DOŚWIADCZENIA Z WDRAŻANIA ROZPORZĄDZENIA DORA PRZEZ BANKI KOMERCYJNE W POLSCE: DOBRE PRAKTYKI, WYZWANIA I REKOMENDACJE

prof. UEP dr hab. Krzysztof Waliszewski – kierownik zespołu
Dr Michał Nowakowski
Dr Marcin Idzik

SYGN. PAB/WIB 5/2026

ISBN 978-83-979917-8-1

Raport opracowany na zlecenie Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości

PROGRAM ANALITYCZNO BADAWCZY

O raporcie

Raport **„Doświadczenia z wdrażania Rozporządzenia DORA przez banki komercyjne w Polsce: dobre praktyki, wyzwania i rekomendacje”** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości.

Autorzy

Krzysztof Waliszewski – profesor Uniwersytetu Ekonomicznego w Poznaniu w Instytucie Finansów w Katedrze Pieniądza i Bankowości, dr hab. nauk ekonomicznych w dyscyplinie ekonomia i finanse. Jego pionierskie badania naukowe koncentrują się na zastosowaniu nowoczesnych technologii w finansach, w szczególności na cyfrowym planowaniu finansów osobistych, automatycznym i hybrydowym doradztwie finansowym (robo-advisory), innowacyjnych modelach pośrednictwa finansowego oraz rozwoju rynku FinTech. W swoich pracach analizuje wpływ algorytmów, sztucznej inteligencji i platform cyfrowych na zachowania finansowe gospodarstw domowych oraz na przyszłość doradztwa finansowego. Recenzent książek, monografii, rozpraw doktorskich oraz licznych artykułów naukowych, w tym dotyczących cyfrowych usług finansowych i FinTech. Jest laureatem prestiżowej Nagrody Prezesa Polskiej Akademii Nauk za wybitne osiągnięcia w zakresie finansów. Członek Prezydium Komitetu Nauk o Finansach PAN (2020-2023, 2024-2027), członek Rady Doradczej Finax, członek Doradczego Komitetu Naukowego przy Rzeczniku Finansowym (2023-2026). Prezes Zarządu Europejskiej Federacji Doradców Finansowych EFFP Polska. Współautor 2 raportów technologicznych wydanych w ramach Programu Analityczno-Badawczego WIB: *Wpływ nowoczesnych technologii na zmianę modeli biznesowych banków* (2022) oraz *Nowoczesne metody wspomagania zarządzania finansami osobistymi na przykładzie usługi robo-advice* (2024).

Marcin Idzik – doktor nauk ekonomicznych, adiunkt w Instytucie Finansów Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie. Od ponad dwóch dekad związany z sektorem finansowym oraz badaniami społeczno-ekonomicznymi. Autor ponad 130 publikacji naukowych i opracowań eksperckich z zakresu bankowości, zastosowań metod ilościowych w badaniach ekonomicznych, koniunktury gospodarczej oraz rynków finansowych. Specjalizuje się w doradztwie strategicznym opartym na badaniach empirycznych, w szczególności w obszarach rozwoju rynku bankowego, regulacji finansowych, reputacji sektorowej oraz zachowań konsumentów na rynku usług finansowych. Jest ekspertem w zakresie badań koniunktury gospodarczej, prognozowania ekonomicznego oraz zarządzania reputacją branż i sektorów gospodarki. Badania empiryczne realizuje w formule kompleksowych projektów badawczych, którymi kieruje jako lider merytoryczny i metodologiczny, we współpracy z największymi instytucjami badawczymi oraz czołowymi agencjami badawczymi w Polsce. Projekty te są prowadzone na potrzeby banków i instytucji okołobankowych i stanowią bezpośrednie zaplecze decyzyjne dla zarządów oraz kadry menedżerskiej. Od 2002 roku realizuje i nadzoruje projekty badawcze dotyczące funkcjonowania rynku bankowego, zachowań finansowych Polaków oraz wizerunku i zaufania do instytucji finansowych. Jako ekspert i komentator aktywnie uczestniczy w debacie publicznej poświęconej stabilności sektora finansowego, odporności regulacyjnej oraz wyzwaniom stojącym przed bankowością. Jest prelegentem konferencji naukowych i branżowych, członkiem komitetów redakcyjnych czasopism naukowych oraz autorem ekspertyz i analiz wykorzystywanych w procesach decyzyjnych instytucji finansowych i organizacji branżowych.

Michał Nowakowski r.pr. – architekt rozwiązań prawnych i biznesowych w obszarze danych oraz projektów AI & Data. Legal Architect i współzałożyciel spółki GovernedAI dostarczającej rozwiązania w zakresie bezpiecznej i efektywnej biznesowo sztucznej inteligencji Doradza instytucjom finansowym w tworzeniu rozwiązań AI oraz Data Governance oraz dostosowania prawnego do wymogów sektorowych, jak również uporządkowania kwestii zarządzania ryzykiem ICT. Przeprowadził liczne wdrożenia w zakresie DORA, zarówno dla instytucji finansowych, jak i dostawców ICT. Jest autorem książek, w tym „*Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych*”, „*Sztuczna inteligencja. Wybrane aspekty zarządzania projektami AI & Data*” czy „*Komentarza do ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*”. Wykłada m.in. na studiach podyplomowych w zakresie controllingu i finansów na Akademii Leona Koźmińskiego czy Uniwersytecie SWPS. Jest współtwórcą Akademii Zarządzania Sztuczną Inteligencją przy Fundacji IT Leader Club.

O programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 r. jako odpowiedź na potrzeby sektora bankowego w zakresie wysokiej jakości analiz i badań z obszaru cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz – w ostateczności – kreowania wartości dla klientów – końcowych użytkowników bankowości.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- **Nowe technologie w sektorze bankowym, cyberbezpieczeństwo banków i systemy płatnicze**
- **Ekonomiczna analiza rozwoju sektora bankowego, stabilności banków, otoczenia makroekonomicznego**
- **Prawno-regulacyjne i legislacyjne uwarunkowania działalności sektora bankowego oraz wyzwania wynikające z orzecznictwa sądów krajowych i europejskich**
- **ESG i sustainable finance**
- **Prace analityczno-badawcze w zakresie poszczególnych obszarów funkcjonowania banków oraz w zakresie funkcjonowania wskaźników referencyjnych**

Więcej na temat działalności programu na stronie www.pabwib.pl

Kontakt

dr Tomasz Pawlonka
Dyrektor Programu
m: 505 917 778
e: tpawlonka@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

dr Radosław Ciukaj
m: 784 680 685
e: radoslaw.ciukaj@zbp.pl

dr Agnieszka Wicha
m: 661 646 474
e: agnieszka.wicha@zbp.pl

Bartosz Przyborowski
m: 795 933 104
e: bartosz.przyborowski@zbp.pl

Spis treści

1. Streszczenie wykonawcze

1.1 Krótkie podsumowanie najważniejszych wniosków

Rozporządzenie DORA stanowi jedno z najistotniejszych wyzwań regulacyjnych dla sektora bankowego w ostatnich latach, redefiniując podejście do zarządzania ryzykiem ICT oraz odpornością operacyjną. Zgodnie z art. 3 pkt. 1 rozporządzenia DORA przez cyfrową odporność operacyjną rozumie się zdolność podmiotu finansowego do budowania, gwarantowania i weryfikowania swojej integralności operacyjnej z technologicznego punktu widzenia przez zapewnianie, bezpośrednio albo pośrednio (korzystając z usług zewnętrznych dostawców usług ICT), pełnego zakresu możliwości w obszarze ICT niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy i które wspierają ciągłe świadczenie usług finansowych oraz ich jakość, w tym w trakcie zakłóceń.[1] Przeprowadzone w ramach raportu analizy regulacyjne oraz badania empiryczne wskazują, że banki komercyjne w Polsce w zdecydowanej większości podjęły intensywne działania przygotowawcze do wdrożenia DORA, **jednak poziom faktycznej gotowości pozostaje zróżnicowany**.

Przedstawione wnioski opierają się na analizie regulacyjnej oraz badaniu empirycznym o charakterze eksploracyjnym i sektorowym, którego celem była identyfikacja trendów wdrożeniowych i doświadczeń instytucji finansowych, a nie przeprowadzenie formalnej, audytowej oceny zgodności regulacyjnej lub odporności operacyjnej.

Najbardziej zaawansowane w procesie wdrożenia są duże banki o wysokiej dojrzałości organizacyjnej i technologicznej, które już wcześniej dysponowały rozbudowanymi systemami zarządzania ryzykiem ICT, bezpieczeństwem informacji oraz ciągłością działania. W ich przypadku DORA pełni przede wszystkim funkcję **standaryzującą i porządkującą**, wzmacniając istniejące ramy zarządcze. Mniejsze i średnie banki napotykają natomiast większe trudności, zarówno o charakterze organizacyjnym, jak i kompetencyjnym, co zwiększa ryzyko traktowania wdrożenia DORA w sposób czysto formalny.

Z perspektywy operacyjnej kluczowym wyzwaniem okazało się **zarządzanie ryzykiem zewnętrznych dostawców usług ICT (Third-Party Risk)**. Skala outsourcingu technologicznego w sektorze bankowym, w szczególności w obszarze usług chmurowych, powoduje, że DORA wymagała od banków przeprowadzenia szeroko zakrojonej rewizji relacji kontraktowych, klasyfikacji usług ICT oraz stworzenia rejestrów umów zgodnych z aktami wykonawczymi. Proces ten był dodatkowo utrudniony przez opóźnienia w publikacji standardów technicznych oraz ograniczoną gotowość części dostawców ICT do akceptacji nowych, bardziej restrykcyjnych wymogów umownych.

Istotnym wnioskiem raportu jest także wskazanie na **znaczną niepewność interpretacyjną**, z jaką mierzyły się banki w trakcie przygotowań do stosowania DORA. Opóźnione przyjmowanie aktów delegowanych, brak jednoznacznych wytycznych na poziomie krajowym oraz równoległe funkcjonowanie innych regulacji (w szczególności NIS2) powodowały trudności w ustaleniu właściwego zakresu obowiązków i priorytetów wdrożeniowych. W praktyce prowadziło to do zachowawczego podejścia banków, polegającego na przyjmowaniu maksymalnie szerokiej interpretacji wymogów regulacyjnych, co zwiększało koszty i obciążenia organizacyjne.

DORA wyraźnie **wzmacnia rolę organów zarządzających**, czyniąc odporność cyfrową elementem odpowiedzialności strategicznej zarządów i rad nadzorczych. Ryzyko ICT przestaje być postrzegane jako domena wyspecjalizowanych jednostek technicznych, a staje się integralnym elementem ładu korporacyjnego, zarządzania ryzykiem oraz długoterminowej stabilności instytucji finansowych. Wymaga to podnoszenia kompetencji decyzyjnych kadry kierowniczej oraz lepszej integracji obszarów biznesowych, technologicznych i compliance.

Pomimo znacznych kosztów wdrożenia, banki coraz częściej postrzegają DORA nie tylko jako obowiązek regulacyjny, lecz także jako **szansę na realne wzmocnienie odporności operacyjnej**, poprawę jakości zarządzania ryzykiem ICT oraz zwiększenie zaufania klientów i regulatorów. W dłuższej perspektywie regulacja ta może przyczynić się do zwiększenia stabilności całego sektora finansowego oraz ograniczenia ryzyka zakłóceń o charakterze systemowym.

1 A. Lachosik, DORA jako prawny instrument ochrony cyfrowego bezpieczeństwa rynku finansowego, Studia Prawnoustrojowe, nr 62/2023.

1.2 Kluczowe rekomendacje dla interesariuszy (banki, regulatorzy, dostawcy ICT)

Rekomendacje dla banków

Banki powinny traktować wdrożenie DORA jako **proces ciągły**, a nie jednorazowy projekt regulacyjny zakończony formalnym spełnieniem wymogów. Kluczowe znaczenie ma trwałe włączenie odporności cyfrowej do strategii biznesowej, systemu zarządzania ryzykiem oraz kultury organizacyjnej. Niezbędne jest wzmocnienie roli zarządów w nadzorze nad ryzykiem ICT, w tym zapewnienie im dostępu do rzetelnych informacji zarządczych oraz regularnych ocen poziomu odporności operacyjnej.

Szczególną uwagę banki powinny poświęcić **zarządzaniu relacjami z dostawcami ICT**, w tym segmentacji dostawców według krytyczności świadczonych usług oraz standaryzacji podejścia kontraktowego. Wykorzystywanie dobrych praktyk sektorowych, takich jak rekomendacje i wzorcowe klauzule opracowywane przez organizacje branżowe, może znacząco ograniczyć koszty transakcyjne i ryzyko negocjacyjne. Jednocześnie banki powinny inwestować w rozwój kompetencji wewnętrznych w obszarze cyberbezpieczeństwa, testowania odporności oraz zarządzania incydentami ICT.

Rekomendacje dla regulatorów i organów nadzorczych

Organy nadzorcze powinny kontynuować działania wspierające sektor bankowy poprzez **zwiększanie przejrzystości interpretacyjnej** przepisów DORA. Szczególnie pożądane są praktyczne wyjaśnienia, zestawy Q&A oraz przykłady dobrych praktyk, które pozwolą ograniczyć rozbieżności interpretacyjne i ryzyko nadmiernie zachowawczych wdrożeń.

W praktyce nadzorczej istotne znaczenie powinno mieć realne stosowanie **zasady proporcjonalności**, uwzględniającej skalę działalności, profil ryzyka oraz znaczenie systemowe poszczególnych instytucji. Dialog z sektorem bankowym, w tym konsultacje i inicjatywy edukacyjne, powinien być postrzegany jako kluczowy element skutecznego nadzoru, sprzyjający podnoszeniu faktycznego poziomu odporności operacyjnej, a nie wyłącznie formalnej zgodności regulacyjnej.

Rekomendacje dla dostawców ICT

Dostawcy usług ICT powinni aktywnie dostosowywać swoje modele biznesowe, organizacyjne i kontraktowe do wymogów DORA, traktując regulację jako **długoterminowy standard rynkowy**, a nie przejściowe obciążenie. Zwiększenie transparentności w obszarze bezpieczeństwa, ciągłości działania oraz zarządzania incydentami może stać się istotnym elementem budowania zaufania i przewagi konkurencyjnej wobec instytucji finansowych.

Kluczowe znaczenie ma także rozwijanie kompetencji w zakresie współpracy regulacyjnej oraz zrozumienie specyfiki ryzyk sektora bankowego. Dostawcy, którzy będą w stanie skutecznie wspierać banki w realizacji obowiązków wynikających z DORA, mogą stać się strategicznymi partnerami w budowie odpornego ekosystemu finansowego.

2. Wprowadzenie

Postępująca cyfryzacja sektora finansowego, rosnąca zależność instytucji bankowych od technologii informacyjno-komunikacyjnych (ICT) oraz dynamiczny wzrost liczby i skali cyberzagrożeń sprawiają, że odporność operacyjna stała się jednym z kluczowych elementów stabilności systemu finansowego. Incydenty ICT – w tym cyberataki, awarie systemów czy problemy związane z dostawcami zewnętrznymi – mogą prowadzić nie tylko do zakłóceń działalności pojedynczych instytucji, lecz także do efektów systemowych, zagrażających zaufaniu klientów i bezpieczeństwu całego rynku finansowego.

W odpowiedzi na te wyzwania Unia Europejska przyjęła Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie cyfrowej odporności operacyjnej sektora finansowego (DORA – Digital Operational Resilience Act). Akt ten wprowadza jednolite ramy regulacyjne w zakresie zarządzania ryzykiem ICT, raportowania incydentów, testowania odporności cyfrowej oraz nadzoru nad dostawcami usług ICT, w tym dostawcami o znaczeniu krytycznym. DORA ma charakter horyzontalny i obejmuje szerokie spektrum podmiotów sektora finansowego, w tym banki komercyjne, które są jednym z kluczowych adresatów nowych obowiązków regulacyjnych.

Niniejszy raport koncentruje się na ocenie stopnia przygotowania banków komercyjnych do wdrożenia rozporządzenia DORA, identyfikacji głównych wyzwań wdrożeniowych oraz wskazaniu dobrych praktyk, które mogą wspierać sektor bankowy w osiągnięciu zgodności regulacyjnej przy jednoczesnym wzmacnianiu faktycznej odporności operacyjnej.

2.1. Cel i zakres raportu

Zakres podmiotowy raportu obejmuje banki komercyjne działające w Polsce objęte obowiązkiem wdrożenia rozporządzenia DORA

W ramach raportu jego autorzy zidentyfikowali cel główny i cele szczegółowe przyczyniające się do osiągnięcia celu głównego. Celem głownym raprtu jest przedstawienie stanu przygotowania banków komercyjnych w Polsce do wdrażania Rozporządzenia DORA, identyfikacja głównych wyzwań i dobrych praktyk oraz sformułowanie rekomendacji dla banków, regulatorów i dostawców ICT w zakresie zwiększania odporności cyfrowej sektora finansowego.

Cele szczegółowe raportu:

- Wyjaśnienie znaczenia Rozporządzenia DORA w kontekście regulacyjnym i jego wpływu na sektor bankowy w Polsce.
- Analiza poziomu przygotowania banków komercyjnych do spełnienia wymogów DORA na podstawie badań empirycznych (ankiety, wywiady, konsultacje).
- Zidentyfikowanie kluczowych wyzwań organizacyjnych, technologicznych i regulacyjnych związanych z implementacją DORA.
- Wskazanie dobrych praktyk i narzędzi ICT wspierających skuteczne wdrożenie regulacji.
- Opracowanie rekomendacji dla banków, regulatorów i dostawców ICT dotyczących efektywnego zarządzania wdrożeniem oraz współpracy w zakresie odporności cyfrowej.
- Określenie obszarów wymagających dalszych analiz, doprecyzowania przepisów lub standaryzacji.

Tak sformułowane cele raportu są **ważne i doniosłe dla instytucji finansowych podlegających DORA** , ponieważ bezpośrednio odpowiadają na kluczowe wyzwania regulacyjne, operacyjne i strategiczne, z jakimi sektor bankowy mierzy się w związku z wdrożeniem rozporządzenia DORA. Ich znaczenie można uzasadnić w kilku komplementarnych wymiarach:

1. Odpowiedź na obowiązek regulacyjny o charakterze systemowym

Rozporządzenie DORA wprowadza jednolite, bezpośrednio stosowane wymogi prawa unijnego, których niespełnienie wiąże się z ryzykiem sankcji nadzorczych, reputacyjnych oraz operacyjnych. Realizacja celu głównego raportu umożliwia instytucjom finansowym obiektywne zidentyfikowanie luki zgodności (compliance gap) pomiędzy stanem obecnym a wymaganiami regulacyjnymi. Dla instytucji finansowych podlegających DORA oznacza to realne wsparcie w minimalizacji ryzyka regulacyjnego.

2. Przełożenie wymogów regulacyjnych na praktykę operacyjną

Raport nie ogranicza się do analizy norm prawnych, lecz koncentruje się na praktycznych aspektach wdrożenia – takich jak zarządzanie ryzykiem ICT, raportowanie incydentów czy testowanie odporności operacyjnej. Dla banków ma to kluczowe znaczenie, ponieważ DORA wymaga integracji regulacji z codziennym funkcjonowaniem organizacji, a nie jedynie formalnego spełnienia obowiązków dokumentacyjnych.

3. Wsparcie zarządzania strategicznego i decyzyjnego

Raport dostarcza bankom materiału porównawczego (benchmarkingowego), pozwalającego ocenić własny poziom przygotowania na tle innych `instytucji o podobnym profilu. Jest to szczególnie istotne dla zarządów i kadry kierowniczej, które ponoszą bezpośrednią odpowiedzialność za wdrożenie DORA i muszą podejmować decyzje dotyczące alokacji zasobów, priorytetyzacji projektów oraz akceptacji ryzyka.

4. Identyfikacja kluczowych ryzyk i kosztów wdrożenia

Raport obejmuje analizę wyzwań organizacyjnych, technologicznych i kosztowych, które są doniosłe, ponieważ wdrożenie DORA wiąże się z istotnymi nakładami finansowymi oraz zmianami strukturalnymi. Banki, dysponując syntetyczną analizą tych wyzwań, mogą lepiej planować budżety, harmonogramy oraz strategie transformacji cyfrowej, ograniczając ryzyko nieefektywnych lub nadmiarowych inwestycji.

5. Uporządkowanie relacji z dostawcami ICT

Szczególne znaczenie ma uwzględnienie w raporcie zagadnień zarządzania ryzykiem zewnętrznym (Third-Party Risk). Dla banków , silnie uzależnionych od outsourcingu ICT i usług chmurowych, właściwe wdrożenie DORA w tym obszarze ma charakter krytyczny. Cele raportu wspierają banki w zrozumieniu, jak nowe wymogi wpływają na modele współpracy z dostawcami oraz jakie zmiany kontraktowe i organizacyjne są konieczne.

6. Redukcja niepewności interpretacyjnej

Jednym z największych wyzwań związanych z DORA są wątpliwości interpretacyjne wynikające z ogólnego charakteru części przepisów oraz stopniowego publikowania aktów wykonawczych. Dlatego raport obejmuje analizę doświadczeń banków oraz relacji z organami nadzorczymi, przyczyniając się do ograniczenia tej niepewności poprzez identyfikację wspólnych problemów interpretacyjnych i oczekiwań nadzorczych.

7. Wzmocnienie faktycznej odporności operacyjnej sektora

W dłuższej perspektywie zagadnienia opisane w raporcie mają znaczenie wykraczające poza samą zgodność regulacyjną. Skoncentrowanie się na odporności operacyjnej, testach odporności cyfrowej oraz dojrzałości procesów ICT wspiera banki w budowie realnej zdolności do reagowania na zakłócenia, co przekłada się na bezpieczeństwo klientów, stabilność rynku oraz zaufanie do sektora bankowego.

Podsumowując, realizacja celów raportu jest ważna dla instytucji finansowych podlegających DORA, ponieważ łączą one perspektywę regulacyjną z praktyką operacyjną i strategiczną, dostarczając narzędzi analitycznych niezbędnych do skutecznego, efektywnego kosztowo i nadzorczego wdrożenia rozporządzenia DORA.

2.2 Znaczenie DORA w kontekście sektora bankowego

Rozporządzenie DORA stanowi jeden z kluczowych elementów unijnej strategii wzmacniania stabilności i bezpieczeństwa sektora finansowego w dobie postępującej cyfryzacji. W kontekście sektora bankowego jego znaczenie jest szczególnie istotne, gdyż banki należą do instytucji najbardziej uzależnionych od technologii informacyjno-komunikacyjnych oraz w największym stopniu narażonych na skutki zakłóceń operacyjnych, awarii systemów informatycznych oraz cyberataków. DORA wprowadza jednolite ramy prawne, których celem jest zwiększenie odporności operacyjnej banków oraz ograniczenie ryzyka systemowego wynikającego z rosnącej cyfrowej zależności sektora finansowego.

Jednym z najważniejszych aspektów DORA jest ujednolicenie wymogów regulacyjnych w obszarze zarządzania ryzykiem ICT na poziomie całej Unii Europejskiej. Przed wejściem w życie rozporządzenia banki funkcjonowały w środowisku zróżnicowanych regulacji krajowych oraz wytycznych sektorowych, co prowadziło do niespójności interpretacyjnych i nierównego poziomu odporności operacyjnej pomiędzy instytucjami. DORA eliminuje te rozbieżności, wprowadzając jednolite standardy w zakresie zarządzania incydentami ICT, testowania odporności cyfrowej, raportowania oraz nadzoru nad dostawcami zewnętrznymi usług ICT.

