyfikacji z procedury zmiany.
c	Wdrożone i testowane plany awaryjne, środki bezpieczeństwa ICT.	AKCEPTUJ; plan ciągłości z testem.
d	Udział i współpraca w testach TLPT klienta.	NEGOCJUJ zakres, zasady bezpieczeństwa i koszty z góry.
e	Nieograniczone prawo dostępu, inspekcji i audytu, także na miejscu.	NEGOCJUJ tryb: zapowiedź, najpierw dowody, audyty wspólne.
f	Strategia wyjścia z obowiązkowym okresem przejściowym.	AKCEPTUJ; cennik usług przejściowych w umowie.

Przy podwykonawstwie usług wspierających funkcje krytyczne lub istotne bank dopisze też warunki z RTS 2025/532: przeniesienie obowiązków na podwykonawców, powiadamianie o istotnych zmianach, prawo sprzeciwu i wypowiedzenia. Polskie banki dodają zwykle postanowienia o tajemnicy bankowej (art. 104 Prawa bankowego), a przy outsourcingu czynności bankowych wymagania art. 6a do 6d tej ustawy.

6 Incydenty i czerwone linie

Pytanie "w jakim czasie poinformujecie nas o incydencie?" jest w każdej ankiecie. Bank zgłasza poważne incydenty ICT do nadzoru (art. 19 DORA) w terminach z rozporządzenia delegowanego (UE) 2025/301, więc potrzebuje Twoich danych szybko.

ETAP	TERMIN BANKU WOBEC NADZORU (RTS 2025/301)	CZEGO BANK POTRZEBUJE OD CIEBIE
Powiadomienie wstępne	4 h od klasyfikacji incydentu jako poważny, najpóźniej 24 h od powzięcia wiadomości	Szybkiej informacji: co, od kiedy, jaka usługa, jaki wpływ
Raport pośredni	72 h od powiadomienia wstępnego	Aktualizacji statusu, działań i szacowanego czasu przywrócenia
Raport końcowy	1 miesiąc od ostatniego raportu pośredniego	Raportu przyczyn i działań naprawczych

Rozsądne stanowisko małej firmy bez całodobowego dyżuru: incydent krytyczny zgłaszasz bez zbędnej zwłoki, nie później niż 2 godziny od wykrycia wpływu na usługę klienta, liczone w oknie dyżuru; incydent istotny w 24 godziny; dyżur 24/7 jako płatna opcja. Aktualizacje co 4 godziny, raport przyczyn w 10 dni roboczych od przywrócenia usługi.

Czerwone linie: nie przyjmuj bez decyzji Zarządu

ŻĄDANIE	DLACZEGO NIE	RUCH ZASTĘPCZY
Powiadomienie o incydencie liczone od wystąpienia albo całodobowo bez dyżuru w umowie	Nie wiesz o incydencie przed wykryciem; doba wymaga płatnego dyżuru.	Do 2 h od wykrycia wpływu na usługę w oknie dyżuru dla incydentu krytycznego, 24 h dla istotnego; 24/7 jako opcja płatna.
Niezapowiedziane wejście na środowisko współdzielone	Narusza poufność innych klientów.	Audyt z zapowiedzią, dowody i raporty, audyt wspólny.
Odpowiedzialność nieograniczona albo kara za sam incydent	Ryzyko niemożliwe do wyceny i ubezpieczenia.	Limit odpowiedzialności, kary za mierzalne naruszenie SLA.
RTO lub dostępność lepsze niż potwierdzone testem	Naruszenie od pierwszego dnia umowy.	Wartość z ostatniego testu i plan poprawy z terminem.
Całkowity zakaz podwykonawstwa przy usłudze w chmurze	Niewykonalny w modelu usługi.	Zamknięta lista podwykonawców, notyfikacja zmian, prawo sprzeciwu.

7 Rejestr informacji, podwykonawcy i co wysłać

Prośba o dane do rejestru informacji to obowiązek banku z art. 28 ust. 3 DORA. Wzory rejestru określa rozporządzenie wykonawcze (UE) 2024/2956.

Bank wpisze Twoje dane identyfikacyjne, opis usług ICT i funkcji, które wspierają, kraje świadczenia usługi i przetwarzania danych oraz łańcuch podwykonawców z rangą w łańcuchu. Przygotuj to raz, w rejestrze usług i rejestrze podwykonawców, a potem odpowiadaj wyciągiem w formacie klienta.

Przy usługach wspierających funkcje krytyczne lub istotne bank zapyta, czy umiesz zidentyfikować i nadzorować istotnych podwykonawców, czy przenosisz na nich wymagania (bezpieczeństwo, incydenty, audyt, ciągłość, wyjście) i czy uprzedzisz o zmianie podwykonawcy z prawem sprzeciwu. Chmura publiczna, zewnętrzny SOC, firma od backupu i freelancer z dostępem do produkcji to też podwykonawcy.

Co wysłać, a czego nie

PROŚBA KLIENTA	WYŚLIJ	NIE WYSYŁAJ
Ankieta	Odpowiedzi w formacie klienta z dowodami; poufne po NDA.	Odpowiedzi ze statusem LUKA bez decyzji Zarządu.
Polityki i procedury	PDF zatwierdzonej polityki, procedury incydentów i planu ciągłości; reszta na żądanie.	Plików DOCX, wersji z pustymi polami i przykładami.
Aneks	Komentarze do aneksu przygotowane z checklisty.	Samej checklisty z czerwonymi liniami.
Rejestr informacji	Wyciąg z rejestru usług i podwykonawców w formacie klienta.	Danych o innych klientach.
Ryzyka, szkolenia, testy	Podsumowanie albo wgląd podczas audytu.	Pełnego rejestru ryzyk.

8 Klient objęty NIS2

Szpital, wodociągi, spółka energetyczna, przewoźnik albo samorząd, który jest podmiotem kluczowym lub ważnym, przenosi na dostawców wymagania łańcucha dostaw trzema kanałami: ankietą, umową i audytem.

Według przepisów przejściowych podmioty spełniające kryteria w dniu wejścia w życie nowelizacji mają rok na wdrożenie obowiązków, czyli do 3 kwietnia 2027 r. Klienci będą więc oczekiwać gotowości dostawców przed tą datą. Poważne incydenty klient zgłasza przez system S46: wczesne ostrzeżenie w 24 godziny, zgłoszenie w 72 godziny, sprawozdanie końcowe w miesiąc, i zapyta Cię o dane do tych zgłoszeń.

Najpierw sprawdź, czy Twoja firma sama nie jest podmiotem kluczowym lub ważnym. Dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa są nimi niezależnie od wielkości, a od średniej wielkości także dostawcy usług zarządzanych, chmury i centrów danych. Wtedy masz własne obowiązki ustawowe, szersze niż wymagania klienta; sprawdź to z prawnikiem.

Wspólny rdzeń. Ankiety NIS2 pytają o to samo co banki: politykę, ryzyko, incydenty, ciągłość i kopie, dostęp i MFA, podatności, podwykonawców, szkolenia i audyt. Różnią się terminy, podstawa prawna i kilka pytań krajowych, na przykład o informację z Krajowego Rejestru Karnego dla osób realizujących zadania u klienta.

Co dalej

Bezpłatna próbka pakietów (pełna mapa ankiety banku na 40 pytań, rejestr podwykonawców, mapa wymagań klienta NIS2 na 30 pytań, rejestr aktywów i usług), bezpłatna analiza luk DORA i NIS2 oraz pakiety Dostawca DORA Start i Dostawca NIS2 Start: realsec.pl/dla-dostawcow-ict

Pytania: kontakt@realsec.pl