DORA istotnie wzmacnia również rolę ładu korporacyjnego w bankach, jednoznacznie przypisując odpowiedzialność za odporność cyfrową organom zarządzającym. Oznacza to, że ryzyko ICT przestaje być postrzegane wyłącznie jako zagadnienie techniczne, a staje się integralnym elementem zarządzania strategicznego i ryzykiem operacyjnym. W praktyce wymusza to większe zaangażowanie zarządów i rad nadzorczych w nadzór nad infrastrukturą technologiczną, bezpieczeństwem informacji oraz ciągłością działania, a także podnoszenie kompetencji decyzyjnych w tym obszarze.

Istotne znaczenie DORA dla sektora bankowego wiąże się również z regulacją relacji z dostawcami zewnętrznymi usług ICT. Banki w coraz większym stopniu korzystają z outsourcingu technologicznego, w tym rozwiązań chmurowych, co zwiększa efektywność operacyjną, ale jednocześnie generuje nowe rodzaje ryzyka. DORA wprowadza kompleksowe ramy zarządzania ryzykiem stron trzecich, obejmujące cały cykl życia relacji outsourcingowej oraz umożliwia nadzór regulacyjny nad kluczowymi dostawcami technologii. Ma to istotne znaczenie dla ograniczenia ryzyka koncentracji oraz wzmocnienia odporności całego ekosystemu bankowego.

Z perspektywy stabilności finansowej DORA pełni także funkcję prewencyjną, zmniejszając prawdopodobieństwo wystąpienia zakłóceń o charakterze systemowym. Obowiązek regularnego testowania odporności operacyjnej, w tym przeprowadzania zaawansowanych testów penetracyjnych opartych na scenariuszach zagrożeń, pozwala bankom na wcześniejszą identyfikację słabych punktów oraz doskonalenie zdolności reagowania na incydenty. W dłuższej perspektywie przekłada się to na większą stabilność sektora oraz wzrost zaufania klientów i regulatorów do banków jako instytucji zaufania publicznego.

Podsumowując, znaczenie DORA w kontekście sektora bankowego wykracza poza ramy klasycznej regulacji technicznej. Rozporządzenie to stanowi istotny element transformacji sposobu zarządzania ryzykiem operacyjnym i cyfrowym w bankach, przyczyniając się do wzmocnienia ich odporności, stabilności oraz zdolności do funkcjonowania w coraz bardziej złożonym i cyfrowym środowisku finansowym.

2.3 Metodyka przygotowania raportu

W celu realizacji założonych celów raportu zastosowano zróżnicowaną metodykę badawczą, łączącą analizę źródeł wtórnych z badaniem empirycznym. Takie podejście umożliwiło zarówno osadzenie analiz w obowiązującym kontekście regulacyjnym, jak i ocenę praktycznego poziomu przygotowania banków komercyjnych do wdrożenia rozporządzenia DORA.

Podstawę analizy teoretyczno-regulacyjnej stanowił przegląd literatury przedmiotu, obejmujący publikacje naukowe oraz opracowania eksperckie dotyczące zarządzania ryzykiem ICT, odporności operacyjnej oraz regulacji sektora finansowego. Uzupełniająco przeanalizowano akty prawne krajowe i unijne, ze szczególnym uwzględnieniem rozporządzenia DORA oraz powiązanych regulacji i wytycznych nadzorczych. Istotnym elementem analizy były również raporty nadzorcze krajowe i unijne (w tym publikacje organów takich jak KNF, EBA, ESMA i EIOPA), a także raporty branżowe, dostarczające aktualnych danych na temat praktyk rynkowych i wyzwań wdrożeniowych.

Empiryczna część badania została przeprowadzona z wykorzystaniem techniki CAWI (Computer-Assisted Web Interviewing). Dobór próby miał charakter celowy i obejmował banki komercyjne działające na rynku polskim. Głównym kryterium doboru był fakt notowania banku na Giełdzie Papierów Wartościowych w Warszawie, co pozwoliło skoncentrować analizę na instytucjach o istotnym znaczeniu rynkowym, wysokim poziomie formalizacji procesów oraz zwiększonych obowiązkach informacyjnych i nadzorczych.

W wyniku przeprowadzonego badania uzyskano kompletne odpowiedzi od 6 banków, wśród których 5 to banki notowane na GPW, co umożliwiło przeprowadzenie analizy porównawczej poziomu przygotowania do wdrożenia rozporządzenia DORA oraz

identyfikację kluczowych różnic i wspólnych tendencji występujących w sektorze bankowym. Zastosowana metodyka zapewnia adekwatność i wiarygodność wniosków, a także pozwala na formułowanie rekomendacji opartych zarówno na przesłankach regulacyjnych, jak i doświadczeniach praktycznych badanych instytucji.

Wyniki badania empirycznego należy interpretować z uwzględnieniem określonych ograniczeń metodologicznych, charakterystycznych dla badań ankietowych i eksploracyjnych prowadzonych na wczesnym etapie implementacji nowych regulacji.

Badanie opierało się na deklaratywnej samoocenie instytucji uczestniczących w badaniu. Tego rodzaju podejście jest standardowo stosowane w analizach wdrożeń regulacyjnych, szczególnie w fazie przygotowawczej, jednak jego ograniczeniem jest możliwość występowania efektu subiektywnej oceny poziomu przygotowania oraz koncentracji na formalnych aspektach zgodności regulacyjnej.

Dobór próby miał charakter celowy i obejmował banki o istotnym znaczeniu rynkowym, w szczególności banki notowane na Giełdzie Papierów Wartościowych w Warszawie. Celem takiego podejścia było uzyskanie pogłębionego wglądu w praktykę wdrażania DORA w instytucjach o wysokim poziomie dojrzałości organizacyjnej, a nie zapewnienie reprezentatywności statystycznej dla całego sektora bankowego.

Raport koncentruje się przede wszystkim na poziomie organizacyjno-zarządczym i regulacyjnym wdrażania DORA, a nie na technicznej weryfikacji rzeczywistej odporności operacyjnej systemów ICT poszczególnych instytucji, co wymagałoby zastosowania metod audytowych, testów technicznych lub bezpośredniej analizy infrastruktury ICT, wykraczających poza zakres niniejszego opracowania.

W konsekwencji raport należy interpretować przede wszystkim jako opracowanie o charakterze analityczno-eksploracyjnym i sektorowym, identyfikujące kierunki przygotowań, główne wyzwania oraz dobre praktyki wdrożeniowe, a nie jako formalny audyt zgodności regulacyjnej ani kompleksową ocenę operacyjnej odporności cyfrowej całego sektora bankowego.

Jednocześnie, ze względu na dobór instytucji o istotnym znaczeniu rynkowym oraz łączenie wyników z analizą regulacyjną i raportami nadzorczymi, przedstawione wnioski stanowią wiarygodne źródło wiedzy o kluczowych trendach i kierunkach wdrażania DORA.

3. Kontekst regulacyjny Rozporządzenia DORA

3.1 Cel i znaczenie Rozporządzenia DORA

Rozporządzenie (EU) 2022/2554 („DORA") jest wyraźną odpowiedzią na brak jednolitych standardów w zakresie zarządzania ryzykiem ICT w sektorze finansowym. Brak takiego podejścia przed przyjęciem przepisów DORA powodował, że w państwach członkowskich można było zidentyfikować wiele rozbieżności w zakresie interpretacji obowiązków, które powinien realizować podmiot finansowy.

Sytuację komplikował również fakt, że pomimo funkcjonowania w „obrocie regulacyjnym" wytycznych wydawanych przez unijne organy, jak Europejski Urząd Nadzoru Bankowego (EUNB), krajowe organy nadzorcze nierzadko wprowadzały własne podejście, które nierzadko utrudniało prowadzenie działalności transgranicznej przez podmioty z siedzibą w innych krajach. Przykładem może być tutaj chociażby Komunikat Urzędu Komisji Nadzoru Finansowego („UKNF") dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej[2], który choć dawał większe poczucie pewności w zakresie oczekiwań nadzorcy, to jednak często był odbierany jako nadmiarowy i niekiedy sprzeczny z podejściem EUNB. Komunikat został uchylony w związku ze stosowaniem przepisów DORA.

Rozporządzenie stanowi także odpowiedź na wyzwania związane z postępującą cyfryzacją gospodarek i społeczeństw, a także rosnącymi zagrożeniami[3] cybernetycznymi, na które narażone są zarówno instytucje finansowe, jak i ich klienci. DORA ma więc na celu wzmocnienie odporności cyfrowej, która ma przyczynić się do zmniejszenia skali zdarzeń i incydentów, które mogą przekładać się na stabilność instytucji (a nawet całych systemów) oraz ich wyniki finansowe, które mogą być narażone na uszczerbek, zarówno wobec konieczności pokrywania strat poniesionych przez klientów w wyników oszustów (fraudów), jak również utraty reputacji i odpływu klientów.

Zauważyć przy tym należy, że niekiedy widoczne są rozbieżności w zakresie znaczenia DORA zarówno wśród samych podmiotów finansowych (te najbardziej dojrzałe jak banki zazwyczaj nie kwestionują potrzeby uporządkowania i ujednolicenia zasad zarządzania ryzykiem ICT), jak również dostawców usług ICT, którzy w sposób pośredni i bezpośredni zostali objęci omawianymi przepisami. Ci dostawcy nierzadko mogą kontestować oczekiwania podmiotów finansowych w zakresie zobowiązań umownych na dostawę usług ICT traktując je jako nieuzasadnione i nadmiarowe.

Dlatego też tak istotne były i są działania uświadamiające, które pozwalają dostawcom usług na zrozumienie powodów dla których konieczne jest wprowadzenie wysokich standardów bezpieczeństwa w ramach całego łańcucha dostaw.

Nie można jednak nie zauważyć, że w miesiącach poprzedzających moment rozpoczęcia obowiązywania DORA podmioty finansowe, w szczególności te o złożonej architekturze IT oraz szerokim spektrum zewnętrznych dostawców usług ICT, musiały mierzyć się z koniecznością nie tylko rewizji istniejących ram odporności cyfrowej, ale również realizować obowiązki w zakresie modyfikacji kontraktów na dostawę tych usług w niespotykanej dotąd skali. Zadanie to utrudniał fakt, że unijne instytucje oraz organy opóźniły się istotnie z publikacją stosownych aktów delegowanych, które miały istotne znaczenie dla prawidłowej implementacji rozporządzenia. Prowadziło to także do wymuszonej bierności ze strony organów krajowych, które wobec braku aktów wykonawczych nie były w stanie wydać stosownych interpretacji czy wytycznych.

Wydaje się, że takie opóźnienie było też powodem dla którego w Polsce „implementacja" krajowych przepisów[4] instytucjonalnych również przebiegła z pewnym opóźnieniem, powodując, że KNF – w sensie formalnym – pozbawiona była możliwości realizacji obowiązków nadzorczych.

3.2 Zakres przedmiotowy i podmiotowy

Zgodnie z przepisami DORA zasadniczym celem rozporządzenia jest „(...) osiągnięcie wysokiego wspólnego poziomu operacyjnej odporności cyfrowej (...)". Jednocześnie wprowadzane obowiązki mają zmierzać także do podniesienia bezpieczeństwa sieci i systemów ICT, które wspierają procesy biznesowe

2 https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf (dostęp: 12.01.2026 r.).

3 https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_Roczny_CSIRT_KNF_2024_93226.pdf (dostęp: 12.01.2026 r.).

4 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20250001069 (dostęp: 14.01.2026 r.).

Schemat 2. Zakres podmiotowy rozporządzenia DORA

Źródło: Wymagania rozporządzenia DORA dla podmiotów stosujących uproszczone ramy zarządzania ryzykiem związanym z ICT, KNF, 2025, https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/wymagania_rozporzadzenia_dora_dla_podmiotow_stosujacych_uproszczone_ramy_zarzadzania_zwiazanym_z_ryzykiem_ICT?articleId=91236&p_id=18 (dostęp 3.02.2026)

podmiotów finansowych. To zaś oznacza, że choć na DORA należy patrzeć z perspektywy zapewnienia bezpieczeństwa, to jednak – na co wskazują także kolejne przepisy – ważnym „zadaniem" jest wspieranie ciągłości działania podmiotów oraz realizacji ich celów biznesowych.

Z formalnego punktu widzenia DORA odnosi się do następujących zagadnień:

1. Wymogi dotyczące operacyjnego bezpieczeństwa, w tym m.in. mechanizmów zarządzania ryzykiem ICT, tzw. pentestów czy wymiany informacji o zagrożeniach (w rzeczywistości jest to nieco dłuższa lista, która szczegółowo zostanie omówiona w dalszej części raportu),

2. Wymogi w zakresie umów zawieranych przez instytucje finansowe z dostawcami usług ICT,

3. Zasady dotyczące nadzoru nad kluczowymi zewnętrznymi dostawcami[5],

4. Zasady dotyczące współpracy między organami odpowiedzialnymi za nadzór nad stosowaniem przepisów DORA.

Istotne jest przy tym to, że samo rozporządzenie jest zaledwie fundamentem, który obudowany jest licznymi aktami delegowanymi wydanymi przez Komisję (UE) przy aktywnym udziale unijnych organów, w tym EUNB. Do tej kwestii wrócimy jeszcze w dalszej części raportu.

5 Lista podmiotów wyznaczonych przez EUNB i pozostałe unijne organy jako kluczowe znajduje się pod tym linkiem: https://www.esma.europa.eu/sites/default/files/2025-11/List_of_designated_CTPPs.pdf (dostęp: 13.01.2026 r.).

W aspekcie „operacyjnym" możemy stwierdzić, że przedmiotem regulacji DORA jest przede wszystkim stworzenie skutecznych i efektywnych mechanizmów zarządzania ryzykiem ICT dla podmiotów finansowych, ale także całych systemów finansów, które te podmioty tworzą. Przekłada się to więc na takie kwestie jak tworzenie i aktualizowanie strategii, polityk, procedur oraz instrukcji, a także rozwijanie architektury korporacyjnej (organizacyjnej) dostosowanej do wyzwań cyfrowych. To także zobowiązania do budowania świadomości i zapewnienia silnych kompetencji oraz ustanowienie wysokich standardów współpracy pomiędzy podmiotami ze strony popytowej (podmioty finansowe) i podażowej (dostawcy usług ICT).

W DORA znajdziemy definicję „operacyjnej odporności cyfrowej" oznaczającej zdolność podmiotu finansowego do budowania, gwarantowania i weryfikowania swojej operacyjnej integralności i niezawodności przez zapewnienie, bezpośrednio albo pośrednio – korzystając z usług zewnętrznych dostawców ICT – pełnego zakresu możliwości w obszarze ICT niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy i które wspierają ciągłe świadczenie usług finansowych oraz ich jakość, w tym w trakcie zakłóceń.

Rozporządzenie DORA wymienia wprost 21 kategorii podmiotów, do których przepisy tego rozporządzenia mają zastosowanie, a także 6 kategorii podmiotów, do których przepisy rozporządzenia DORA nie mają zastosowania.

Zakres podmiotowy DORA, jest dość szeroki i obejmuje szeroko rozumiane podmioty finansowe, jak instytucje kredytowe, instytucje płatnicze czy zakłady ubezpieczeń (pełen zakres podmiotów określa art. 2 ust. 1 DORA), ale także zewnętrznych dostawców usług ICT. Ci ostatni zostali zdefiniowani w rozporządzeniu i jest to jedna z kluczowych definicji, która wyznacza także zakres podmiotowy stosowania przepisów po „obu stronach".

Dlatego w tym miejscu raportu należy odnieść się do dwóch pojęć, tj. usługi ICT oraz zewnętrznego dostawcy usług ICT, który został opisany dość prosto jako przedsiębiorstwo świadczące usługi ICT. Dlatego ta pierwsza definicja ma zdecydowanie większe znaczenie:

Zgodnie z DORA „usługi ICT" oznaczają usługi cyfrowe i usługi w zakresie danych świadczone w sposób ciągły za pośrednictwem systemów ICT na rzecz co najmniej jednego użytkownika wewnętrznego lub zewnętrznego, łącznie ze sprzętem komputerowym jako usługą i usługami w zakresie sprzętu komputerowego obejmującymi zapewnienie wsparcia technicznego za pośrednictwem aktualizacji oprogramowania lub oprogramowania układowego przez dostawcę sprzętu, z wyłączeniem tradycyjnych usług telefonii analogowej.

Definicja ta, w trakcie dostosowywania się przez sektor bankowy, bo na nim skupia się raport, budziła wiele emocji związanych z nie do końca jasnymi pojęciami „wewnętrznymi". Skutkiem tego i wykonując mandat przewidziany w DORA, Komisja (UE) po stosownych konsultacjach przyjęła Rozporządzenie wykonawcze Komisji (UE) 2024/2956 z dnia 29 listopada 2024 r. ustanawiające wykonawcze standardy techniczne do celów stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do standardowych wzorów na potrzeby rejestru informacji, które w załączniku III prezentuje wykaz usług ICT, które powinny znaleźć się w rejestrze umów, a tym samym stanowi wyraźną wskazówkę co do tego, jak interpretować takie usługi. Jest ich 19:

Rodzaj usług ICT	Opis
1. Zarządzanie projektami ICT	Świadczenie usług związanych z funkcją kierownika projektu
2. Rozwój ICT	Świadczenie usług związanych z: analizą biznesową, projektowaniem i tworzeniem programów komputerowych, testowaniem.
3. Dział pomocy technicznej ICT i wsparcie pierwszej linii	Świadczenie usług związanych z: wsparciem ze strony działu pomocy technicznej i udzielaniem wsparcia pierwszej linii w przypadku incydentów związanych z ICT

Rodzaj usług ICT	Opis
4. Usługi zarządzania bezpieczeństwem ICT	Świadczenie usług związanych z: bezpieczeństwem ICT (ochrona, wykrywanie, reagowanie i przywracanie pracy systemów), w tym reagowanie na incydenty związane z bezpieczeństwem i informatyka śledcza
5. Przekazywanie danych	Subskrypcja usług dostawców danych (usługa w zakresie danych cyfrowych)
6. Analiza danych	Świadczenie usług związanych ze wspieraniem analizy danych (usługa w zakresie danych cyfrowych)
7. ICT, infrastruktura i usługi hostingu (z wyłączeniem usług w chmurze)	Udostępnianie infrastruktury ICT, obiektów i usług hostingu, w tym dostawa mediów (energia, zarządzanie ciepłem itp.), dostęp telekomunikacyjny i bezpieczeństwo fizyczne (z wyłączeniem usług w chmurze), działalność w zakresie przetwarzania płatności lub eksploatacja infrastruktury płatniczej
8. Zasoby obliczeniowe	Zapewnienie zdolności przetwarzania cyfrowego (w tym obliczania danych), z wyłączeniem usług obliczeniowych świadczonych w kontekście środowiska usług przetwarzania w chmurze
9. Przechowywanie danych poza chmurą	Udostępnianie platformy przechowywania danych (z wyłączeniem usług w chmurze)
10. Usługi telekomunikacyjne	Operacje w zakresie systemów telekomunikacyjnych i zarządzania przepływem. Tradycyjne usługi telefonii analogowej są wyraźnie wyłączone na podstawie art. 3 pkt 21 rozporządzenia (UE) 2022/2554
11. Infrastruktura sieciowa	Udostępnianie infrastruktury sieciowej
12. Sprzęt i urządzenia fizyczne	Udostępnianie stacji roboczych, telefonów, serwerów, urządzeń do przechowywania danych, sprzętu itp. w formie usługi
13. Licencjonowanie oprogramowania (z wyłączeniem SaaS)	Dostarczanie oprogramowania użytkowanego stacjonarnie
14. Zarządzanie operacjami ICT (w tym utrzymanie)	Świadczenie usług związanych z: konfiguracją infrastruktury (systemów i sprzętu z wyjątkiem sieci), utrzymaniem, instalowaniem, zarządzaniem zdolnością przepustową, zarządzaniem ciągłością działania itp. W tym dostawcy usług zarządzanych

Rodzaj usług ICT	Opis
15. Doradztwo w zakresie ICT	Świadczenie eksperckich usług intelektualnych / w dziedzinie ICT
16. Zarządzanie ryzykiem związanym z ICT	Weryfikacja zgodności z wymogami w zakresie zarządzania ryzykiem związanym z ICT zgodnie z art. 6 ust. 10 rozporządzenia (UE) 2022/2554
17. Usługi w chmurze: IaaS	Infrastruktura jako usługa
18. Usługi w chmurze: PaaS	Platforma jako usługa
19. Usługi w chmurze: SaaS	Oprogramowanie jako usługa

Problem, który identyfikowały banki w okresie dostosowawczym to spóźniona reakcja organów oraz Komisji, która spowodowała, że rozporządzenie pojawiło się późno, utrudniając bankom ustalanie jaką relację należy uznać za podlegającą DORA, a które nie.

Tak czy inaczej, w oparciu o powyższe definicje banki oraz pozostałe podmioty finansowe były (i nadal są) w stanie ustalić także zakres podmiotowy DORA. Klasyfikacja określonego podmiotu jako zewnętrznego dostawcy usług ICT „triggerowała" obowiązki po stronie tego podmiotu, jak również samego podmiotu finansowego w zakresie rozporządzenia.

W rezultacie wiele instytucji finansowych, szczególnie tych o złożonej architekturze IT oraz danych i sporej zależności od zewnętrznych dostawców, musiało przeprowadzić rewizję nawet kilkuset umów, aby dostosować je do wymagań, które stawia rozporządzenie. Ponieważ DORA wprowadziła także pojęcie krytycznej lub istotnej funkcji w kontekście powierzenia usług ICT, to również i w tym zakresie konieczna była weryfikacja podmiotów i świadczonych przez nich umów. W przypadku „pozytywnej" klasyfikacji, oba podmioty (powierzający i podmiot, któremu powierzano określone działania) musiały zrealizować wyższe wymagania niż w przypadku usług ICT o charakterze „tradycyjnym".

Należy również w tym miejscu zwrócić uwagę na art. 4, który wyznacza w ramach DORA zasadę proporcjonalności. Oznacza ona po prostu, że przy dostosowywaniu się do wymagań DORA podmioty finansowe powinny brać pod uwagę swoją wielkość, ogólny profil ryzyka, charakter, skalę i stopień złożoności swoich usług, działań i operacji. Zasada ta ma szczególne znaczenie w odniesieniu do banków spółdzielczych, które – w porównaniu z dużymi bankami komercyjnymi – prowadzą działalność na mniejszą skalę, funkcjonują w oparciu o bardziej ograniczone zasoby organizacyjne i technologiczne oraz obsługują głównie lokalne społeczności. W praktyce oznacza to, że wdrażanie wymogów DORA przez banki spółdzielcze powinno uwzględniać ich specyfikę modelu biznesowego, w tym niższy poziom złożoności infrastruktury ICT, mniejszą liczbę świadczonych usług cyfrowych czy większe uzależnienie od zewnętrznych dostawców usług technologicznych, często działających w ramach zrzeszeń lub systemów ochrony instytucjonalnej. Proporcjonalność nie zwalnia tych podmiotów z obowiązku zapewnienia odporności cyfrowej, lecz pozwala na takie kształtowanie mechanizmów zarządzania ryzykiem ICT, testowania odporności operacyjnej czy raportowania incydentów, które będą adekwatne do skali ich działalności. W konsekwencji regulacyjne oczekiwania wobec banków spółdzielczych powinny być interpretowane w sposób umożliwiający efektywne spełnienie wymogów DORA bez nakładania nieproporcjonalnych obciążeń organizacyjnych i kosztowych, które mogłyby negatywnie wpłynąć na ich stabilność finansową oraz

zdolność do realizacji lokalnej funkcji społeczno-gospodarczej.

Zasady tej nie należy jednak interpretować w taki sposób, że im mniejszy podmiot, tym mniejsze wymagania, bowiem także mały podmiot, ale mający istotne znaczenie dla (eko)systemu może wymagać najwyższych standardów. Emanacją zasady proporcjonalności są również wyłączenia i uproszczenia, np. w zakresie systemu zarządzania ryzykiem ICT czy pewnych kategorii pośredników ubezpieczeniowych, którzy mogą nie podlegać wymaganiom DORA.

3.3 Kluczowe obowiązki instytucji finansowych wynikające z DORA

Punktem wyjścia dla określenia obowiązków po stronie adresatów DORA jest art. 5. Wymaga on, aby podmioty finansowe posiadały wewnętrzne ramy zarządzania i kontroli, które będą w stanie zapewnić, że dany podmiot jest w stanie skutecznie i ostrożnie zarządzać wszystkimi rodzajami ryzyka związanego z ICT, co ma na koniec przełożyć się na wysoki poziom odporności cyfrowej, czyli swoisty „ultimate goal" DORA.

W efekcie oczekuje się, aby organy zarządzające (tutaj można to intepretować nie tylko jako zarządy, ale również rady nadzorcze lub inne organy o podobnym charakterze, np. rada dyrektorów) odpowiadały (formalnie w zakresie ram odpowiedzialności i faktycznie) za określanie, zatwierdzanie i nadzorowanie wdrażania ram zarządzania ryzykiem ICT.

Rozciąga się to na konieczność m.in. wprowadzania polityk wyznaczających podejście podmiotu do zapewnienia wysokich standardów dostępności, autentyczności, integralności i poufności danych, zapewnienie zasobów, rozdzielenie odpowiedzialności czy też zatwierdzanie i nadzorowanie wdrażania odpowiednich strategii. Rzecz jasna tych obowiązków jest więcej, ale ze względu na ograniczone ramy raportu nie sposób ich wszystkich tutaj wymienić.

Można natomiast stwierdzić, że rola organów zarządzających jest w kontekście DORA nie tylko „formalna" i ograniczająca się do zatwierdzania dokumentacji. Od organów tych wymaga się, aby dysponowały odpowiednią wiedzą i kompetencjami (i na bieżąco ją aktualizowały), które mają przekładać się na lepsze zarządzanie ryzykiem ICT i wysoki poziom odporności. Co ważne, te banki (i oczywiście inne podmioty finansowe również) mają obowiązek wyznaczenia członka kadry kierowniczej wyższego szczebla jako odpowiedzialnego za de facto obowiązki DORA.

Oczywiście rozciągać będzie się to także na wiele obowiązków stricte zarządczych, które związane będą z delegowaniem zadań oraz odpowiedzialności za obszary objęte DORA. Nie oznacza to, że organy te odpowiadają za operacyjne kwestie, ale stają się strażnikiem realizacji i jednocześnie przyjmują na siebie odpowiedzialność za ewentualne niedopatrzenia. Takie ukształtowanie tych zasad powoduje także, że kwestie związane z odpowiednim zarządzaniem ryzykiem ICT stają się kwestią strategiczną i fundamentalną dla banku. Ma to szczególne znaczenie w świecie, który staje się coraz bardziej dano-centryczny i w którym zależności pomiędzy różnymi systemami stają się bardziej złożone.

3.3.1 Zarządzanie ryzykiem ICT

DORA definiuje pojęcie „ryzyka związanego z ICT", które należy rozumieć jako dającą się racjonalnie określić okoliczność związaną z użytkowaniem sieci i systemów informatycznych, która – jeżeli dojdzie do jej urzeczywistnienia – może zagrozić bezpieczeństwu sieci i systemów informatycznych, dowolnego narzędzia lub procesu zależnego od tej technologii, bezpieczeństwu operacji i procesów lub świadczeniu usług poprzez wywoływanie negatywnych skutków w środowisku cyfrowym lub fizycznym.

Innymi słowy, są to zdarzenia, których materializacja może wpłynąć na prawidłowe działanie banku i świadczenie przez ten bank usług, które ma związek z szeroko rozumianym obszarem ICT (teleinformatycznym). Warto przy tym wskazać, że DORA definiuje także „ryzyko ze strony zewnętrznych dostawców ICT", które może być częścią szerszej kategorii ryzyk ICT.

Tak czy inaczej materializacja takiego ryzyka może mieć istotne negatywne konsekwencje dla banku, np. w formie roszczeń o odszkodowanie czy kar nadzorczych, ale także całych systemów finansowych, które są ze sobą często sprzężone. Dlatego problematyka zarządzania ryzykiem ICT została w DORA postawiona niejako w centrum zainteresowania i stanowi punkt wyjścia dla innych obowiązków, które zostaną omówione jeszcze w raporcie.

DORA dość skąpo opisuje oczekiwania w zakresie ram zarządzania ryzykiem ICT, choć niektóre ich elementy zostają doprecyzowane na poziomie aktów

niższego rzędu[6]. Nie jest to wynikiem niedbałości prawodawcy, ale koniecznością ujednolicenia oczekiwań względem podmiotów o zróżnicowanej „naturze" oraz umożliwieniu dopasowania odpowiednich środków do profilu ryzyka i apetytu na to ryzyko.

Dla banków takie ramy zarządzania ryzykiem ICT nie stanowią w zasadzie nowości i wpisują się w już istniejące ramy ogólnego systemu zarządzania ryzykiem, do którego są one zobowiązane chociażby na mocy ustawy Prawo bankowe i aktów wykonawczych. W przypadku DORA większy akcent kładzie się jednak na te zagrożenia, które mają techniczny charakter, choć nie należy tego jednocześnie utożsamiać wyłącznie z koncentracją na oprogramowaniu czy infrastrukturze wykorzystywanej w codziennej działalności.

Adresaci DORA są zobowiązani do zastosowania co najmniej „minimalnego" zestawu podejść i dokumentacji (a w praktyce też konkretnych procesów), do którego należą strategie, polityki, procedury, protokoły i narzędzia ICT, które w założeniu mają chronić zasoby / aktywa ICT, w tym również te fizyczne. Te ramy muszą być udokumentowane w odpowiedni sposób i podlegać regularnemu przeglądowi oraz ewentualnej aktualizacji (zarówno tej przewidzianej, jak i nieprzewidzianej, która może pojawić się np. na skutek konkretnego incydentu ICT). Podlegają one także audytowi, zarówno wewnętrznemu, jak i zewnętrznemu (w określonych przypadkach).

To na co zwraca uwagę DORA to fakt, że ramy zarządzania ryzykiem związanym z ICT muszą obejmować strategię operacyjnej odporności cyfrowej, która powinna określać to, w jaki sposób bank będzie przeciwdziałał materializacji ryzyk. W praktyce te metody określają nam środki, które należy przedsięwziąć w celu ochrony i do których należą m.in. takie działania jak posiadanie odpowiednich rejestrów zasobów oraz architektury rozwiązań czy testowanie odporności, np. poprzez testy penetracyjne.

Praktyczne znaczenie przepisów dotyczących zarządzania ryzykiem związanym z ICT w przypadku banków sprowadza się w zasadzie do uporządkowania dobrze znanych aspektów bezpieczeństwa informacji, ale także do zwrócenia większej uwagi na kwestie związane z komunikacją, zarządzaniem incydentami czy traktowaniem tej kwestii jako strategicznej.

Co istotne, w art. 6 ust. 10 przewidziano, że możliwe jest powierzenie w ramach outsourcingu zadań związanych z weryfikacją funkcjonowania systemu zarządzania ryzykiem ICT, przy czym takie powierzenie nie zwalnia samego banku z odpowiedzialności za te kwestie.

Przepisy DORA od art. 7 do art. 16 stanowią doszczegółowienie oczekiwań prawodawcy w zakresie ram zarządzania ryzykiem ICT. Znajdziemy tam wymogi odnoszące się do:

1. Systemów, protokołów i narzędzi ICT,

2. Sposobu identyfikacji ryzyka związanego z ICT (jest dość standardowe podejście zmierzające do zmapowania funkcji biznesowych, zadań i obowiązków, aktywów i przypisanie im klas, typów i skali ryzyka); w przepisach zwrócono szczególną uwagę na kwestię ryzyk związanych z relacjami z zewnętrznymi dostawcami ICT, co znajduje zresztą odzwierciedlenie w dalszych wymogach DORA,

3. Monitorowania i ochrony zasobów ICT, czyli swoisty SecurityOps – całokształt działań, które bank podejmuje w celu upewnienia się, że ryzyka podlegają stosownemu zaopiekowaniu i bank jest przygotowany na ewentualną ich materializację,

4. Wykrywania, co nakłada na banki stosowanie odpowiednich i adekwatnych mechanizmów wykrywania różnych atypowych działań, które mogą wpływać na to jak działa cały system ICT banku i pozwalających na podjęcie ewentualnych działań zaradczych lub naprawczych,

5. Reagowania i przywracania sprawności, a więc m.in. posiadania i realizowania planów ciągłości działania (BCP) oraz disaster recovery (działań, które podejmujemy po „upadku"),

6. Polityk i procedur tworzenia kopii zapasowych oraz metod i procedur przywracania i odzyskiwania danych, co wiąże się też z pkt 5 powyżej,

7. Uczenia się i rozwoju, któremu warto poświęcić nieco więcej uwagi, bowiem jest to de facto wezwanie do zapewnienia z jednej strony procesu ciągłego uczenia się organizacji (co jest niezwykle istotne w świecie dynamicznie zmieniających się zagrożeń z obszaru ICT), ale także budowania solidnych kompetencji po stronie

6 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1774&qid=1720433556083 (dostęp: 14/01/2026 r.).

i samego banku, jak i podmiotów wykonujących na ich zlecenie określone czynności (zewnętrzni dostawcy usług ICT); to także niezwykle istotne działania z zakresu cyberhigieny; kwestie związane z obowiązkiem poddawania się szkoleniom przez dostawców ICT budziły wiele kontrowersji i często stanowiły argument negocjacyjny w rozmowach na temat ostatecznej wysokości wynagrodzenia,

8. Komunikacji, która odnosi się zarówno do komunikacji wewnętrznej i eskalacji (w tym w zakresie incydentów ICT), jak i komunikacji „na zewnątrz", w tym do klientów; to jeden z tych obszarów, który wiąże się z szerokimi kampaniami uświadamiającymi, ale także komunikatami „post factum", gdy doszło do zdarzenia.

Co istotne, wiele z kwestii, które zostały wskazane powyżej, zostaje doprecyzowanych na poziomie aktów delegowanych, np. odnoszących się do stosowanych metod szyfrowania. Oczywiście nie jest to wystarczające, aby sprostać tym wymaganiom, toteż w procesie implementacji i ciągłego doskonalenia (CI/CD) duże znaczenie mają standardy i wytyczne (np. ENISA) oraz dobre praktyki, które stosowane są powszechnie w obszarze cyberbezpieczeństwa.

3.3.2. Zgłaszanie incydentów ICT

Jednym z istotniejszych zagadnień, któremu poświęcono wiele miejsca w DORA, jest zarządzanie incydentami ICT. Podobnie jak w przypadku ryzyka i tutaj prawodawca wyposażył nas w definicję „incydentu związanego z ICT", jak również „podtypów" tych incydentów, co może mieć znaczenie w kontekście realizacji obowiązków, np. raportowych. Ze względu na ograniczone ramy zwrócimy tutaj uwagę jedynie na sam „incydent związany z ICT", sygnalizując jednocześnie potrzebę całościowego uwzględnienia zagadnienia.

Incydent taki to pojedyncze zdarzenie lub seria powiązanych ze sobą zdarzeń, nieplanowanych przez dany podmiot finansowy, które zagrażają bezpieczeństwu sieci i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub na usługi świadczone przez ten podmiot finansowy. Co ważne, DORA przewiduje też inne istotne definicje, które mogą mieć znaczenie w procesie zarządzania incydentami, jak np. znaczące cyberzagrożenia, które podlegają specjalnemu rejestrowaniu.

Uznanie, że w banku mamy do czynienia z incydentem (co wymaga ustalenia procesu identyfikacji, eskalacji i klasyfikacji) będzie zobowiązywało do dalszej analizy, a przykładowo w przypadku incydentów poważnych[7] do podjęcia dalej idących działań, w tym zaraportowania do KNF. Warto przy tym zauważyć, że kwestie związane z incydentami ICT w rozumieniu DORA mogą niekiedy zazębiać się i przenikać z incydentami, o których mowa w przepisach implementujących dyrektywę NIS (1 i 2), w szczególności wobec prac nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa – tam wprost znajdziemy też wyłączenia niektórych przepisów tej ustawy ze względu na wyższy standard wynikający z DORA czy też próbę uniknięcia dublowania raportowania.

Kwestii zarządzania incydentami poświęcono rozdział III DORA oraz stosowne akty delegowane. Najważniejszym wymogiem, który „schodzi" na niższe poziomy jest obowiązek określenia, ustanowienia i wdrożenia procesu zarządzania incydentami związanymi z ICT. Powinien on uwzględniać różne poziomy i skalę wpływu, a także pomóc podejmować stosowne decyzje w przypadkach ich wystąpienia.

Procesy związane z obsługą incydentów powinny uwzględniać m.in. konieczność wprowadzenia systemów wczesnego ostrzegania, wspomniane już klasyfikowanie incydentów (do tej kwestii jeszcze wrócimy), podział ról i obowiązków (najlepiej w ramach matrycy RASCI, choć nie jest to wprost wymóg zawarty w DORA), odpowiednie działania komunikacyjne oraz informacyjne czy też obowiązki związane z poważnymi incydentami oraz działaniami następczymi po wystąpieniu incydentów.

Wspomniana klasyfikacja ma nie tylko znaczenie operacyjne, ale także regulacyjne. W art. 18 wskazano na konieczność dokonywania przez banki klasyfikacji incydentów oraz cyberzagrożeń ze względu na określone kryteria. W tym zakresie największe znaczenie ma rozporządzenie delegowane Komisji (UE) nr 2024/1772[8], które wskazuje konkretne kryteria klasyfikacji, w tym kwalifikowania incydentów jako poważnych.

7 Kryteria te zostały wskazane w stosownym rozporządzeniu delegowanym Komisji (UE): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1772&qid=1720433556083 (dostęp: 14.01.2026 r.).

8 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1772&qid=1720433556083 (dostęp: 16.01.2026 r.).

Ta ostatnia kwestia jest o tyle istotna, że DORA zobowiązuje banki oraz inne podmioty finansowe do dokonywania zgłoszeń poważnych incydentów oraz ich całościowej obsługi technicznej i regulacyjnej. Tutaj również Unia Europejska zapewnia zestaw wymagań, które znajdziemy w rozporządzeniu delegowanym Komisji (UE) nr 2025/301[9] oraz 2025/302[10], a Urząd Komisji Nadzoru Finansowego przygotował stosowną instrukcję wraz ze wzorami[11], a także podjął liczne inicjatywy edukacyjne dla rynku w ramach spotkań CEDUR. Jest to o tyle istotne, że KNF jest również CSIRT, czyli sektorowym zespołem cyberbezpieczeństwa, który obsługuje m.in. incydenty zgłaszane na podstawie ustawy o krajowym systemie cyberbezpieczeństwa (uKSC), ale także pełni inne wspierające role w obszarze bezpieczeństwa informacji.

Wprowadzenie tych obowiązków na poziomie DORA spowodowało uchylenie niektórych obowiązków (np. w zakresie tzw. incydentów PSD2) w dotychczasowej formie (bazujących na wytycznych) i ujednolicenie ich z obowiązkami stricte ICT.

Należy również mieć w pamięci, że część banków może być obowiązana do raportowania incydentów na gruncie nowelizowanej w chwili pisania raportu uKSC. Nowelizacja przewiduje pewne odstępstwa i ułatwienia, również w tym zakresie.

3.3.3. Testowanie odporności operacyjnej

Każdy system mający być odporny na różnego rodzaju zdarzenia oraz incydenty o charakter ICT powinien być regularnie testowany pod kątem realnej zdolności do m.in. odpierania ataków czy „podnoszenia" się po awarii. Z tego względu również w DORA przewidziano obowiązki z tym związane.

Jednym z najistotniejszych jest ten wskazany w art. 24 ust. 1, który zobowiązuje banki do ustanawiania i utrzymania „prawidłowego i kompleksowego programu testowania operacyjnej odporności cyfrowej". Ma to być jeden z kluczowych elementów zarządzania ryzykiem ICT i musi być regularnie przeglądany i aktualizowany, tym bardziej, że pewne zdarzenia bądź incydenty mogą wręcz zmuszać do przeprowadzenia stosownej rewizji.

Z praktycznego punktu widzenia odpowiedni program czy plan w zakresie testowania będzie składał się ze zróżnicowanej dokumentacji, która określać będzie w jaki sposób takie testy będą przeprowadzane, np. poprzez pentesty czy regularne skanowanie oraz ocenę podatności (bardziej szczegółowo oczekiwania w tym zakresie określa art. 25 DORA). Co istotne, również i w tym zakresie zastosowano zasadę proporcjonalności, która odnosi się także do doboru środków ze względu na skalę działalności, ale również profil ryzyka.

Banki powinny dysponować jasno określonymi kryteriami przeprowadzania testów, ale także wyboru audytorów zewnętrznych i wewnętrznych i „przyjmowania wniosków poaudytowych".

Ważnym i zarazem kosztownym obowiązkiem jest przeprowadzanie tzw. testów TLPT, czyli zgodnie z DORA - testów penetracyjnych pod kątem wyszukiwania zagrożeń (TLPT), oznaczających ramy naśladujące taktykę, techniki i procedury stosowane w rzeczywistości przez agresorów uznanych za stanowiących rzeczywiste cyberzagrożenie, które zapewniają kontrolowane, dostosowane do konkretnych zagrożeń, oparte na analizie zagrożeń (red team) testy działających na bieżąco krytycznych systemów produkcji podmiotu finansowego. W praktyce to zorganizowana akcja z użyciem fałszywych agresorów (red team) oraz odpierających (blue team), czasem rozszerzanych o zespoły wspierające.

W tym przypadku obowiązują także wymagania określone w rozporządzeniu delegowanym Komisji (UE) 2025/1190, które określają nie tylko kryteria doboru podmiotów, które takie testy muszą przeprowadzić, ale także te odnoszące się bezpośrednio do metodyki ich przeprowadzania. Jest to uzupełnienie także art. 27 odnoszące się do wymogów testerów w kontekście testów TLPT. W kontekście tych testów UKNF opracował wyjaśnienie oczekiwań w formie artykułu dostępnego na stronie Urzędu[12].

Takie testy przeprowadzane są nie rzadziej niż co trzy lata, ale wiele z dobrych praktyk czy standardów

9 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:L_202500301 (dostęp: 16.01.2026 r.).

10 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:L_202500302 (dostęp: 16.01.2026 r.).

11 https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Incydenty_DORA (dostęp: 16.01.2026 r.).

12 https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/testy_TLPT_nowe_podejscie?articleId=90547&p_id=18 (dostęp: 16.01.2026r.)

wskazuje na potrzebę częstszego ich przeprowadzania. W sytuacji poważniejszego incydentu, który np. wykazał istotne luki w systemach, takie testy niewątpliwie będą pożądane.

3.3.4 Zarządzanie ryzykiem zewnętrznym (Third-Party Risk)

Jest to jeden z najważniejszych i – niestety – najbardziej obciążających obowiązków po stronie banków i innych podmiotów finansowych. Wyrażony w art. 28 DORA obowiązek zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT wydaje się na pierwszy rzut oka „niewinny", jednak jego praktyczne (i operacyjne) znaczenie dla podmiotów finansowych jest znaczące.

Taki system zarządzania ryzykiem musi być wpisany w ogólne ramy zarządzania ryzykiem ICT i obejmuje m.in. konieczność zawierania umów z zewnętrznymi dostawcami usług ICT w określonej formie (a przynajmniej z zapewnieniem, że określone postanowienia obligatoryjne zostaną tam zawarte), rejestrowania takich umów i rzecz jasna monitorowanie ich spełnienia (np. poprzez SLA). To jednak znacznie więcej, bowiem od banków oczekuje się ustalenia odpowiedniej strategii w odniesieniu do poszczególnych kategorii dostawców (a ściślej usług, które się im powierza).

Te kwestie zostały szczegółowo opisane w art. 30 DORA (najważniejsze postanowienia umowne), gdzie określone zostały oczekiwania co do obligatoryjnych postanowień umownych w podziale na umowy zwykłe oraz te wspierające usługi krytyczne bądź istotne. W praktyce wielu banków spowodowało to opracowanie dwóch wersji załączników, aneksów lub klauzul, które dopasowane były do specyfiki danego przypadku i służyły albo jako materiał do negocjacji z dostawcą, albo też podstawę „taktyki" *take it or leave it*. Nierzadko renegocjacja umów z dostawcami, którzy nie byli świadomi wyzwań, które stawia przed bankami i nimi samymi DORA, spowodowała, że negocjowanie umów stawało się procesem wielomiesięcznym i pochłaniającym liczne zasoby ludzkie po stronie banków.

Wspomniany już rejestr umów nie może być rejestrem prowadzonym w dowolnej formie, ale w tej, którą przewiduje rozporządzenie delegowane Komisji (UE) nr 2024/2956, którego późne przyjęcie (koniec listopada 2024 r.) spowodowało wiele trudności po stronie banków. Co istotne, z rejestrem tym wiążą się określone obowiązki sprawozdawcze, które zostały szczegółowo opisane i zakomunikowane przez KNF (zarówno co do treści, jak i sposobu raportowania)[13].

Choć wiele banków do czasu wprowadzenia przepisów DORA prowadziło już rejestry umów outsourcingowych, to jednak szczegółowość informacji oraz rozszerzenie zakresu spowodowało wzrost obciążeń regularnych i administracyjnych, związanych także z koniecznością wyznaczenia osób odpowiedzialnych za jego prowadzenie i monitorowanie.

W tym miejscu nie sposób nie odnieść się do inicjatywy Związku Banków Polskich, który przygotował rekomendacje w zakresie wzorcowych aneksów zapewniających zgodność z DORA. Dokument ten zawiera dwa wzory: dla dostawców wspierających funkcje krytyczne lub istotne oraz dla pozostałych funkcji - które po odpowiednim dostosowaniu do potrzeb organizacji, a także konkretnego przypadku - można zastosować do zapewnienia zgodności z DORA, przy czym Związek Banków Polskich wyraźnie wyłącza swoją odpowiedzialność wskazując na „rekomendacyjny" charakter dokumentu.

To jednak nie koniec obowiązków, bowiem przykładowo przed podpisaniem stosownej umowy, dostawcy usług ICT powinni zostać poddani stosownemu procesowi due diligence (badania m.in. reputacji czy zdolności podmiotu do wykonania umowy), który ma pomóc ocenić, czy dostawca daje odpowiednią rękojmię i gwarancję wykonania. Kwestie szczegółowe znalazły się m.in. w rozporządzeniu delegowanym Komisji (UE)[14] nr 2025/1773.

Z tym zagadnieniem, przynajmniej pośrednio, wiąże się kolejne oczekiwanie wyrażone w art. 29 DORA, czyli koniecznością dokonania wstępnej oceny koncentracji w obszarze ICT. Jest to obowiązek realizowany w odniesieniu do powierzenia usług wspierających funkcje krytyczne lub istotne i których nie da się przykładowo łatwo zastąpić. W takich sytuacjach banki powinny przykładać szczególną wagę do oceny potencjalnego ryzyka i środków, które mają pomóc nim zarządzić.

W tym miejscu należy wskazać, że praktyki w zakresie realizacji obowiązków różnią się w zależności od banku, skali jego działalności, ekspozycji na ryzyko ICT oraz innych czynników wpływających na „głębokość" stosowa-

13 https://www.knf.gov.pl/?articleId=93323&p_id=18 (dostęp: 16.01.2026 r.).

14 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1773&qid=1720433556083 (dostęp: 16.01.2026 r.) .

nych środków. Nie ma jednak wątpliwości, że największe znaczenie mają dostawcy, którzy świadczą usługi ICT wspierające funkcje krytyczne lub istotne banku. W przypadku tych podmiotów nierzadko utrudnione było (jest?) negocjowanie umów według określonych i zindywidualizowanych szablonów. Takie podmioty nierzadko albo starały się wykazać, że w konkretnych use case przykładowo nie należy interpretować usług w ten sposób, bądź też nawet starały się wykazywać, że w ogóle nie są dostawcami usług ICT.

3.3.5 Nadzór nad dostawcami ICT o znaczeniu krytycznym

DORA wprowadziła także pojęcie kluczowych zewnętrznych dostawców ICT. W rozporządzeniu delegowanym Komisji (UE) nr 2024/1502 określone zostały szczegółowe kryteria, którymi europejskie urzędy nadzoru powinny się kierować przy wyborze takich podmiotów. Wybór taki został ogłoszony 18 listopada 2025 r.[15] a na liście znalazło się 19 podmiotów, których działalność ma charakter międzysektorowy.

W ramach nadzoru DORA nad kluczowymi dostawcami istotne znaczenie mają unijne organy reprezentujące sektor finansowy, ubezpieczeniowy oraz inwestycyjny (stąd też podmioty znajdujące się na liście mają „agnostyczny" sektorowo profil działalności), które przyjmują projekty wspólnych stanowisk oraz aktów, nadzorują kluczowe wskaźniki (wpływające na bezpieczeństwo i stabilność systemu) w obszarze ryzyka ICT czy też de facto weryfikują spełnienie przez te podmioty wymagań w zakresie ram zarządzania ryzykiem ICT. W art. 33 DORA przewidziano szczegółowy katalog zadań tzw. wiodącego organu nadzorczego, który pełni też funkcję punktu kontaktowego oraz zapewnia współpracę z podmiotami o kluczowym znaczeniu oraz innymi organami. Art. 35 wskazuje z kolei jakie kompetencje mają takie wiodące organy i należą do nich m.in. możliwość wydawania zaleceń czy prowadzenie dochodzeń i kontroli.

Co istotne, przepisy DORA przewidują także określone uprawnienia w sytuacji, gdy działania nadzorcze wymagają działania poza Unią Europejską. Na dzień sporządzenia raportu nie dysponowaliśmy wiedzą na temat podejmowanych działań ze względu na krótki okres od opublikowania listy podmiotów kluczowych.

3.4. Harmonogram wdrożenia i akty wykonawcze

Proces stosowania przepisów DORA i dostosowywania się banków oraz innych podmiotów finansowych był dość skomplikowany i obfitujący w niespodziewane zwroty akcji. Wynikało to z faktu, że dla pełnego dostosowania się do przepisów konieczne było przyjęcie i opublikowanie przez Komisję (UE) stosownych aktów delegowanych, które były przyjmowane na bazie tego co dostarczały jej organy unijne odpowiedzialne za nadzór nad poszczególnymi rynkami. Nie zawsze stanowiska organów pokrywały się z podejściem Komisji, co spowodowało m.in. przekroczenie terminów na dostosowanie niektórych aktów delegowanych, w tym dotyczących rejestrów.

Tym samym banki i inne podmioty finansowe stawały przed niełatwym zadaniem dostosowania się, bez pewności czy interpretacja przepisów jest właściwa. Atmosferę w tym zakresie pogarszał fakt, że organy krajowe stawały w większość państw, w tym Polsce, na stanowisku, że do zapewnienia zgodności nie jest niezbędne odnoszenie się do aktów delegowanych, a przepisy DORA są wystarczająco szczegółowe. Szczegółowy harmonogram prac nad rozporządzeniem DORA przedstawiono na schemacie 1.

Stąd też obowiązującą datą na dostosowanie się do przepisów DORA był 17 stycznia 2025 r. Należy jednak podkreślić, że przepisy, które formalnie umożliwiły Komisji Nadzoru Finansowego sprawowanie nadzoru nad rynkiem z perspektywy DORA zostały przyjęte ustawą z dnia 25 czerwca 2025 r. Ustawa nowelizująca utrzymała w mocy także niektóre akty wykonawcze i przedłużyła ich obowiązywanie o dodatkowe 12 miesięcy. Jednocześnie wiele z aktów delegowanych zostało przyjętych przez Komisję znacząco po terminie.

UKNF w niektórych sytuacjach przychylał się do uwag rynku i akceptował wydłużenie terminów na spełnienie niektórych obowiązków, jak miało to przykładowo miejsce w odniesieniu do rejestru umów[16].

Zauważyć należy, że wiele z obowiązków nakładanych na banki w drodze DORA ma charakter ciągły, toteż nie powinno się ich rozpoznawać z perspektywy spełnienia na dzień 17 stycznia 2025 r., ale w ca-

15 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.esma.europa.eu/sites/default/files/2025-11/List_of_designated_CTPPs.pdf (dostęp: 16.01.2026 r.).

16 https://www.knf.gov.pl/?articleId=93323&p_id=18 (dostęp: 12.01.2026 r.).

Schemat 1. Kalendarium prac nad rozporządzeniem DORA

Źródło: K. Proczka, M. Groniewski, Krajobraz cyberbezpieczeństwa rynku finansowego w Polsce a poziom edukacji finansowej – perspektywa organu nadzoru nad rynkiem finansowym oraz jego interesariuszy, Studia Politologiczne, nr 77/2025

łym cyklu życia. Przykładem takiego obowiązku jest konieczność utrzymywania umów z zewnętrznymi dostawcami usług ICT i prowadzenie rejestru umów.

W tym miejscu należy także podkreślić, że wobec stosowania przepisów DORA po stronie banków pojawiła się konieczność realizacji obowiązków raportowych wobec KNF. Są one realizowane na bieżąco – wykaz terminów oraz zakresu obowiązków raportowych przedstawił UKNF na swojej stronie internetowej w formie przystępnej tabeli[17]. UKNF przygotował także listę wszystkich rozporządzeń wykonawczych do DORA, która zostały wydane przez Komisję (UE)[18] – jest to znaczne ułatwienie dla podmiotów o mniejszych zasobach organizacyjnych.

3.5 Powiązania z innymi regulacjami i wytycznymi

Do czasu, gdy DORA zaczęła obowiązywać, wiele z aspektów związanych z zarządzaniem ryzykiem ICT była przedmiotem wytycznych i rekomendacji, zarówno EBA / ESMA, jak i KNF. Przepisy DORA same w sobie nie są zbyt szczegółowe i stanowią raczej pewien fundament, który wymaga „operacjonalizacji" na poziomie rozwiązań architektonicznych, organizacyjnych, technicznych czy też procesów, które w danej instytucji będą obowiązywać. Sama DORA oraz towarzysząca jej dyrektywa 2022/2556[19] należą do tzw. poziomu 1 unijnej legislacji i regulacji.

Sytuacja wygląda nieco inaczej w przypadku aktów wykonawczych, które bardziej szczegółowo regulują niektóre kwestie, jak omawiane już obowiązki w zakresie zarządzania incydentami ICT. Mają one charakter uzupełniający względem rozporządzenia i należą do tzw. poziomu 2[20] i akty te nie mają charakteru ustawodawczego – nie mogą zmieniać istotnych elementów samego rozporządzenia. Mają jednak istotne znaczenie z perspektywy adresatów DORA, bowiem dookreślają oczekiwania także organów regulacyjnych w tym zakresie i stanowią podstawę do ewentualnego pociągnięcia do odpowiedzialności za ewentualne niedostosowanie

17 https://www.knf.gov.pl/dla_rynku/dora/sprawozdawczosc/obowiazki_sprawozdawcze_w_zwiazku_z_rozporzadzeniem_dora?articleId=91834&p_id=18 (dostęp: 12.01.2026 r.).

18 https://www.knf.gov.pl/dla_rynku/dora (dostęp: 12.01.2026 r.).

19 https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022L2556 (dostęp: 18.01.2026 r.).

20 https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en (dostęp: 18.01.2026 r.).

Nie wszystkie obszary zawarte w DORA uzyskały status aktów delegowanych. W związku z tym DORA towarzyszą także wytyczne[21] i rekomendacje, a nawet tzw. QnA[22], czyli zestawy pytań i odpowiedzi do rozporządzenia. Jest to tzw. poziom 3 i choć dokumenty te nie mają takiej samej mocy jak te z poziomu 1 i 2, to jednak ich znaczenie jest duże ze względu na autorytet i pozycję wydających je organów.

3.5.1 Relacja do przepisów dyrektywy NIS2[23]

Dyrektywa nr 2022/2555[24] (NIS2) reguluje wiele z aspektów związanych z zarządzaniem bezpieczeństwem informacji i oczekuje na implementację do porządku krajowego w formie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa („uKSC"). Na dzień sporządzania raportu projekt znajdował się w sejmowym procesie prawodawczym.

Relacja DORA do NIS2 może być rozpatrywana z dwóch perspektyw. Samo rozporządzenie wyraźnie wskazuje w preambule, że „(...) rozporządzenie stanowi lex specialis względem dyrektywy (UE) 2022/2555". Wynika to z faktu, że rozporządzenie w wielu miejscach stawia bardziej restrykcyjne wymogi niż dyrektywa i tym samym przepisy DORA powinny mieć pierwszeństwo w przypadku ewentualnej kolizji z NIS2. Przepisy implementujące dyrektywę odnoszą się przy tym do pewnej określonej grupy podmiotów, w tym banków oraz instytucji kredytowych.

Z tego względu należy dopuszczać możliwość występowania takiej kolizji. W projekcie nowelizacji uKSC przewidziano w art. 8i[25], który wprowadza wyłączenie od stosowania niektórych przepisów uKSC dla podmiotów kluczowych i podmiotów ważnych z sektora bankowości, które odnoszą się m.in. do kwestii systemu zarządzania bezpieczeństwem informacji czy też zgłaszania poważnych incydentów. Jednocześnie przewidziano, że niektóre przepisy ustawy należy stosować odpowiednio.

Można jednocześnie przyjąć, że dostosowanie do DORA zapewnia znaczny poziom zgodności z NIS2, gdyż samo rozporządzenie w sposób znacznie bardziej szczegółowy reguluje tę samą materię.

3.5.2. Relacja do wytycznych EBA i ESAs

Jak wspomnieliśmy w raporcie nie wszystkie kwestie związane z prawidłową implementacją DORA zostały zawarte na poziomie rozporządzenia oraz aktów z poziomu 2. Jednocześnie w momencie uchwalenia DORA funkcjonowały wytyczne i rekomendacje (oraz opinie) unijnych organów regulacyjnych (m.in. EBA czy ESMA) oraz towarzyszące im dokumenty wydawane przez organy krajowe, w tym KNF.

Pozostała więc do rozwiązania kwestia jak należy traktować te dokumenty lub w jaki sposób usunąć ewentualne wątpliwości. Wśród działań „porządkujących" możemy wskazać wprowadzenie istotnych zmian i ograniczenie zakresu m.in. wytycznych EBA/2019/04[26] w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT czy też prace nad projektem wytycznych w sprawie zarządzania ryzykiem stron trzecich w odniesieniu do usług nie będących usługami ICT[27] (jakkolwiek jest obszar poza DORA", to jednak jego podjęcie wynika właśnie z przyjęcia tych przepisów).

21 https://www.eiopa.europa.eu/document/download/f92c9ae0-889f-45ed-89bc-7123012e0417_en?filename=JC%202024-34_Guidelines%20on%20costs%20and%20losses_DORA.pdf (dostęp: 18.01.2026 r.).

22 https://www.eiopa.europa.eu/about/governance-structure/joint-committee/joint-qas_en (dostęp: 18.01.2026 r.).

23 https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=pl (dostęp: 18.01.2026 r.).

24 https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=pl (dostęp: 18.01.2026 r.).

25 Art. 8i [wersja dostępna na dzień 18.01.2026 r.]. 1. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych nie stosuje się przepisów ustawy dotyczących systemu zarządzania bezpieczeństwem informacji lub zgłaszania poważnych incydentów, z wyjątkiem art. 3a, art. 5 ust. 1–3, art. 7–7m, art. 8 ust. 1 pkt 1 i pkt 2 lit. j, art. 8h, art. 9, art. 11 ust. 1 pkt 5 i 6, art. 13, art. 16, art. 26a ust. 2–4, art. 32, art. 33 ust. 5, 7 i 8, art. 36a, art. 36b, art. 37, art. 43, art. 45 ust. 3, art. 46 ust. 1 pkt 1, 2, 4–7 i ust. 4–6, art. 67a, art. 67c, art. 67d oraz art. 67g–67i.
2. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych stosuje się odpowiednio przepisy art. 8c–8f, art. 12 ust. 7 oraz art. 31 ust. 1.
3. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych stosuje się przepisy rozdziałów 11 i 14 ustawy w zakresie art. 3a, art. 5 ust. 1–3, art. 7–7m, art. 8 ust. 1 pkt 1 i pkt 2 lit. j, art. 8h, art. 9, art. 11 ust. 1 pkt 5 i 6, art. 13, art. 15, art. 16, art. 26a ust. 2–4, art. 32, art. 33 ust. 5, 7 i 8, art. 36a, art. 36b, art. 37, art. 43, art. 45 ust. 3, art. 46 ust. 1 pkt 1, 2, 4–7 i ust. 4–6, art. 67a, art. 67c, art. 67d, art. 67g–67i oraz stosowanych odpowiednio przepisów art. 8c–8f, art. 12 ust. 7 oraz art. 31 ust. 1.

26 https://www.eba.europa.eu/publications-and-media/press-releases/eba-amends-its-guidelines-ict-and-security-risk-management-measures-context-dora-application (dostęp: 18.01.2026 r.).

27 https://www.eba.europa.eu/publications-and-media/press-releases/eba-launches-consultation-its-draft-guidelines-third-party-risk-management-regard-non-ict-related (dostęp: 18.01.2026 r.).

EBA uchyliła także wytyczne odnoszące się raportowania poważnych incydentów „pod" PSD2[28] a jej śladem poszła również KNF, która doprecyzowała te kwestie w stosownym komunikacie[29].

KNF również podjęła stosowne działania związane ze stosowaniem DORA, w tym poprzez uchylenie stosownych rekomendacji i stanowisk związanych z obszarem ICT[30], które pokryte zostały przez pakiet DORA. Wśród istotnych dokumentów znalazła się m.in. Rekomendacja D (i D-SKOK) dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach czy też tzw. komunikat chmurowy[31].

W konsekwencji w zasadzie całość kwestii związanych z zarządzaniem ryzykiem ICT w bankach została przeniesiona na poziom 1 i 2 z mniejszym znaczeniem poziomu 3 (z zastrzeżeniem rosnącego znaczenia tzw. QnA).

Jedynie na marginesie należy wskazać, że dokonując implementacji DORA pod uwagę bierze się często także normy standaryzacyjne, jak ISO 27001 czy 22301, które odnoszą się do takich kwestii jak system zarządzania bezpieczeństwem informacji i ciągłość działania, jak również dobre praktyki i standardy w zakresie cyberbezpieczeństwa, m.in. MITRE czy OWASP.

3.5.3. Spójność z innymi aktami sektorowymi (CRD, MiFID, PSD2)

Wejście w życie DORA oraz towarzyszącej dyrektywy spowodowało pewne „zamieszanie" związane ze spójnością rozporządzenia z innymi aktami prawnymi o charakterze sektorowym. Wspomniana już dyrektywa 2022/2556 wprowadziła kilka usprawnień w tym zakresie poprzez narzucenie obowiązku dostosowania się do DORA przez adresatów m.in. MiFID, PSD2 oraz CRD.

Ponieważ jednak są to przepisy dyrektywy, to wymagają one implementacji na poziomie prawa krajowego. Tak też się stało i ustawa wdrażająca DORA[32] jest tego przykładem.

Jest rzecz jasna tak, że przepisy DORA są przepisami obowiązującymi wprost i niewymagającymi implementacji jako takiej. Oznacza to, że zarówno podmioty objęte reżimem dla instytucji kredytowych, obszaru inwestycyjnego czy płatniczego są zobowiązane do stosowania rozporządzenia z uwzględnieniem zasady proporcjonalności. Wynika to także z faktu, że DORA jest lex specialis względem przepisów dyrektywy.

Ewentualne rozbieżności pomiędzy prawem krajowym a DORA powinny być rozstrzygane na korzyść unijnych przepisów.

28 https://www.eba.europa.eu/publications-and-media/press-releases/eba-repeals-guidelines-major-incident-reporting-under-revised-payment-services-directive (dostęp: 18.01.2026 r.).

29 https://www.knf.gov.pl/dla_rynku/Informacje_dla_podmiotow_nadzorowanych/Sektor_bankowy/raportowanie_incydentow_PSD2 (dostęp: 18.01.2026 r.).

30 https://www.knf.gov.pl/?articleId=92241&p_id=18 (dostęp: 18.01.2026 r.).

31 Historycznie: https://www.knf.gov.pl/?articleId=91751&p_id=18 (dostęp: 18.01.2026 r.).

32 https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20250001069/T/D20251069L.pdf (dostęp: 18.01.2026 r.).

4. Ocena poziomu przygotowania banków komercyjnych w procesie wdrożenia DORA na podstawie badania empirycznego

4.1 Metodyka badania

Badanie zostało przeprowadzone wśród 6 banków komercyjnych działających na rynku polskim. Udział w badaniu miał charakter dobrowolny. Pozostałe banki, do których skierowano zaproszenie, nie wzięły udziału z uwagi na odmowę uczestnictwa lub brak możliwości zaangażowania w wyznaczonym terminie.

Badanie zrealizowano w okresie grudzień 2025 – styczeń 2026, tj. w bezpośrednim otoczeniu wejścia w życie regulacji DORA oraz w fazie intensywnych działań wdrożeniowych po stronie instytucji finansowych. Termin realizacji pozwolił na zebranie opinii respondentów opartych zarówno na doświadczeniach przygotowawczych, jak i pierwszych praktycznych doświadczeniach związanych z funkcjonowaniem regulacji.

Podstawowym narzędziem badawczym była ankieta przygotowana do samodzielnego wypełnienia, obejmująca pytania zamknięte (w tym pytania jednokrotnego i wielokrotnego wyboru oraz skalę ocen) oraz pytania otwarte, umożliwiające jakościowe uzupełnienie odpowiedzi. Konstrukcja ankiety pozwalała na ocenę zarówno poziomu formalnej zgodności regulacyjnej, jak i faktycznej dojrzałości organizacyjnej w obszarze odporności cyfrowej.

Zakres tematyczny ankiety obejmował w szczególności:

- ogólny poziom przygotowania banku do wdrożenia regulacji DORA,
- identyfikację przyczyn ewentualnych opóźnień we wdrażaniu wymogów regulacyjnych,
- ocenę adekwatności zasobów ludzkich i budżetowych przeznaczonych na wdrożenie DORA,
- poziom dostosowania do DORA w kluczowych obszarach tematycznych, w tym:
  - zarządzania ryzykiem ICT,
  - zgłaszania i zarządzania incydentami ICT,
  - testowania odporności cyfrowej (w tym TLPT),
  - zarządzania ryzykiem stron trzecich (ICT Third-Party Risk),
  - wymiany informacji i współpracy sektorowej,
- zakres i charakter zmian w istniejących systemach zarządzania ryzykiem ICT,
- identyfikację głównych wyzwań wdrożeniowych (interpretacyjnych, organizacyjnych, technologicznych i relacyjnych),
- ocenę współpracy z organami nadzorczymi (KNF, EBA) oraz oczekiwań wobec nadzoru,
- ocenę poziomu przygotowania kompetencyjnego organizacji w zakresie DORA,
- identyfikację dobrych praktyk, narzędzi oraz rozwiązań wspierających skuteczne wdrażanie regulacji,
- wskazanie obszarów wymagających dalszych analiz, doprecyzowania lub standaryzacji,
- ocenę ogólnej dojrzałości organizacyjnej w kontekście odporności cyfrowej.

Respondentami były osoby pełniące kluczowe role w strukturach zarządzania i nadzoru banków, odpowiedzialne za obszary bezpieczeństwa informacji, ICT i cyberbezpieczeństwa, zarządzania ryzykiem, compliance oraz funkcji prawnych (legal). Osoby te reprezentowały kadrę menadżerską, posiadającą bezpośrednią wiedzę operacyjną oraz decyzyjną w zakresie wdrażania regulacji DORA, co zapewniało wysoki poziom merytoryczny i wiarygodność uzyskanych odpowiedzi.

Z uwagi na ograniczoną liczebność próby oraz dobrowolny charakter udziału w badaniu, uzyskane wyniki mają charakter jakościowo-diagnostyczny i nie stanowią podstawy do uogólnień statystycznych na cały sektor bankowy. Badanie pozwala jednak na identyfikację dominujących trendów, wspólnych wyzwań oraz dobrych praktyk wdrożeniowych, które mogą stanowić wartościowy punkt odniesienia dla dalszych analiz regulacyjnych i branżowych.

Celem badania nie było przeprowadzenie audytu zgodności regulacyjnej ani pełnej, ilościowej diagnozy poziomu odporności operacyjnej sektora bankowego, lecz identyfikacja doświadczeń wdrożeniowych, postrzeganych wyzwań oraz stosowanych praktyk organizacyjnych w wybranych instytucjach o istotnym znaczeniu rynkowym. Uzyskane

wyniki należy interpretować jako odzwierciedlenie percepcji i doświadczeń badanych instytucji, stanowiących istotne uzupełnienie analizy regulacyjnej i sektorowej.

4.2 Uogólnienia wprowadzające, kluczowe wnioski, rekomendacje i oczekiwania banków wobec wdrożenia DORA

Wyniki badania wskazują, że banki objęte badaniem wchodził w regulacje DORA z relatywnie wysokim poziomem przygotowania organizacyjnego, procesowego i zarządczego. Pomimo opóźnień w publikacji aktów delegowanych oraz utrzymującej się niepewności interpretacyjnej, banki objęte badaniem traktowały DORA jako istotny priorytet regulacyjny i podejmowały działania dostosowawcze z odpowiednim wyprzedzeniem. Wysoka samoocena gotowości – bez wystąpienia ocen niskich lub wskazujących na brak przygotowań – świadczy o dojrzałości w obszarze zarządzania ryzykiem ICT oraz odpornością operacyjną jeszcze przed formalnym wejściem regulacji w życie.

Analiza uzyskanych opinii wskazuje, że badane banki dysponowały już ramami zarządzania ryzykiem ICT, procedurami reagowania na incydenty oraz mechanizmami raportowania, które mogły zostać zaadaptowane do wymogów DORA. Regulacja nie była więc postrzegana jako punkt zerowy ani rewolucja technologiczna, lecz jako proces harmonizacji, standaryzacji i uszczegółowienia istniejących praktyk w jednolite, audytowalne ramy regulacyjne.

Równocześnie badanie ujawnia, że pełna operacjonalizacja DORA była i pozostaje procesem rozłożonym w czasie. Największe wyzwania wdrożeniowe miały charakter interpretacyjny, koordynacyjny i relacyjny, a nie techniczny. Niejasności regulacyjne, opóźnienia w publikacji wytycznych wykonawczych, zmienność standardów sprawozdawczych oraz ograniczona przewidywalność komunikacji z nadzorem istotnie wpływały na tempo i sposób realizacji projektów wdrożeniowych. W konsekwencji badane banki były zmuszone prowadzić działania adaptacyjne w trybie równoległym: projektować rozwiązania, jednocześnie oczekując na doprecyzowanie oczekiwań nadzorczych.

Badanie pokazuje również, że poziom dojrzałości wdrożeniowej nie jest jednorodny we wszystkich obszarach DORA. Najwyższy poziom gotowości osiągnięto w obszarach o ugruntowanych ramach regulacyjnych i operacyjnych, takich jak zarządzanie ryzykiem ICT czy zgłaszanie i obsługa incydentów. Z kolei obszary wymagające silnej integracji end-to-end – w szczególności testowanie odporności cyfrowej z udziałem dostawców oraz zarządzanie ryzykiem stron trzecich – pozostają kluczowym polem.

W ujęciu całościowym DORA jawi się jako regulacja systemowa, która testuje nie tyle poziom zaawansowania technologicznego banków, ile ich zdolność do integracji zarządzania ryzykiem ICT z ładem korporacyjnym, relacjami z dostawcami, kompetencjami organizacyjnymi oraz współpracą sektorową. Osiągnięcie trwałej odporności cyfrowej wymaga więc nie jednorazowego wdrożenia, lecz długofalowego procesu adaptacyjnego, w którym kluczowe znaczenie mają stabilność zasobów, klarowność interpretacyjna oraz jakość współpracy w całym systemie finansowo-technologicznym.

Kluczowe wnioski z badania

1. Badane banki weszły w reżim DORA z wysokim poziomem przygotowania organizacyjnego i strukturalnego.
2. 100% badanych banków oceniło poziom gotowości jako wysoki lub bardzo wysoki, mimo opóźnień aktów delegowanych.
3. DORA była postrzegana jako regulacja adaptacyjna i harmonizująca, a nie rewolucyjna.
4. Ewentualne opóźnienia wdrożeniowe miały głównie charakter zewnętrzny, a nie organizacyjny.
5. Największym wyzwaniem okazały się niejasności interpretacyjne i zmienność standardów wykonawczych.
6. Obszary procesowe (incydenty ICT, podstawowe zarządzanie ryzykiem) są najbardziej dojrzałe.
7. Testowanie odporności cyfrowej oraz integracja dostawców ICT pozostają obszarami dalszego dojrzewania.
8. Wysoka formalna zgodność nie zawsze przekłada się jeszcze na pełną dojrzałość operacyjną.

9. Kompetencje w zakresie DORA są skoncentrowane głównie w wyspecjalizowanych jednostkach, a nie w całej organizacji.

10. Zasoby ludzkie i budżetowe stanowią istotny czynnik różnicujący tempo i jakość wdrożenia.

11. Współpraca z nadzorem funkcjonowała, lecz była postrzegana jako niewystarczająco wspierająca operacyjnie.

12. Kluczowym czynnikiem sukcesu jest integracja DORA z istniejącym modelem zarządzania ryzykiem operacyjnym.

Rekomendacje wynikające z badania

1. Traktować DORA jako trwały program organizacyjny, a nie jednorazowy projekt wdrożeniowy.

2. Wzmacniać centralizację zarządzania ryzykiem ICT i ryzykiem dostawców w jednym modelu odpowiedzialności.

3. Rozszerzać kompetencje DORA poza zespoły specjalistyczne na jednostki biznesowe i menedżerskie.

4. Koncentrować dalsze działania na testowaniu odporności end-to-end, w tym z udziałem kluczowych dostawców.

5. Zapewnić stabilne, długofalowe zasoby kadrowe i budżetowe dla utrzymania zgodności i dojrzałości operacyjnej.

6. Budować wspólne standardy umowne i operacyjne z dostawcami ICT.

7. Traktować odporność cyfrową jako odpowiedzialność systemową, a nie wyłącznie instytucjonalną.

8. Zapewnić wcześniejsze, stabilne i jednoznaczne wytyczne interpretacyjne.

9. Ograniczyć dynamiczne zmiany standardów sprawozdawczych w trakcie cyklu wdrożeniowego.

10. Wzmocnić dialog operacyjny z sektorem, w tym poprzez przewidywalne mechanizmy odpowiedzi.

11. Wspierać standaryzację testów odporności oraz podejścia do outsourcingu ICT na poziomie sektorowym.

Potrzeby i oczekiwania banków wobec regulatora oraz dostawców ICT

Odpowiedzi respondentów wskazują, że najważniejszą potrzebą banków w procesie wdrażania DORA jest zwiększenie klarowności interpretacyjnej regulacji. Wszystkie badane banki (100% wskazań) oczekują od regulatora jasnych, spójnych i jednoznacznych wytycznych interpretacyjnych, które ograniczyłyby ryzyko rozbieżnych interpretacji i konieczność podejmowania decyzji wdrożeniowych w warunkach niepewności. Potrzeba ta dotyczy zarówno ogólnej wykładni przepisów DORA, jak i ich praktycznego zastosowania w konkretnych obszarach operacyjnych.

Drugim kluczowym oczekiwaniem jest usprawnienie komunikacji z nadzorem (83% wskazań). Respondenci sygnalizują potrzebę bardziej bezpośredniego, szybszego i operacyjnie użytecznego dialogu z regulatorem, w tym możliwości uzyskiwania jednoznacznych odpowiedzi na pytania interpretacyjne w trakcie trwających projektów wdrożeniowych, a nie dopiero po ich zakończeniu.

Istotnym obszarem potrzeb są również działania edukacyjne i standaryzacyjne. Znaczna część banków wskazuje na potrzebę organizacji szkoleń i warsztatów sektorowych oraz opracowania wspólnych standardów, w szczególności w zakresie testowania odporności cyfrowej (w tym TLPT). Oczekiwania te pokazują, że banki poszukują nie tylko interpretacji przepisów, ale również praktycznych wzorców ich stosowania, które pozwoliłyby na ujednolicenie podejścia w całym sektorze.

Połowa respondentów wskazała także na potrzebę większej elastyczności w harmonogramach wdrożeniowych, zwłaszcza w sytuacjach, gdy publikacja aktów delegowanych i wytycznych następuje z opóźnieniem. Oczekiwanie to wynika z presji czasowej oraz konieczności dostosowywania projektów regulacyjnych do zmieniającego się otoczenia interpretacyjnego.

W odniesieniu do współpracy z dostawcami ICT respondenci wskazują, że największą potrzebą jest większa elastyczność negocjacyjna po stronie dostawców (83% wskazań). Proces dostosowania

umów do wymogów DORA, zwłaszcza w relacjach z dużymi i międzynarodowymi dostawcami usług ICT, jest postrzegany jako jedno z najbardziej czasochłonnych i ryzykownych ogniw wdrożenia regulacji.

Badane banki oczekują również ujednoliconych standardów umownych oraz spójnych standardów polityk i procedur ICT (po 50% wskazań). Potrzeba ta dotyczy w szczególności obszarów bezpieczeństwa, raportowania, testowania odporności operacyjnej oraz zarządzania ryzykiem ICT i ryzykiem stron trzecich. Standaryzacja po stronie dostawców mogłaby znacząco ograniczyć koszty wdrożenia, skrócić procesy negocjacyjne i zmniejszyć ryzyko niezgodności. Znacznie mniejsze znaczenie przypisywane jest kwestiom podziału kosztów edukacji, co sugeruje, że dla banków kluczowe są przede wszystkim aspekty formalne, kontraktowe i organizacyjne, a nie dostęp do wiedzy czy szkoleń oferowanych przez dostawców.

Odpowiedzi jakościowe wskazują na wyraźną potrzebę dalszego doprecyzowania definicji i klasyfikacji usług ICT, w szczególności w zakresie kwalifikacji usług do kategorii S01–S19, jednoznacznego rozumienia pojęcia usługi ICT oraz podejścia do specyficznych modeli współpracy, takich jak body leasing czy jednoosobowe działalności gospodarcze.

Respondenci podkreślają również potrzebę standaryzacji i doprecyzowania zasad testowania odporności operacyjnej, w tym testowania kluczowych dostawców ICT oraz stosowania zasady proporcjonalności wymagań do skali i profilu działalności instytucji. Wskazywana jest także konieczność zapewnienia realnej zgodności dużych, międzynarodowych dostawców usług ICT z wymogami DORA.

Kolejnym istotnym obszarem potrzeb jest analiza łańcucha poddostawców, w tym kwestie związane z chmurą obliczeniową, monitorowaniem ryzyka ICT oraz zarządzaniem kluczowymi dostawcami. Respondenci zwracają uwagę na potrzebę stabilnych, niezmienianych w trakcie procesu wdrożeniowego standardów sprawozdawczych, jasnych definicji pojęć oraz poprawy funkcjonowania systemów raportowania (w szczególności SDD).

Istotnym postulatem pozostaje również poprawa komunikacji z KNF, w tym wprowadzenie bardziej przewidywalnych zasad udzielania odpowiedzi na pytania sektora (np. SLA po stronie nadzoru), co pozwoliłoby ograniczyć niepewność regulacyjną i ryzyko rozbieżnych wdrożeń.

4.3 Ocena przygotowań banków do wdrożenia DORA

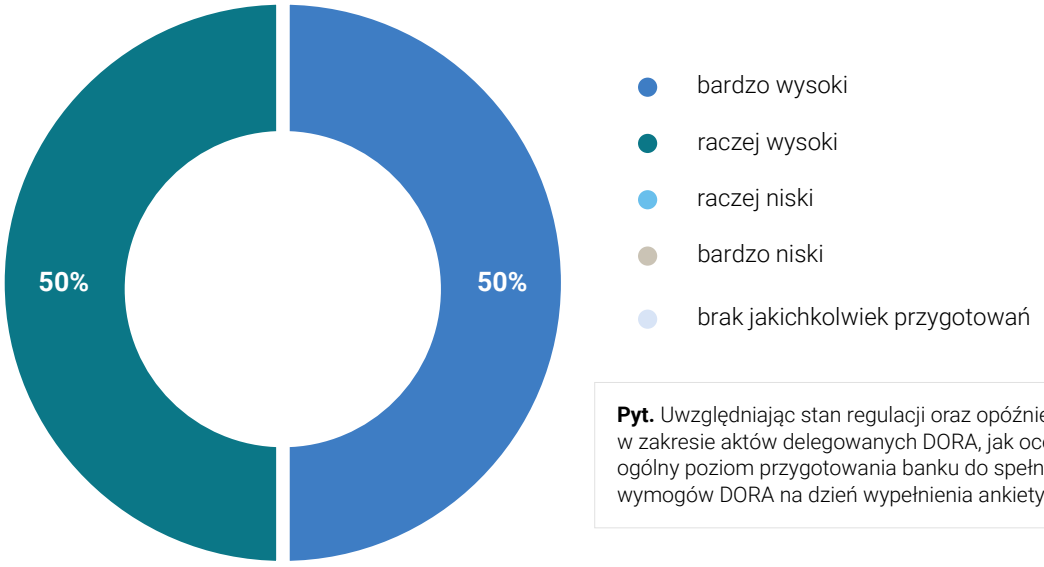
Banki objęte badaniem weszły w reżim regulacyjny DORA z relatywnie wysokim poziomem przygotowania, zarówno na poziomie strategicznym, jak i organizacyjnym. Pomimo opóźnień w publikacji aktów delegowanych oraz utrzymującej się niepewności interpretacyjnej, wszystkie badane instytucje oceniły swój poziom gotowości jako wysoki lub bardzo wysoki, co potwierdza, że DORA była traktowana jako istotny priorytet regulacyjny i przedmiot działań adaptacyjnych podejmowanych z odpowiednim wyprzedzeniem.

Jednocześnie uzyskane wyniki pokazują, że przygotowanie to miało w dużej mierze charakter strukturalny i proceduralny, natomiast pełna operacjonalizacja wymogów regulacyjnych była procesem rozłożonym w czasie i silnie uzależnionym od dynamiki działań nadzorczych, dostępności aktów wykonawczych oraz adekwatności zasobów ludzkich i budżetowych. W konsekwencji wdrożenie DORA należy postrzegać nie jako jednorazowy projekt, lecz jako długofalowy proces adaptacyjny, wymagający ciągłego dostosowywania organizacji do zmieniających się oczekiwań regulacyjnych i nadzorczych.

Kluczowe wnioski w obszarze - poziom przygotowania do wdrożenia DORA:

- Banki objęte badaniem charakteryzowały się wysokim poziomem przygotowania do wdrożenia regulacji DORA, pomimo opóźnień w publikacji aktów delegowanych i wytycznych wykonawczych.
- 100% badanych banków oceniło poziom przygotowania jako wysoki lub bardzo wysoki, co potwierdza, że DORA była traktowana przez banki jako priorytet regulacyjny i została uwzględniona w planach strategicznych z odpowiednim wyprzedzeniem.
- Brak ocen niskich lub wskazujących na brak przygotowań sugeruje, że banki nie odkładały działań dostosowawczych do momentu pełnej klarowności regulacyjnej.
- Ewentualne opóźnienia we wdrażaniu DORA miały przede wszystkim charakter zewnętrzny i regulacyjny, a nie organizacyjny – kluczowym czynnikiem były opóźnienia w wydawaniu aktów delegowanych oraz niejednoznaczna komunikacja ze strony regulatora.

Wykres 4.1. Ogólna ocena poziomu przygotowania banku do spełnienia wymogów DORA.



Pyt. Uwzględniając stan regulacji oraz opóźnienia w zakresie aktów delegowanych DORA, jak ocenia Pan(i) ogólny poziom przygotowania banku do spełnienia wymogów DORA na dzień wypełnienia ankiety?

Źródło: wyniki badań własnych.

- Relatywnie niski odsetek wskazań na przyczyny wewnętrzne (braki zasobowe, późne rozpoznanie skali zmian) potwierdza, że banki były świadome zakresu i znaczenia regulacji, a problemy wdrożeniowe wynikały głównie z ograniczonej przewidywalności otoczenia regulacyjnego.

- Dostępność zasobów ludzkich i budżetowych stanowiła istotny czynnik różnicujący tempo i sprawność wdrożenia, przy czym tylko część banków była w stanie zapewnić je w pełni już na moment wejścia w życie regulacji.

- DORA okazała się regulacją o wysokim stopniu złożoności i dynamiki, wymagającą elastycznego podejścia do zarządzania zmianą.

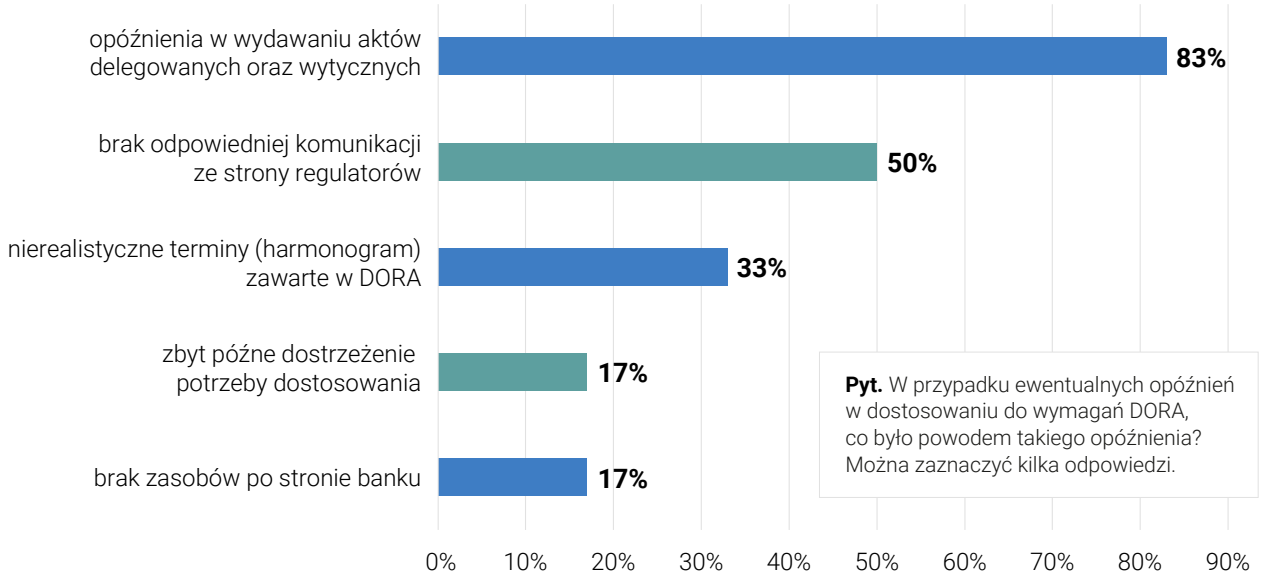
- W ujęciu całościowym DORA nie była postrzegana jako regulacja wymagająca budowy systemów od podstaw, lecz jako proces adaptacyjny, harmonizujący i porządkujący istniejące ramy zarządzania ryzykiem ICT i odpornością operacyjną.

Uzyskane wyniki (wykres 4.1) wskazują na relatywnie wysoką ocenę poziomu przygotowania banków do spełnienia wymogów DORA. Połowa banków (50%) oceniła poziom przygotowania jako bardzo wysoki, natomiast pozostałe 50% jako raczej wysoki. W badanej grupie nie odnotowano ocen wskazujących na niski poziom przygotowania ani odpowiedzi sugerujących brak przygotowań. Oznacza to, że mimo występujących opóźnień w zakresie aktów delegowanych, badani postrzegają swoje banki jako dobrze przygotowane do wdrożenia regulacji DORA na dzień realizacji badania.

Uzyskane wyniki jednoznacznie wskazują na wysoki poziom przygotowania badanych banków do spełnienia wymogów regulacji DORA na moment realizacji badania. Banki – pomimo niepewności regulacyjnej oraz opóźnień w publikacji aktów delegowanych – podjęły działania adaptacyjne z odpowiednim wyprzedzeniem. Sugeruje to, że sektor bankowy traktował DORA jako istotny priorytet regulacyjny, a ryzyko niezgodności było aktywnie zarządzane już na etapie projektowym. Wysoka samoocena przygotowania może również odzwierciedlać doświadczenie banków w implementacji wcześniejszych regulacji ICT oraz dojrzałość istniejących ram zarządzania ryzykiem operacyjnym i cybernetycznym.

Jednocześnie należy zauważyć, że wysoki poziom deklarowanego przygotowania nie oznacza braku wyzwań wdrożeniowych, co potwierdzają odpowiedzi udzielone w kolejnych pytaniach badania. W szczególności dotyczy to obszarów interpretacyjnych, zasobowych oraz współpracy z nadzorem. Oznacza to, że przygotowanie banków miało w dużej mierze charakter organizacyjny i proceduralny,

Wykres 4.2. Powody opóźnień w dostosowaniu do wymagań DORA.



Źródło: wyniki badań własnych.

natomiast pełna operacjonalizacja wymogów DORA była – i w części przypadków nadal jest – procesem rozłożonym w czasie.

Najczęściej identyfikowanym źródłem opóźnień we wdrażaniu wymogów DORA były czynniki regulacyjne, a nie ograniczenia po stronie samych banków (wykres 4.2). Aż 83% respondentów wskazało na opóźnienia w wydawaniu aktów delegowanych oraz wytycznych, co potwierdza istotny wpływ niepewności regulacyjnej na tempo prac dostosowawczych.

Połowa badanych (50%) zwróciła uwagę na niewystarczającą komunikację ze strony regulatorów, co dodatkowo utrudniało planowanie i priorytetyzację działań wdrożeniowych. 33% respondentów wskazało na nierealistyczne harmonogramy zawarte w regulacji DORA, które w praktyce okazały się trudne do realizacji.

Czynniki wewnętrzne po stronie banków były wskazywane znacznie rzadziej. Jedynie 17% respondentów zadeklarowało, że opóźnienia wynikały ze zbyt późnego rozpoznania skali dostosowania, a taki sam odsetek wskazał na braki zasobowe po stronie banku.

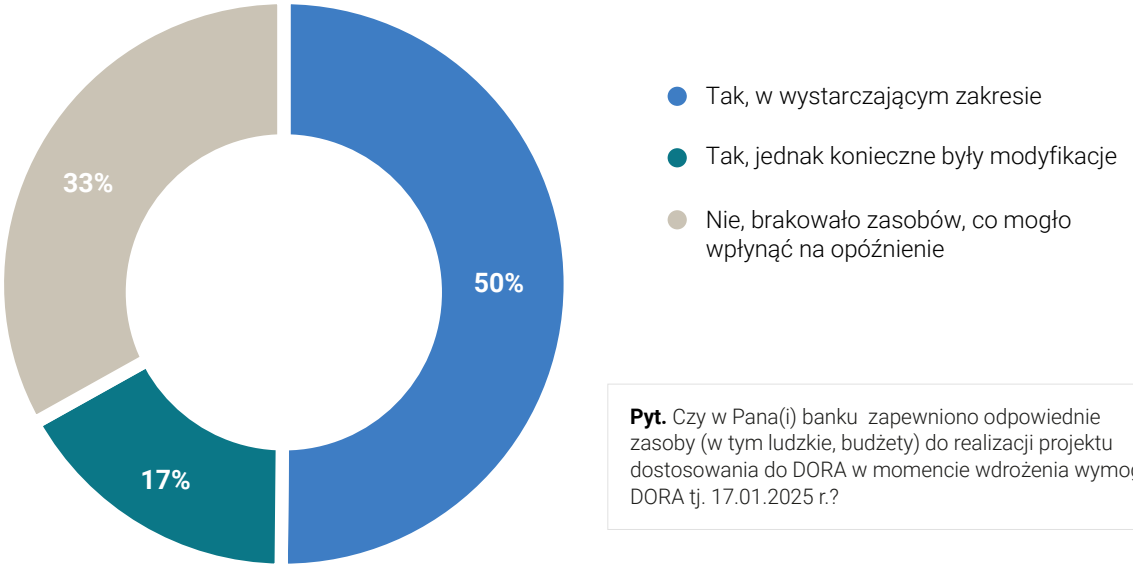
Uzyskane wyniki sugerują, że ewentualne opóźnienia w dostosowaniu do DORA miały charakter systemowy i zewnętrzny, a nie organizacyjny, co potwierdza relatywnie wysoki poziom gotowości banków przy jednoczesnym silnym uzależnieniu procesu wdrożenia od dynamiki działań regulacyjnych.

Wyniki badania wskazują, że ewentualne opóźnienia w dostosowaniu banków do wymogów DORA miały w przeważającej mierze charakter zewnętrzny i regulacyjny, a nie organizacyjny. Dominującym czynnikiem opóźnień były opóźnienia w publikacji aktów delegowanych oraz wytycznych wykonawczych, które znacząco ograniczały możliwość precyzyjnego zaplanowania działań wdrożeniowych oraz alokacji zasobów. Wysoki odsetek wskazań tego czynnika potwierdza, że banki działały w warunkach podwyższonej niepewności interpretacyjnej, zmuszone do równoległego projektowania rozwiązań i oczekiwania na ostateczne rozstrzygnięcia regulacyjne.

Równie istotnym źródłem trudności okazała się niewystarczająca komunikacja ze strony organów nadzorczych, co dodatkowo potęgowało ryzyko rozbieżnych interpretacji przepisów i zwiększało koszty dostosowania. W połączeniu z nierealistycznymi harmonogramami wdrożenia wskazanymi przez część respondentów, czynniki te tworzyły środowisko, w którym nawet dobrze przygotowane organizacje napotykały obiektywne bariery realizacyjne.

Relatywnie niski odsetek wskazań dotyczących przyczyn wewnętrznych – takich jak braki zasobowe czy zbyt późne rozpoznanie skali zmian – potwierdza, że banki w dużej mierze były świadome wyzwań

Wykres 4.3. Ocena zasobów banku do realizacji projektu dostosowania do DORA w momencie wdrożenia wymogu DORA.



Pyt. Czy w Pana(i) banku zapewniono odpowiednie zasoby (w tym ludzkie, budżety) do realizacji projektu dostosowania do DORA w momencie wdrożenia wymogu DORA tj. 17.01.2025 r.?

Źródło: wyniki badań własnych.

związanych z DORA i podejmowały działania przygotowawcze odpowiednio wcześnie. Opóźnienia nie wynikały więc z braku gotowości organizacyjnej, lecz z ograniczonej przewidywalności otoczenia regulacyjnego.

W szerszym ujęciu uzyskane wyniki wskazują na potrzebę lepszej synchronizacji procesów regulacyjnych i wdrożeniowych w przyszłych inicjatywach nadzorczych. Dla skutecznego i terminowego wdrażania regulacji o wysokim stopniu złożoności, takich jak DORA, kluczowe znaczenie ma zapewnienie wcześniejszej dostępności aktów wykonawczych, spójnej komunikacji oraz realnych harmonogramów, które umożliwią instytucjom finansowym przejście z etapu interpretacji do efektywnej realizacji wymogów regulacyjnych.

W większości banków zapewniono zasoby niezbędne do realizacji projektu dostosowania do wymogów DORA, jednak nie zawsze w pełni adekwatnym zakresie (wykres 4.3). Połowa badanych banków (50%) zadeklarowała, że zasoby ludzkie i budżetowe były wystarczające na moment wejścia w życie regulacji, tj. 17 stycznia 2025 r.

Jednocześnie 17% badanych wskazało, że choć zasoby zostały zapewnione, to konieczne były modyfikacje w trakcie realizacji projektu, co sugeruje potrzebę elastycznego podejścia do planowania zasobów w warunkach zmieniającego się otoczenia regulacyjnego.

Z kolei 33% respondentów przyznało, że nie zapewniono wystarczających zasobów, co mogło mieć bezpośredni wpływ na opóźnienia lub zwiększenie ryzyka w procesie wdrożenia DORA.

Mimo relatywnie wysokiego poziomu przygotowania organizacyjnego banków, kwestia adekwatności i skalowalności zasobów pozostaje jednym z kluczowych czynników ryzyka w realizacji dużych projektów regulacyjnych, takich jak DORA. Dostępność i adekwatność zasobów stanowiła jeden z kluczowych czynników różnicujących tempo i sprawność wdrażania regulacji DORA w badanych bankach. Choć większość instytucji podjęła działania zapewniające niezbędne zasoby ludzkie i budżetowe, skala oraz stabilność tego wsparcia nie zawsze okazywały się wystarczające.

Fakt, że jedynie połowa respondentów zadeklarowała pełną wystarczalność zasobów już na moment wejścia w życie regulacji, potwierdza, iż DORA była dla wielu banków projektem o wysokim stopniu złożoności i niepewności. Konieczność modyfikowania założeń zasobowych w trakcie realizacji projektu – wskazywana przez część badanach banków – podkreśla znaczenie elastycznego zarządzania projektami regulacyjnymi oraz zdolności do szybkiego

reagowania na nowe interpretacje, akty delegowane i wytyczne nadzorcze.

Jednocześnie relatywnie wysoki odsetek badanych banków, które nie zapewniły wystarczających zasobów, wskazuje, że ograniczenia kadrowe i budżetowe mogły realnie wpływać na ryzyko opóźnień, obniżenie jakości wdrożenia lub koncentrację działań wyłącznie na spełnieniu minimalnych wymogów zgodności. W kontekście wcześniejszych wyników badania, dotyczących niejasności interpretacyjnych oraz presji czasowej, niedobory zasobowe należy uznać za istotny czynnik wzmacniający ryzyko wdrożeniowe.

W szerszym ujęciu wyniki te potwierdzają, że skuteczna implementacja DORA wymaga nie tylko formalnego zaangażowania organizacyjnego, lecz także odpowiednio zaplanowanych, skalowalnych i długofalowych zasobów. Regulacja ta powinna być postrzegana nie jako jednorazowy projekt wdrożeniowy, lecz jako trwały element funkcjonowania banku, generujący stałe potrzeby w zakresie kompetencji, finansowania oraz zarządzania zmianą.

Podsumowując, badanie wskazuje, że zapewnienie adekwatnych zasobów pozostaje jednym z kluczowych warunków osiągnięcia dojrzałości regulacyjnej w obszarze DORA. Banki, które już na wczesnym etapie zagwarantowały stabilne wsparcie kadrowe i budżetowe, znajdują się w bardziej korzystnej pozycji do dalszego rozwoju odporności cyfrowej i spełniania przyszłych oczekiwań nadzorczych.

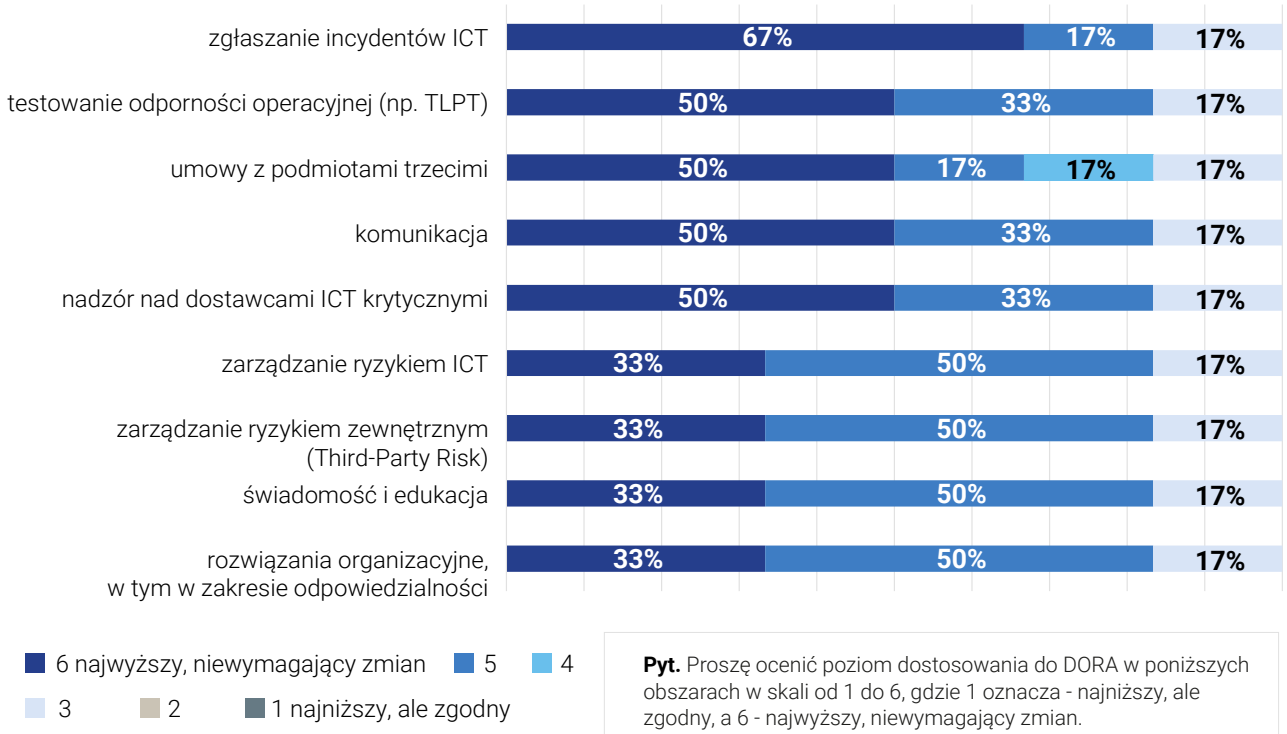
4.4 Ocena dostosowania banków do obszarów regulacji DORA

Banki osiągnęły wysoki, choć niejednorodny poziom dostosowania do poszczególnych obszarów tematycznych regulacji DORA. We wszystkich analizowanych obszarach instytucje spełniają co najmniej minimalne wymogi zgodności regulacyjnej, co potwierdza skuteczną mobilizację organizacyjną sektora bankowego w odpowiedzi na nowe obowiązki. Jednocześnie zróżnicowanie poziomu dojrzałości pomiędzy obszarami procesowymi, technicznymi i organizacyjnymi pokazuje, że DORA w praktyce nie jest regulacją jednowymiarową, lecz kompleksowym testem zdolności banków do integracji technologii, procesów, zarządzania ryzykiem oraz ładu korporacyjnego. Najwyższy poziom gotowości osiągnięto tam, gdzie wcześniejsze regulacje i nadzór wymusiły już ustrukturyzowane podejście operacyjne, natomiast obszary wymagające zmian kompetencyjnych i organizacyjnych pozostają kluczowym polem dalszego dostosowania regulacyjnego.

Kluczowe wnioski dotyczące dostosowania w obszarach regulacji DORA:

- Badane banki osiągnęły wysoki poziom zgodności regulacyjnej we wszystkich analizowanych obszarach, co potwierdza brak ocen niskich i wskazuje na skuteczne wdrożenie minimalnych wymogów DORA.
- Najwyższy poziom dojrzałości dotyczy obszarów procesowych i operacyjnych, w szczególności zgłaszania incydentów ICT oraz testowania odporności operacyjnej, które w wielu bankach funkcjonowały w ustrukturyzowanej formie już przed wejściem w życie DORA.
- W obszarach takich jak testowanie odporności, umowy z podmiotami trzecimi, komunikacja oraz nadzór nad krytycznymi dostawcami ICT dominują wysokie oceny, co wskazuje na zaawansowany etap wdrożenia, choć z zachowanym potencjałem dalszych usprawnień.
- Relatywnie niższy poziom dojrzałości występuje w obszarach zarządzania ryzykiem ICT, ryzykiem zewnętrznym (Third Party Risk), świadomości i edukacji oraz rozwiązań organizacyjnych, w tym przypisania ról i odpowiedzialności. Obszary te wymagają nie tylko doprecyzowania procedur, lecz także długofalowych działań w zakresie kultury organizacyjnej, kompetencji oraz integracji odpowiedzialności na poziomie całej instytucji.
- Pojawiające się niższe oceny wskazują na lokalne luki wdrożeniowe, które mogą wynikać z opóźnień regulacyjnych, ograniczeń zasobowych lub trwających jeszcze prac adaptacyjnych.
- Wyniki badania potwierdzają, że DORA pełni przede wszystkim rolę regulacji harmonizującej i porządkującej, a nie rewolucyjnej, zmuszającej banki do całkowitej przebudowy istniejących systemów.
- Kluczowym wyzwaniem nie była architektura technologiczna sama w sobie, lecz dostosowanie istniejących rozwiązań do spójnych

Wykres 4.4. Ocena dostosowania banków do obszarów regulacji DORA.



Pyt. Proszę ocenić poziom dostosowania do DORA w poniższych obszarach w skali od 1 do 6, gdzie 1 oznacza - najniższy, ale zgodny, a 6 - najwyższy, niewymagający zmian.

Źródło: wyniki badań własnych.

i jednoznacznych ram regulacyjnych, obejmujących procesy, odpowiedzialność oraz nadzór zarządczy.

- Ostatecznie badanie pokazuje, że trwała odporność cyfrowa banków będzie w największym stopniu zależeć od dojrzałości organizacyjnej i zarządczej, a nie wyłącznie od wdrożenia narzędzi technologicznych.

Uzyskane wyniki wskazują na zróżnicowany poziom dostosowania banków do wymogów DORA w analizowanych obszarach, przy jednoczesnym braku ocen skrajnie niskich (1–2), co sugeruje, że wszystkie badane instytucje osiągnęły co najmniej minimalny poziom zgodności regulacyjnej (wykres 4.4). Najwyżej ocenionym obszarem jest zgłaszanie incydentów ICT, gdzie 67% badanych banków wskazało najwyższy poziom dojrzałości (6 – niewymagający zmian). Oznacza to, że procesy raportowania incydentów są w większości banków dobrze ustrukturyzowane, wdrożone i operacyjnie sprawne. Pozostałe odpowiedzi w tym obszarze również potwierdzają wysoki stopień gotowości, z niewielkim marginesem na dalsze usprawnienia. Relatywnie wysoki poziom dostosowania odnotowano także w obszarach takich jak testowanie odporności operacyjnej (np. TLPT), umowy z podmiotami trzecimi, komunikacja oraz nadzór nad krytycznymi dostawcami ICT. W tych kategoriach około 50% banków oceniło swój poziom jako najwyższy (6), natomiast 33% wskazało ocenę 5, co sugeruje, że rozwiązania są w dużej mierze wdrożone, ale mogą wymagać dalszego doprecyzowania lub dostosowania do aktów wykonawczych i wytycznych nadzorczych.

Niższy – choć nadal zgodny – poziom dojrzałości widoczny jest w obszarach zarządzania ryzykiem ICT, zarządzania ryzykiem zewnętrznym (Third Party Risk), świadomości i edukacji oraz rozwiązań organizacyjnych, w tym przypisania odpowiedzialności. W tych obszarach dominują oceny 5 (50%) oraz 4 (17%), a jedynie 33% banków deklaruje najwyższy poziom dojrzałości. Wskazuje to, że są to obszary bardziej złożone organizacyjnie i kulturowo, wymagające dalszej pracy, integracji procesów oraz wzmocnienia kompetencji i odpowiedzialności na poziomie całej organizacji.

Istotne jest również to, że we wszystkich obszarach pojawia się niewielki odsetek ocen na poziomie 3 (17%), co może świadczyć o punktowych lukach

wdrożeniowych, wynikających m.in. z opóźnień regulacyjnych, ograniczeń zasobowych lub trwających jeszcze prac adaptacyjnych.

Podsumowując, badanie pokazuje, że banki osiągnęły wysoki, lecz niejednorodny poziom dostosowania do DORA. Największa dojrzałość dotyczy obszarów procesowych i operacyjnych (incydenty ICT, testy odporności), natomiast największy potencjał dalszych usprawnień widoczny jest w obszarach zarządczych, kompetencyjnych i organizacyjnych, które mają kluczowe znaczenie dla trwałej odporności cyfrowej w długim horyzoncie.

Uzyskane wyniki wskazują, że badane banki znajdują się na zaawansowanym etapie dostosowania do wymogów DORA, przy czym poziom tej dojrzałości nie jest jednorodny we wszystkich analizowanych obszarach. Brak ocen skrajnie niskich potwierdza, że wszystkie badane banki osiągnęły co najmniej minimalny poziom zgodności regulacyjnej, co świadczy o skutecznej mobilizacji organizacyjnej w odpowiedzi na nowe wymogi.

Najwyższy poziom dojrzałości widoczny jest w obszarach o charakterze procesowym i operacyjnym. Obszary te były już wcześniej przedmiotem intensywnego nadzoru i regulacji, co sprzyjało wcześniejszemu wypracowaniu stabilnych i funkcjonujących mechanizmów.

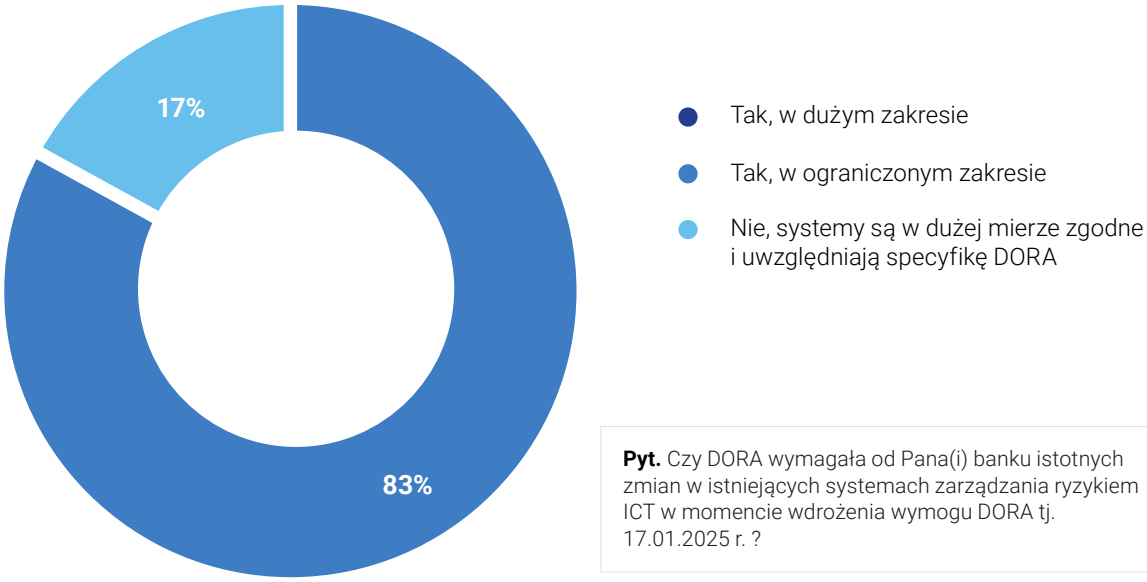
Jednocześnie badanie ujawnia, że relatywnie niższy – choć nadal zgodny – poziom dojrzałości dotyczy obszarów zarządczych i organizacyjnych. Są to obszary wymagające nie tylko zmian proceduralnych, lecz także długofalowych działań kulturowych, kompetencyjnych i strukturalnych, które trudniej wdrożyć w krótkim horyzoncie czasowym.

W szerszym ujęciu wyniki potwierdzają, że DORA nie jest regulacją czysto technologiczną, lecz regulacją systemową, która w największym stopniu testuje zdolność banków do integracji zarządzania ryzykiem ICT z ładem korporacyjnym, odpowiedzialnością menedżerską oraz kulturą organizacyjną. Osiągnięcie najwyższego poziomu dojrzałości w tych obszarach będzie kluczowe dla trwałej odporności cyfrowej sektora finansowego, zwłaszcza w kontekście rosnącej zależności od zewnętrznych dostawców ICT oraz złożoności ekosystemów technologicznych.

Wdrożenie regulacji DORA w większości banków wymagało zmian w istniejących systemach zarządzania ryzykiem ICT, jednak zmiany te miały przede wszystkim charakter ograniczony, a nie fundamentalny (wykres 4.5).

Zdecydowana większość badanych banków (83%) zadeklarowała, że DORA wymagała zmian w ograniczonym zakresie. Oznacza to, że banki posiadały już wcześniej funkcjonujące ramy zarządzania ryzykiem

Wykres 4.5. Ocena potrzeby istotnych zmian w istniejących systemach zarządzania ryzykiem ICT w momencie wdrożenia wymogu DORA.



Pyt. Czy DORA wymagała od Pana(i) banku istotnych zmian w istniejących systemach zarządzania ryzykiem ICT w momencie wdrożenia wymogu DORA tj. 17.01.2025 r. ?

Źródło: wyniki badań własnych.

ICT, które w znacznym stopniu spełniały nowe wymogi regulacyjne, natomiast konieczne było ich dostosowanie, uzupełnienie lub sformalizowanie, np. poprzez doprecyzowanie procedur, rozszerzenie zakresu kontroli, lepsze udokumentowanie procesów czy wzmocnienie mechanizmów nadzorczych.

Jednocześnie 17% badanych banków wskazało, że DORA nie wymagała istotnych zmian, ponieważ istniejące systemy zarządzania ryzykiem ICT były już w dużej mierze zgodne z regulacją i uwzględniały jej specyfikę. Może to dotyczyć instytucji, które wcześniej wdrożyły zaawansowane rozwiązania w zakresie odporności operacyjnej, bezpieczeństwa ICT oraz zarządzania ryzykiem zewnętrznym, często w odpowiedzi na wcześniejsze wytyczne nadzorcze lub międzynarodowe standardy.

Warto podkreślić, że żaden z badanych banków nie wskazał odpowiedzi „Tak, w dużym zakresie", co sugeruje, iż DORA nie była postrzegana jako regulacja wymuszająca całkowitą przebudowę systemów zarządzania ryzykiem ICT. Zamiast tego pełniła ona raczej rolę czynnika harmonizującego i porządkującego, integrującego dotychczasowe praktyki w spójne, jednolite ramy regulacyjne.

Wyniki badania potwierdzają, że regulacja DORA nie stanowiła dla większości banków punktu zerowego w obszarze zarządzania ryzykiem ICT, lecz raczej mechanizm konsolidujący i standaryzujący wcześniej wdrożone rozwiązania. Ograniczony zakres zmian deklarowany przez respondentów wskazuje na relatywnie wysoki poziom dojrzałości sektora bankowego w obszarze zarządzania ryzykiem technologicznym jeszcze przed formalnym wejściem w życie DORA.

Jednocześnie fakt, że większość banków była zmuszona do przynajmniej częściowych modyfikacji istniejących systemów, wskazuje, iż wcześniejsze rozwiązania – choć funkcjonalne – nie zawsze spełniały w pełni wymagania w zakresie formalizacji, dokumentacji, spójności procesowej oraz nadzoru korporacyjnego, jakie narzuca DORA.

W szerszym ujęciu badanie sugeruje, że rzeczywistym wyzwaniem wdrożeniowym nie była sama architektura systemów ICT, lecz ich dostosowanie do jednolitych, szczegółowych i audytowalnych ram regulacyjnych. DORA ujawniła tym samym różnice nie tyle w poziomie technologii, co w stopniu integracji zarządzania ryzykiem ICT z ładem korporacyjnym, raportowaniem oraz odpowiedzialnością zarządczą w bankach.

4.5 Wyzwania we wdrożeniu DORA

Wdrażanie regulacji DORA było dla badanych banków przede wszystkim wyzwaniem o charakterze interpretacyjnym i koordynacyjnym, a dopiero w drugiej kolejności technologicznym i zasobowym. Respondenci jednoznacznie akcentują, że kluczową barierą nie był brak narzędzi lub gotowych rozwiązań, lecz niepewność dotycząca praktycznej operacjonalizacji wymogów DORA, w tym spójności interpretacji i oczekiwań nadzorczych. Istotnym obszarem trudności okazało się również przeniesienie wymogów regulacyjnych na relacje z podmiotami trzecimi — w szczególności w zakresie nadzoru nad dostawcami ICT oraz renegocjacji umów — co wymagało jednoczesnego zaangażowania funkcji prawnych, zakupowych, bezpieczeństwa, IT i zarządzania ryzykiem. W konsekwencji badanie sugeruje, że największe ryzyka wdrożeniowe DORA wynikają z otoczenia regulacyjno-kontraktowego i złożoności zarządzania dostawcami, a nie z samej technologii.

Kluczowe wnioski dotyczące wyzwań wdrożeniowych DORA:

- Największym wyzwaniem we wdrażaniu DORA były niejasności interpretacyjne — wskazane przez 100% respondentów — co potwierdza, że główną barierą była niepewność regulacyjna, a nie braki technologiczne. Dominacja wyzwań interpretacyjnych oznacza, że banki musiały prowadzić wdrożenie w trybie „równoległym": projektowanie rozwiązań + ciągłe doprecyzowywanie interpretacji, co utrudniało harmonogramowanie i decyzje inwestycyjne.

- Drugi kluczowy blok wyzwań dotyczył podmiotów trzecich (third parties): nadzór i współpraca z dostawcami zewnętrznymi oraz renegocjacje umów z dostawcami zostały wskazane przez 83% banków, co pokazuje, że DORA najmocniej „uderza" w obszar kontraktowy, wymaga koordynacji wielu jednostek i negocjacji z dostawcami.

- Problemy stricte technologiczne i procesowe (integracja wymogów DORA z systemami ICT oraz ramami zarządzania ryzykiem) były wskazywane rzadziej (33%), co sugeruje, że w badanej próbie banki posiadały już relatywnie dojrzałe fundamenty ICT/ERM.

- Brak wsparcia regulatora pojawia się jako wyzwanie na poziomie 33%, ale w kontekście wy-

ników całości badania należy je interpretować jako element szerszego problemu: braku jednoznacznych wytycznych i spójnego przekazu.

- Bariery zasobowe i kosztowe miały drugorzędne znaczenie: braki kadrowe/kompetencyjne oraz koszty wdrożenia wskazało jedynie 17% respondentów — co oznacza, że w tej grupie banków kluczowe ryzyko wdrożenia wynikało bardziej z złożoności regulacyjnej i kontraktowej, niż z ograniczeń budżetowych.

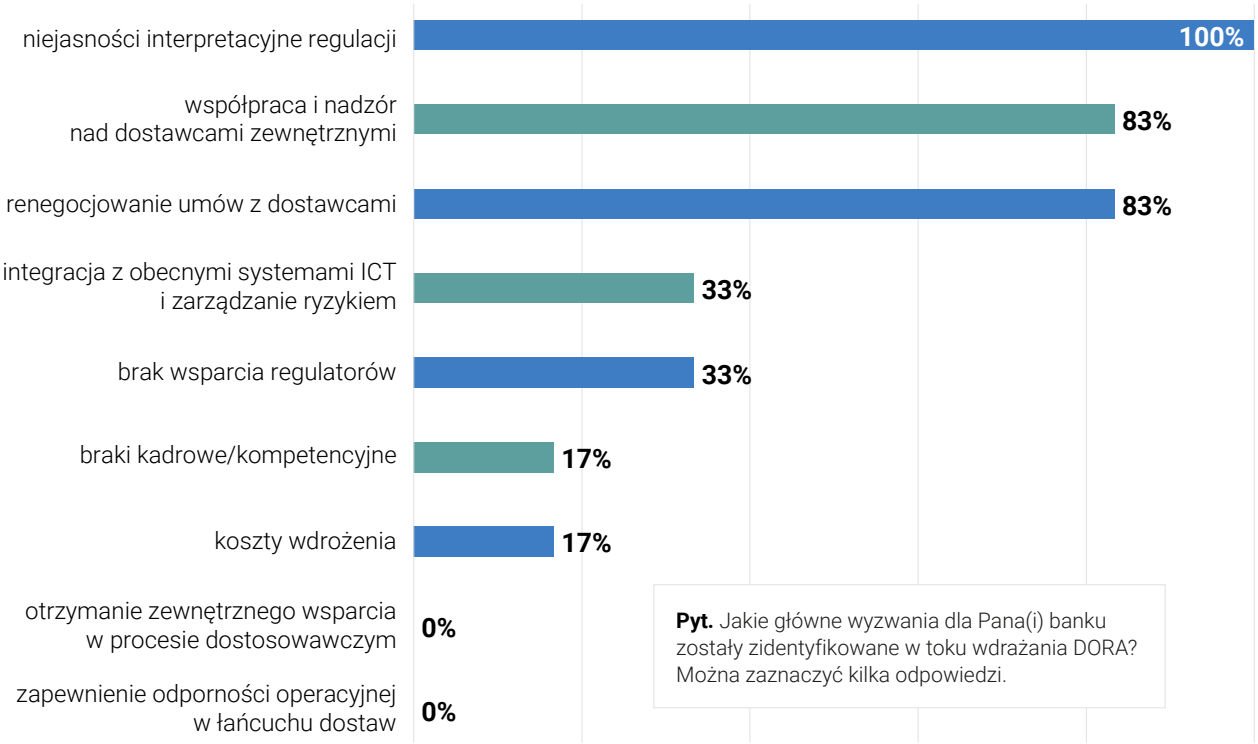
- Brak wskazań dotyczących trudności w pozyskaniu zewnętrznego wsparcia oraz odporności w łańcuchu dostaw (0%) sugeruje, że banki miały dostęp do rynku eksperckiego i bazowych mechanizmów ciągłości działania.

Wyniki badania jednoznacznie wskazują, że największym wyzwaniem we wdrażaniu regulacji DORA były kwestie interpretacyjne. Aż 100% respondentów wskazało niejasności interpretacyjne regulacji jako kluczowy problem w procesie dostosowawczym (wykres 4.6). Oznacza to, że banki mierzyły się przede wszystkim z brakiem jednoznacznych wytycznych co do sposobu praktycznego wdrożenia poszczególnych wymogów, co utrudniało planowanie działań, harmonogramowanie projektów oraz podejmowanie decyzji inwestycyjnych.

Drugą grupą istotnych wyzwań okazały się kwestie związane z relacjami z podmiotami trzecimi. Zarówno współpraca i nadzór nad dostawcami zewnętrznymi, jak i negocjowanie umów z dostawcami zostały wskazane przez 83% badanych banków. Wynik ten podkreśla, że jednym z najbardziej wymagających elementów DORA było dostosowanie relacji kontraktowych i nadzorczych do nowych obowiązków, w szczególności w zakresie dostawców ICT uznawanych za krytycznych. Proces ten wymagał nie tylko zmian prawnych, ale także koordynacji organizacyjnej.

Znacznie rzadziej wskazywanymi wyzwaniami były integracja wymogów DORA z istniejącymi systemami ICT oraz procesami zarządzania ryzykiem (33% odpowiedzi) oraz brak wsparcia ze strony regulatorów (33%). Może to sugerować, że od strony technologicznej i procesowej banki dysponowały już względnie dojrzałymi rozwiązaniami, natomiast brakowało im jednoznacznego kontekstu interpretacyjnego oraz jasnych sygnałów nadzorczych ułatwiających implementację.

Wykres 4.6. Wyzwania dla banku zidentyfikowane w toku wdrażania DORA.



Źródło: wyniki badań własnych.

Relatywnie najmniejsze znaczenie respondenci przypisali barierom zasobowym i finansowym. Braki kadrowe lub kompetencyjne oraz koszty wdrożenia zostały wskazane jedynie przez 17% badanych. Wynik ten potwierdza, że w analizowanej grupie banków DORA nie była postrzegana jako regulacja ograniczona głównie przez brak zasobów, lecz raczej jako wyzwanie o charakterze koncepcyjnym, prawnym i koordynacyjnym.

Co istotne, żaden z badanych banków nie wskazał problemów związanych z pozyskaniem zewnętrznego wsparcia w procesie dostosowawczym ani z zapewnieniem odporności operacyjnej w łańcuchu dostaw (0% odpowiedzi). Może to świadczyć o tym, że banki miały dostęp do odpowiednich źródeł wsparcia eksperckiego oraz posiadały już wcześniej mechanizmy zapewniające ciągłość działania i odporność operacyjną na poziomie całego łańcucha dostaw.

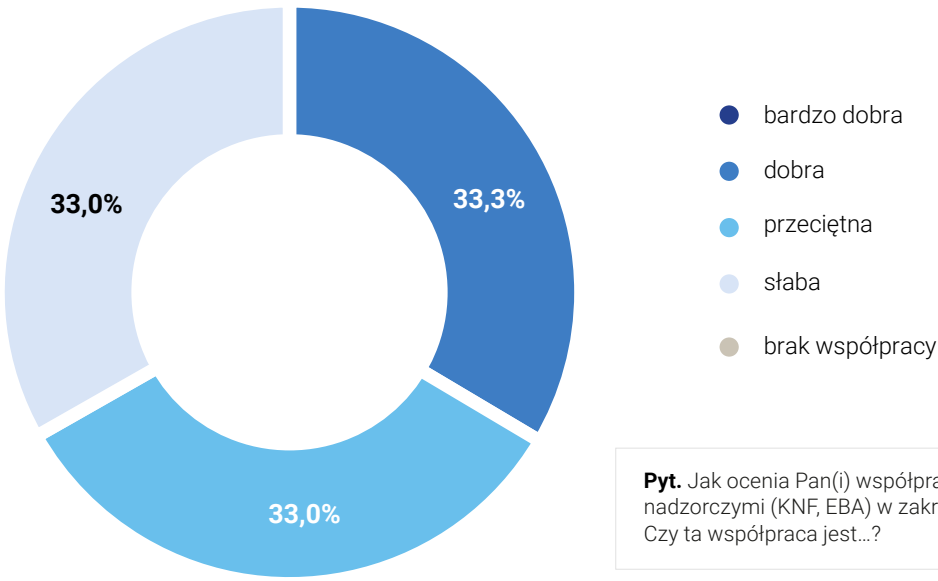
Uzyskane wyniki pozwalają stwierdzić, że badane banki osiągnęły relatywnie wysoki poziom dojrzałości organizacyjnej w obszarze wdrażania regulacji DORA, a sama regulacja jest postrzegana nie tylko jako obowiązek formalny, lecz także jako impuls wzmacniający cyberodporność i jakość zarządzania ryzykiem operacyjnym. Dominująca zgoda respondentów co do pozytywnego wpływu DORA na poziom cyberodporności banku oraz jej integracji z procesami zarządzania ryzykiem potwierdza, że regulacja została w znacznej mierze skutecznie osadzona w istniejących ramach zarządczych.

W szerszym kontekście całego badania wyniki te wpisują się w obserwowaną wcześniej tendencję, zgodnie z którą największe wyzwania związane z DORA nie mają charakteru stricte technicznego, lecz dotyczą interpretacji wymogów, koordynacji działań oraz długofalowego utrzymania zdolności organizacyjnych. DORA pełni zatem rolę regulacyjnego katalizatora zmian, który podnosi standardy zarządzania ryzykiem ICT, ale jednocześnie ujawnia różnice w gotowości organizacyjnej poszczególnych banków.

Wyniki badania wskazują na zróżnicowaną ocenę współpracy banków z organami nadzorczymi w procesie wdrażania regulacji DORA (wykres 4.7). Po 33,3% badanych banków oceniło tę współpracę jako dobrą, przeciętną oraz słabą, co oznacza brak dominującej, jednoznacznie pozytywnej lub negatywnej oceny relacji z nadzorem.

Jednocześnie żaden z badanych banków nie wskazał oceny „bardzo dobrej", co może sugerować, że współpraca – choć w wielu przypadkach istniała – nie była postrzegana jako w pełni wystarczająca. Równie istotne jest to, że nie odnotowano odpowiedzi wskazujących na całkowity brak współpracy, co potwierdza, że kanały komunikacji pomiędzy bankami a instytucjami nadzorczymi funkcjonowały. Roz-

Wykres 4.7. Ocenia współpracy banku z organami nadzorczymi (KNF, EBA) w zakresie wdrożenia DORA



Pyt. Jak ocenia Pan(i) współpracę banku z organami nadzorczymi (KNF, EBA) w zakresie wdrożenia DORA? Czy ta współpraca jest…?

Źródło: wyniki badań własnych.

kład odpowiedzi sugeruje, że jakość i efektywność tej współpracy była silnie zróżnicowana pomiędzy bankami w procesie implementacji DORA.

W kontekście wcześniejszych wyników badania, wskazujących na powszechne niejasności interpretacyjne regulacji, brak ocen „bardzo dobrych" oraz znaczący odsetek ocen „słabych" może sugerować, że banki oczekiwały bardziej jednoznacznych wytycznych, intensywniejszego dialogu oraz większego wsparcia interpretacyjnego ze strony KNF i EBA w kluczowych obszarach wdrożenia DORA.

Wyniki dotyczące oceny współpracy z organami nadzorczymi wskazują, że relacja banków z KNF i EBA w procesie wdrażania DORA miała charakter funkcjonalny, lecz w wielu przypadkach niewystarczająco wspierający z perspektywy instytucji wdrażających regulację. W kontekście całego badania DORA można wnioskować, że jednym z kluczowych czynników ograniczających efektywność wdrożenia była niedostateczna klarowność interpretacyjna oraz brak spójnego, jednolitego przekazu ze strony nadzoru. Banki, mimo aktywnego zaangażowania we wdrożenie regulacji, często zmuszone były samodzielnie interpretować wymagania DORA, co zwiększało ryzyko rozbieżnych praktyk, wydłużało procesy dostosowawcze i generowało dodatkowe obciążenia organizacyjne. Uzyskane wyniki potwierdzają, że skuteczność implementacji tak złożonych regulacji jak DORA w istotnym stopniu zależy nie tylko od gotowości samych instytucji finansowych, lecz również od jakości dialogu regulacyjnego. W tym kontekście badanie wskazuje na potrzebę dalszego wzmacniania roli nadzoru jako aktywnego partnera wdrożeniowego – poprzez wcześniejsze publikowanie wytycznych, bardziej jednoznaczne interpretacje oraz systematyczne działania edukacyjne skierowane do sektora bankowego.

Analiza jakościowa odpowiedzi respondentów wskazuje na spójny zestaw problemów i napięć, które pojawiały się w relacjach banków z organami nadzorczymi w procesie wdrażania regulacji DORA.[33]

> *„Zakres informacji wymagany do przekazania do KNF był nieadekwatny do wyznaczonego terminu. Przykładem jest wprowadzenie wymagania zaraportowania SPF_PF_01 w trakcie opracowywania i przekazywania raportów SPF_PF_26 oraz SPF_PF_27"*

> *„Adresowaliśmy wyzwania do organów nadzorczych KNF związane z DORA za pośrednictwem ZBP. Często poruszane przez nas kwestie pozostawały bez konkretnych i jednoznacznych odpowiedzi regulatora, pozostawiając spory wachlarz interpretacyjny, co w konsekwencji miało ogromny wpływ na wdrożenie. Na plus odnotowujemy ostatnie działania szkoleniowe (CEDUR) dotyczące wypełniania poszczególnych raportów zarządczych."*

> *„Testowanie odporności operacyjnej, w tym kluczowych dostawców. Proporcjonalność środków i wymagań względem skali działania podmiotu. Zapewnienie zgodności dużych i międzynarodowych dostawców usług ICT"*

> *„Wymagania sprawozdawcze zaprezentowane zbyt późno w stosunku do wymaganych terminów dostarczenia informacji. Zakres sprawozdań powinien być zaprezentowany wcześniej, żeby dostosować swoje wewnętrzne procedury zbierania danych."*

> *„Banki do ostatniej chwili nie wiedzą jakich informacji będzie się od nich oczekiwać, a w momencie opublikowania sprawozdań mają bardzo krótki okres na dostarczenie informacji."*

> *„Z otrzymanych sprawozdań SPR-PR-01 zauważamy podejście interpretacyjne dotyczące DORA zakorzenione w wymaganiach rekomendacji D w zakresie analizy ryzyka. Nowa forma raportowania- formularze KNF SPR--PR-01 – został obarczony błędami co powoduje brak możliwości przekazania formularza do systemu SDD"*

Pomimo różnic w sformułowaniach, odpowiedzi koncentrują się wokół kilku wyraźnych obszarów tematycznych.

1. Opóźnienia i nieadekwatność wymagań sprawozdawczych

Respondenci wielokrotnie wskazywali na zbyt późne publikowanie wymagań raportowych

33 Pyt. A biorąc pod uwagę współpracę Pana(i) banku z organami nadzorczymi (KNF, EBA) w zakresie wdrożenia DORA, czy ma Pan(i) jakieś uwagi do tej współpracy? Jeśli tak proszę je syntetycznie opisać.

w stosunku do terminów ich realizacji. Zakres informacji wymaganych przez KNF był oceniany jako nieproporcjonalny do dostępnego czasu, co znacząco utrudniało przygotowanie danych oraz dostosowanie wewnętrznych procesów raportowych. Wskazywano również na sytuacje, w których nowe obowiązki sprawozdawcze pojawiały się w trakcie trwania innych procesów raportowych, co prowadziło do kumulacji obciążeń i chaosu organizacyjnego.

2. Brak jednoznacznych interpretacji regulacyjnych

Istotnym wątkiem było poczucie niewystarczającej klarowności interpretacyjnej po stronie regulatorów. Respondenci podkreślali, że zgłaszane – często za pośrednictwem ZBP – pytania i wątpliwości dotyczące DORA pozostawały bez precyzyjnych odpowiedzi, co skutkowało szerokim polem interpretacyjnym. Taka sytuacja wymuszała na bankach podejmowanie decyzji wdrożeniowych w warunkach wysokiej niepewności regulacyjnej, zwiększając ryzyko niezgodności lub konieczności późniejszych korekt.

3. Problemy techniczne i operacyjne w procesie raportowania

W odpowiedziach pojawiły się również uwagi dotyczące niskiej jakości narzędzi raportowych udostępnianych przez regulatora. Przykładem są formularze raportowe, które – według respondentów – zawierały błędy techniczne, uniemożliwiające ich poprawne przesłanie do systemów KNF. Tego rodzaju problemy były szczególnie dotkliwe w sytuacji krótkich terminów i braku alternatywnych ścieżek raportowania.

4. Proporcjonalność wymagań i rola dostawców zewnętrznych

Respondenci zwracali uwagę na niewystarczające uwzględnienie zasady proporcjonalności, zwłaszcza w kontekście testowania odporności operacyjnej oraz nadzoru nad kluczowymi dostawcami ICT. Wskazywano, że wymagania wobec banków nie zawsze były adekwatne do skali ich działalności, a jednocześnie brakowało jasnych mechanizmów zapewnienia zgodności dużych, międzynarodowych dostawców usług ICT z wymogami DORA.

5. Pozytywne sygnały – działania edukacyjne regulatora

Mimo licznych krytycznych uwag, respondenci odnotowali również pozytywne aspekty współpracy, w szczególności w postaci działań szkoleniowych organizowanych przez KNF (CEDUR). Szkolenia dotyczące wypełniania raportów zarządczych zostały ocenione jako krok w dobrym kierunku, choć pojawiały się relatywnie późno w procesie wdrożenia.

Analiza odpowiedzi otwartych wskazuje, że głównym problemem we współpracy banków z organami nadzorczymi w procesie wdrażania DORA nie był brak kontaktu, lecz niedostateczna przewidywalność, jednoznaczność i operacyjna użyteczność przekazywanych wymagań. Opóźnienia w publikowaniu wytycznych, szerokie pole interpretacyjne oraz problemy techniczne w raportowaniu znacząco zwiększały obciążenie organizacyjne banków i podnosiły ryzyko wdrożeniowe.

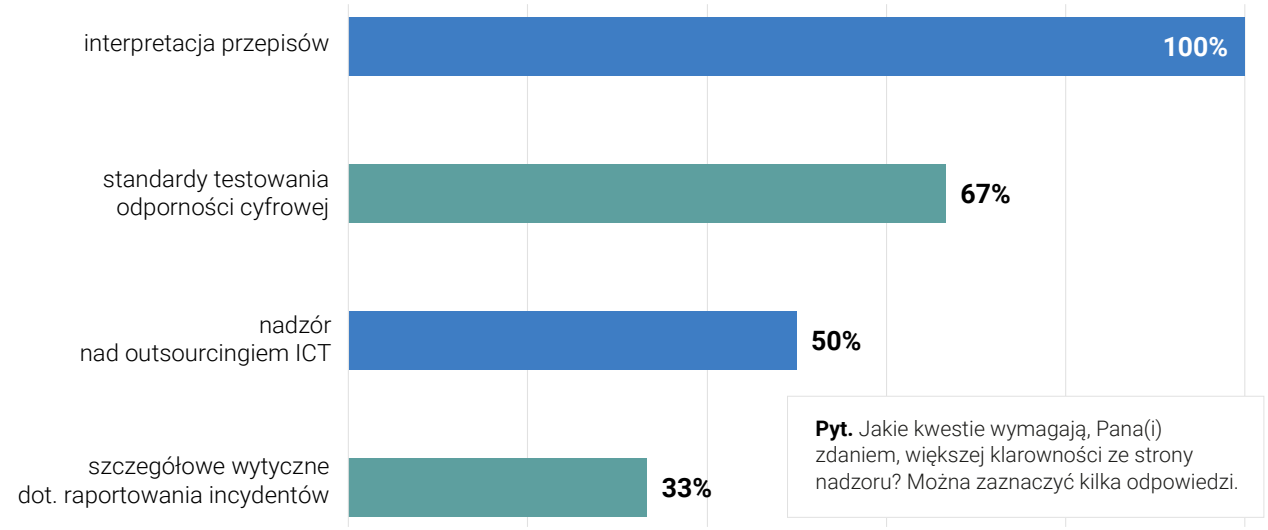
Jednocześnie odpowiedzi respondentów sugerują, że rola regulatora ewoluuje w kierunku bardziej aktywnego wsparcia edukacyjnego, co zostało pozytywnie ocenione. Wyniki badania wskazują jednak, że aby skutecznie wspierać implementację tak złożonych regulacji jak DORA, niezbędne jest wcześniejsze udostępnianie stabilnych wymagań, większa jednoznaczność interpretacyjna oraz lepsze przygotowanie narzędzi operacyjnych.

W kontekście całego badania można stwierdzić, że jakość współpracy z nadzorem stanowi jeden z kluczowych czynników wpływających na tempo, koszty i ryzyko wdrożenia DORA w bankach, a doświadczenia z tego procesu będą miały istotne znaczenie dla przyszłych regulacji z obszaru odporności operacyjnej i zarządzania ryzykiem ICT.

Odpowiedzi respondentów jednoznacznie wskazują, że największym obszarem niepewności regulacyjnej pozostaje interpretacja przepisów DORA (wykres 4.8). Wszyscy uczestnicy badania (100%) zaznaczyli tę odpowiedź, co potwierdza, że brak jednoznacznych i spójnych interpretacji jest postrzegany jako kluczowa bariera w procesie wdrażania regulacji. Wynik ten koresponduje z wnioskami płynącymi z pytania otwartego, w którym respondenci podkreślali szerokie pole interpretacyjne i niewystarczające wsparcie merytoryczne ze strony nadzoru.

Drugim najczęściej wskazywanym obszarem wymagającym doprecyzowania są standardy testo-

Wykres 4.8. Kluczowe kwestie wymagające większej klarowności ze strony nadzoru.



Źródło: wyniki badań własnych.

wania odporności cyfrowej, w tym w szczególności testy zaawansowane (np. TLPT). Aż 67% respondentów uznało ten element za wymagający większej klarowności. Wskazuje to na istotne wątpliwości dotyczące zakresu, częstotliwości oraz proporcjonalności testów, a także roli dostawców zewnętrznych w procesie testowania odporności operacyjnej.

Kolejnym ważnym obszarem jest nadzór nad outsourcingiem ICT, który został wskazany przez 50% respondentów. Wynik ten sugeruje, że banki oczekują bardziej precyzyjnych wytycznych dotyczących odpowiedzialności, zakresu kontroli oraz praktycznych oczekiwań nadzorczych wobec relacji z dostawcami zewnętrznymi, w szczególności tymi o charakterze krytycznym i transgranicznym.

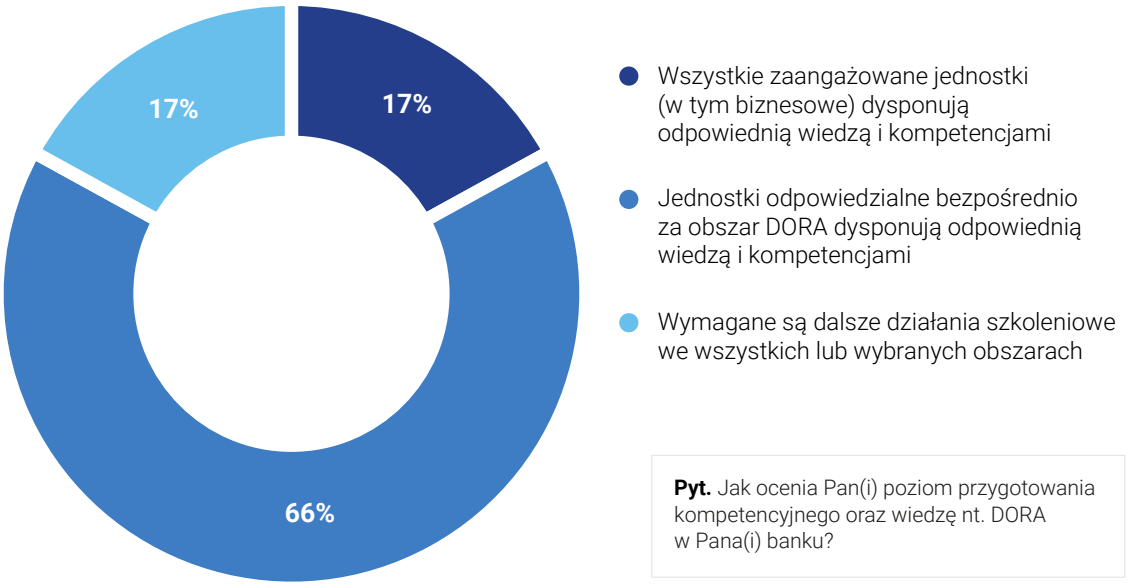
Relatywnie rzadziej, choć nadal istotnie, wskazywano na potrzebę doprecyzowania szczegółowych wytycznych dotyczących raportowania incydentów ICT (33%). Może to świadczyć o tym, że ogólna struktura procesu raportowania jest już w bankach rozpoznana, jednak nadal występują wątpliwości dotyczące klasyfikacji incydentów, progów istotności oraz zakresu wymaganych informacji.

Kluczowym wyzwaniem wdrożeniowym DORA nie są same cele regulacji, lecz brak wystarczającej precyzji w ich operacjonalizacji. Badani w największym stopniu oczekują od nadzoru jasnych, jednoznacznych i możliwych do praktycznego zastosowania interpretacji przepisów, które ograniczyłyby ryzyko rozbieżnych wdrożeń oraz późniejszych korekt.

Z perspektywy całego badania można stwierdzić, że zwiększenie klarowności regulacyjnej – zwłaszcza w obszarach interpretacji przepisów, testowania odporności cyfrowej oraz outsourcingu ICT – byłoby jednym z najważniejszych czynników wspierających stabilne i efektywne wdrożenie DORA w sektorze bankowym. Jednocześnie brak takiej klarowności zwiększa koszty wdrożenia, obciążenie organizacyjne oraz ryzyko regulacyjne po stronie banków.

Uzyskane wyniki wskazują na zróżnicowany, lecz generalnie umiarkowanie pozytywny poziom przygotowania kompetencyjnego banków w zakresie DORA (wykres 4.9). Największa grupa banków (66%) zadeklarowała, że odpowiednią wiedzą i kompetencjami dysponują jednostki bezpośrednio odpowiedzialne za obszar DORA. Oznacza to, że kluczowe funkcje odpowiedzialne za wdrożenie regulacji zostały w większości banków przygotowane merytorycznie do realizacji nowych wymogów. Jednocześnie jedynie 17% respondentów wskazało, że wszystkie zaangażowane jednostki – w tym jednostki biznesowe – posiadają wystarczającą wiedzę i kompetencje w zakresie DORA. Wynik ten sugeruje, że świadomość regulacyjna oraz zrozumienie wymogów DORA nie są jeszcze w pełni rozpowszechnione w całej organizacji, a wiedza ta pozostaje w dużej mierze skoncentrowana w wyspecjalizowanych zespołach. Istotnym sygnałem jest również fakt, że 17% badanych uznało, iż wymagane są dalsze działania szkoleniowe we wszystkich lub wybranych obszarach banku. Choć odsetek ten nie jest dominujący, wskazuje on na realną potrzebę kontynuowania lub pogłębiania działań edukacyjnych, szczególnie

Wykres 4.9. Ocena poziomu przygotowania kompetencyjnego oraz wiedzy nt. DORA w banku?



Pyt. Jak ocenia Pan(i) poziom przygotowania kompetencyjnego oraz wiedzę nt. DORA w Pana(i) banku?

Źródło: wyniki badań własnych.

w kontekście rosnącej roli jednostek biznesowych w procesach zarządzania ryzykiem ICT, outsourcingiem oraz reagowaniem na incydenty operacyjne.

Banki skoncentrowały wysiłki kompetencyjne przede wszystkim na jednostkach bezpośrednio odpowiedzialnych za wdrożenie DORA, co było naturalnym i koniecznym pierwszym krokiem. Jednocześnie jednak pełna operacjonalizacja DORA wymaga szerszego zakorzenienia wiedzy regulacyjnej w całej organizacji, w tym po stronie biznesu, zakupów, zarządzania relacjami z dostawcami oraz kadr menedżerskich.

Z perspektywy całości badania można stwierdzić, że kompetencje w zakresie DORA są obecnie „punktowo dojrzałe", lecz organizacyjnie nierównomiernie rozłożone. Oznacza to, że dalsze etapy wdrażania regulacji – zwłaszcza te związane z testowaniem odporności operacyjnej, outsourcingiem ICT oraz raportowaniem incydentów – będą wymagały systematycznych, ukierunkowanych działań szkoleniowych i komunikacyjnych, aby zapewnić spójność podejścia w całym banku.

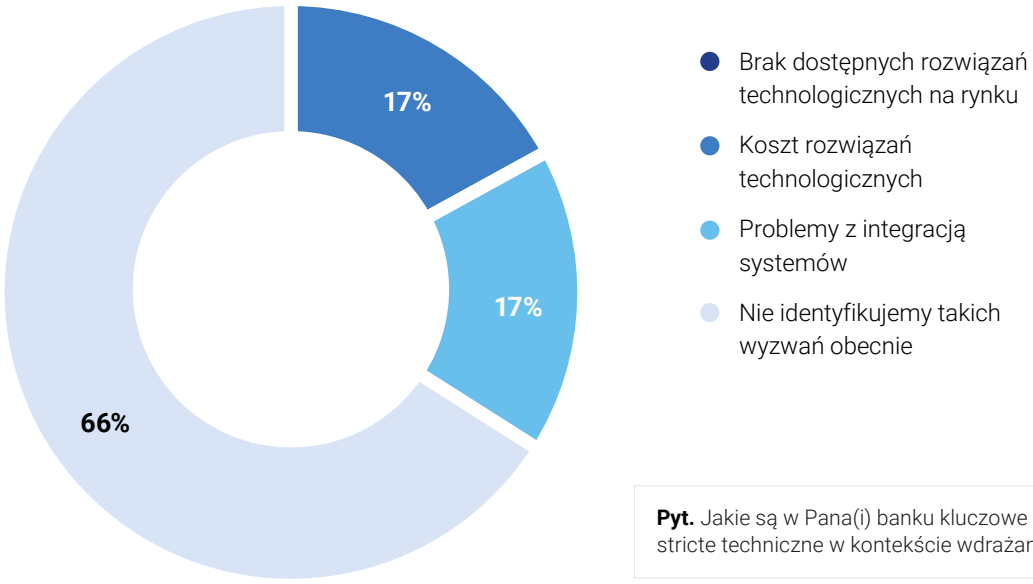
Większość badanych banków nie identyfikuje obecnie istotnych barier stricte technicznych we wdrażaniu DORA (wykres 4.10). 66% badanych banków zadeklarowało, że nie występują w ich organizacjach znaczące wyzwania technologiczne związane z implementacją regulacji. Może to świadczyć o relatywnie wysokim poziomie dojrzałości infrastruktury ICT oraz o tym, że kluczowe rozwiązania technologiczne zostały już wdrożone lub są wystarczające do spełnienia podstawowych wymogów DORA. Jednocześnie 17% badanych wskazało na problemy z integracją systemów, co sugeruje, że w części banków wyzwaniem pozostaje połączenie nowych rozwiązań lub procesów DORA z istniejącą architekturą ICT. Kolejne 17% badanych wskazało na koszt rozwiązań technologicznych jako istotne wyzwanie. Odpowiedź ta pokazuje, że choć dostępność narzędzi rynkowych nie stanowi zasadniczego problemu, to nakłady finansowe związane z ich zakupem, wdrożeniem i utrzymaniem mogą stanowić barierę.

Warto również zauważyć, że żaden z respondentów nie wskazał na brak dostępnych rozwiązań technologicznych na rynku jako problem, co potwierdza, że rynek dostawców ICT w obszarze DORA jest postrzegany jako wystarczająco rozwinięty.

4.6 Dobre praktyki i narzędzia

Skuteczne wdrożenie DORA w bankach opiera się nie na pojedynczym narzędziu, lecz na spójnym modelu zarządczym, który łączy: dojrzałe ramy zarządzania ryzykiem ICT, uporządkowane zarządzanie dostawcami, ustandaryzowane rejestry i ewidencje, stały monitoring oraz silne umocowanie projektu na poziomie Zarządu. Respondenci wskazują, że naj-

Wykres 4.10. Kluczowe wyzwania stricte techniczne w kontekście wdrażania DORA.



Pyt. Jakie są w Pana(i) banku kluczowe wyzwania stricte techniczne w kontekście wdrażania DORA?

Źródło: wyniki badań własnych.

większą wartość daje centralizacja działań DORA (zarówno w obszarze ryzyka ICT, jak i third-party), wsparcie procesów przez praktyczne narzędzia (mapowanie wymagań, rejestry, monitoring), a także: szkolenia, komunikacja i budowanie świadomości w całej organizacji. W praktyce oznacza to wdrożenie DORA jako programu organizacyjnego, a nie wyłącznie inicjatywy compliance/IT.

Kluczowe wnioski – dobre praktyki

- Centralizacja DORA pojawia się jako jeden z pożądanych modeli. Łączenie zarządzania ryzykiem ICT oraz ryzykiem dostawców ICT w spójnym modelu odpowiedzialności.
- Najczęściej powtarzającym się filarem jest Vendor Management / Third-Party Risk Management: proces oceny dostawców usług IT, jednolita ewidencja dostawców i usług ICT, rejestr umów + porządkowanie relacji kontraktowych.
- Banki wskazują, że wdrożenie DORA przyspiesza, gdy ma formułę projektu o odpowiedniej randze: powołanie Komitetu Sterującego, zaangażowanie Zarządu i top managementu, dedykowany koordynator / zespół DORA.
- Wysoko oceniane są monitoring IT w czasie rzeczywistym, uporządkowane zarządzanie incydentami ICT, regularne testy ciągłości działania (BCM), systemowa ocena ryzyka ICT, narzędzia cyberbezpieczeństwa jako część jednego systemu.
- Respondenci podkreślają znaczenie kompletnej dokumentacji i rejestrów jako praktycznego warunku zgodności: rejestr zasobów ICT, rejestr umów, regulacje wewnętrzne (polityki/procedury).

Odpowiedzi otwarte respondentów pokazują, że skuteczne wdrażanie DORA w badanych bankach opiera się na połączeniu wymagań regulacyjnych, procesów operacyjnych oraz silnego modelu zarządczego.[34]

„Dobrze zaimplementowane standardy Rekomendacji D. Dobrze wdrożone procesy Vendor Managementu i oceny dostawców usług IT."

„Centralizacja procesu DORA (zarządzenie ryzykiem ICT oraz zarzadzanie ryzykiem ze strony dostawców ICT."

„Monitorowanie IT w czasie rzeczywistym, uporządkowane zarządzanie incydentami,

34 Jakie praktyki lub narzędzia ICT w Pana(i) banku wspierają skuteczne wdrażanie DORA?

regularne testy ciągłości działania oraz ocena ryzyka ICT. W połączeniu z procesami cyberbezpieczeństwa daje to spójny system zarządzania odpornością operacyjną."

„Wsparcie firm zewnętrznych we wdrożeniu DORA."

„System zarzadzania ryzykiem ICT. System Zarządzania Ciągłością Działania."

„Powołanie Komitetu Sterującego."

„Zaangażowanie Zarządu i najwyższej kadry kierowniczej."

„Jednolita ewidencja Dostawców i Usług ICT."

„Dedykowany Zespół/Koordynator pod klasyfikację i raportowanie incydentów

Rejestr umów."

„Rejestr zasobów ICT."

„Narzędzia cyberbezpieczeństwa."

„Regulacje wewnętrzne."

„Powołanie koordynatora wdrażania DORA, prowadzenie Excela z mapowaniem wymagań."

„Wsparcie CIO oraz zewnętrznych ekspertów w razie potrzeby."

Na podstawie wypowiedzi można wyróżnić kilka kluczowych obszarów.

1. Wykorzystanie istniejących ram regulacyjnych i wewnętrznych

Silnym motywem w odpowiedziach jest odwołanie do dobrze zaimplementowanych standardów Rekomendacji D, które stanowią naturalny punkt wyjścia dla DORA. Respondenci wskazują, że: wcześniejsze inwestycje w regulacje krajowe, uporządkowane polityki i procedury pozwoliły ograniczyć skalę zmian i szybciej zaadaptować nowe wymagania. DORA jest w tym ujęciu raczej rozszerzeniem i uszczegółowieniem istniejących ram niż zupełnie nowym obszarem.

2. Zarządzanie dostawcami ICT

Bardzo wyraźnie wybrzmiewa znaczenie dobrze wdrożonych procesów Vendor Managementu oraz oceny dostawców usług IT. Respondenci wskazują na jednolitą ewidencję dostawców i usług ICT, rejestry umów, cykliczną ocenę ryzyka dostawców, formalne wymagania kontraktowe. Praktyki te są postrzegane jako kluczowe dla spełnienia wymogów DORA.

3. Centralizacja zarządzania DORA i ryzykiem ICT

Podobnie jak w poprzednich pytaniach, respondenci silnie akcentują centralizację procesu DORA, obejmującą zarządzanie ryzykiem ICT, zarządzanie ryzykiem dostawców ICT, koordynację raportowania i klasyfikacji incydentów. Centralizacja ta jest wspierana przez dedykowanych koordynatorów lub zespoły, Komitety Sterujące, bezpośrednie zaangażowanie Zarządu i najwyższej kadry kierowniczej. Taki model pozwala na spójność decyzyjną, lepszą kontrolę oraz skuteczniejsze reagowanie na incydenty i ryzyka.

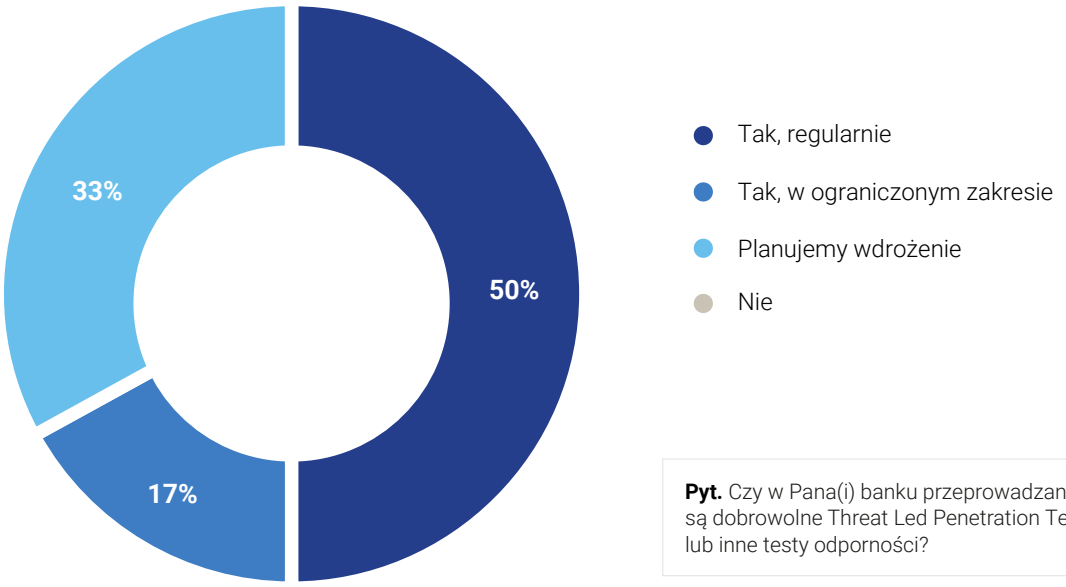
4. Operacyjne mechanizmy odporności i monitoringu

Respondenci wskazują na szeroki zestaw narzędzi i praktyk operacyjnych, które razem tworzą spójny system zarządzania odpornością operacyjną, w tym: monitorowanie IT w czasie rzeczywistym, uporządkowane procesy zarządzania incydentami, regularne testy ciągłości działania, systemowe zarządzanie ryzykiem ICT, narzędzia cyberbezpieczeństwa. Kluczowe jest podkreślenie, że narzędzia te funkcjonują w powiązaniu z procesami, a nie jako autonomiczne rozwiązania technologiczne.

5. Zarządzanie informacją, ewidencją i dokumentacją

W odpowiedziach pojawia się również silny nacisk na rejestry zasobów ICT, ewidencje umów i dostawców, mapowanie wymagań DORA. Respondenci wskazują, że transparentność informacji i porządek dokumentacyjny znacząco ułatwiają zarówno wdrożenie, jak i bieżące utrzymanie zgodności regulacyjnej.

Wykres 4.11. Realizacja dobrowolnych Threat Led Penetration Testing (TLPT) w banku.



Pyt. Czy w Pana(i) banku przeprowadzane są dobrowolne Threat Led Penetration Testing (TLPT) lub inne testy odporności?

Źródło: wyniki badań własnych.

Analiza pokazuje, że skuteczne wdrażanie DORA w badanych bankach jest rezultatem synergii trzech elementów: ram regulacyjnych, uporządkowanych procesów operacyjnych oraz silnego modelu zarządczego. Respondenci nie wskazują pojedynczych „kluczowych narzędzi", lecz raczej zintegrowany system zarządzania odpornością operacyjną, w którym technologia pełni rolę wspierającą, a nie dominującą. Wyniki te są spójne z wcześniejszymi wnioskami badania i potwierdzają, że: DORA nie jest regulacją stricte technologiczną, największą wartość przynoszą rozwiązania systemowe i organizacyjne, banki, które wcześniej zainwestowały w zarządzanie ryzykiem ICT, Vendor Management i ład korporacyjny, osiągają dziś najwyższy poziom dojrzałości.

Uzyskane wyniki wskazują, że testowanie odporności operacyjnej, w tym TLPT lub inne formy testów bezpieczeństwa, jest w badanych bankach w różnym stopniu zaawansowania (wykres 4.11). Połowa badanych banków (50%) zadeklarowała, że testy odporności są przeprowadzane regularnie, co świadczy o wysokiej dojrzałości w obszarze zarządzania ryzykiem ICT oraz o proaktywnym podejściu do wymogów DORA, wykraczającym poza minimalny poziom zgodności regulacyjnej. Jednocześnie 17% badanych wskazało, że testy są realizowane, ale w ograniczonym zakresie. Może to oznaczać, że działania testowe koncentrują się na wybranych obszarach infrastruktury lub procesach krytycznych, bez pełnego wdrożenia podejścia Threat Led Penetration Testing, które zakłada kompleksowe, scenariuszowe testowanie odporności organizacji na zaawansowane zagrożenia. Istotna część respondentów (33%) zadeklarowała, że w ich bankach testy odporności są dopiero planowane. Wskazuje to, że mimo świadomości znaczenia testowania odporności operacyjnej w kontekście DORA, część banków znajduje się nadal na etapie przygotowawczym — obejmującym m.in. projektowanie podejścia testowego, ocenę gotowości organizacyjnej lub analizę kosztów i zasobów niezbędnych do realizacji TLPT. Warto podkreślić, że żaden z respondentów nie wskazał odpowiedzi „Nie", co oznacza, że wszystkie badane banki albo już realizują testy odporności, albo planują ich wdrożenie. Jest to istotny sygnał wysokiego poziomu świadomości regulacyjnej oraz powszechnego uznania testów odporności za kluczowy element systemu zarządzania ryzykiem ICT w ramach DORA.

Testowanie odporności operacyjnej staje się standardem w sektorze bankowym, choć poziom jego zaawansowania jest zróżnicowany. Banki, które już regularnie realizują TLPT lub inne testy, są lepiej przygotowane na spełnienie przyszłych oczekiwań nadzorczych oraz na skuteczne zarządzanie zaawansowanymi zagrożeniami cybernetycznymi. Jednocześnie znaczący odsetek banków planujących wdrożenie testów wskazuje, że DORA pełni rolę katalizatora przyspieszającego rozwój praktyk testowania odporności, nawet tam, gdzie wcześniej miały one charakter ograniczony lub incydentalny.

Analiza wypowiedzi respondentów pokazuje wysoki poziom spójności w postrzeganiu tego, co realnie działa przy wdrażaniu DORA. Odpowiedzi koncentrują się przede wszystkim na modelu zarządczym, organizacyjnym i koordynacyjnym, co jest zgodne z wcześniejszymi wynikami badania wskazującymi, że DORA jest regulacją systemową, a nie wyłącznie technologiczną.[35] Do kluczowych dobrych praktyk, które badani rekomendują przy wdrażaniu DORA należą:

„Centralizacja procesu DORA (zarządzenie ryzykiem ICT oraz zarzadzanie ryzykiem ze strony dostawców ICT."

„Wypracowanie standardu szablonu Umów z regulacjami DORA. Realizacja w formule projektowej w Banku (odpowiednia ranga)."

„Szkolenia użytkowników, zwiększanie świadomości i zasadności wytycznych w tym zakresie. Wdrożenie zarządzania incydentami ICT."

„Powołanie projektu mającego na celu wdrożenie zmian regulacyjnych i operacyjnych wymagane w całej organizacji."

„Analiza luk i mapowanie procesów."

„Włączenie zespołów IT, bezpieczeństwa, compliance, ryzyka i biznesu w proces wdrożenia Regularna komunikacja i szkolenia dla pracowników."

„Wdrożenie spójnych procedur oceny ryzyka dla systemów i dostawców. Wdrożenie narzędzi do ciągłego monitorowania ryzyk ICT i incydentów."

„Powołanie Komitetu Sterującego. Zaangażowanie Zarządu i najwyższej kadry kierowniczej Jednolita ewidencja Dostawców i Usług ICT."

„Stworzenie kompleksowych, udokumentowanych ram zarządzania ryzykiem ICT Przeprowadzanie regularnych audytów wewnętrznych i przeglądu procesów."

„Powołanie koordynatora wdrażania DORA."

„Prowadzenie Excela z mapowaniem wymagań."

„Zaangażowanie stron biznesowych."

„Wsparcie CIO oraz zewnętrznych ekspertów w razie potrzeby."

Na podstawie odpowiedzi można wyróżnić kilka kluczowych obszarów dobrych praktyk.

1. Centralizacja i formalizacja zarządzania DORA

Jednym z najsilniej akcentowanych wątków jest potrzeba centralizacji procesu DORA, obejmującej zarówno zarządzanie ryzykiem ICT, jak i zarządzanie ryzykiem dostawców ICT. Respondenci wskazują, że rozproszenie odpowiedzialności znacząco utrudnia skuteczne wdrożenie regulacji, natomiast centralny model ułatwia spójność interpretacyjną, ogranicza dublowanie działań, zwiększa kontrolę nad postępem prac. Centralizacja jest często powiązana z powołaniem koordynatora DORA, dedykowanego zespołu lub formalnego projektu o odpowiedniej randze organizacyjnej.

2. Projektowy model wdrożenia i silne umocowanie zarządcze

Respondenci jednoznacznie wskazują, że skuteczne wdrożenie DORA wymaga realizacji w formule projektu, powołania Komitetu Sterującego, bezpośredniego zaangażowania Zarządu i najwyższej kadry kierowniczej. DORA jest postrzegana jako regulacja przekrojowa, wymagająca decyzji strategicznych, priorytetyzacji zasobów oraz rozstrzygnięć na poziomie zarządczym.

3. Analiza luk, mapowanie wymagań i porządkowanie procesów

Dobrą praktyką jest przeprowadzenie analizy luk (gap analysis), mapowanie wymagań DORA na istniejące procesy, systemy i regulacje wewnętrzne oraz dokumentowanie zgodności.

Respondenci podkreślają, że nawet nieskomplikowane narzędzia, jeśli są konsekwentnie stosowane,

35 Jakie dobre praktyki mogliby Państwo zarekomendować przy wdrażaniu DORA?

pozwalają zachować kontrolę nad zakresem regulacji, ułatwić raportowanie i audyty oraz ograniczyć chaos interpretacyjny.

4. Współpraca i zaangażowanie

Wybrzmiewa potrzeba włączenia wielu obszarów organizacji w proces wdrożenia IT, bezpieczeństwa, ryzyka, compliance, jednostek biznesowych.

Respondenci wskazują, że DORA nie może być realizowana wyłącznie przez IT lub compliance. Skuteczność wdrożenia zależy od zrozumienia regulacji przez biznes, wspólnego wypracowania rozwiązań oraz regularnej komunikacji i szkoleń dla pracowników.

5. Standaryzacja relacji z dostawcami ICT

Pojawiającą się dobrą praktyką jest wypracowanie standardowych szablonów umów zgodnych z DORA, prowadzenie jednolitej ewidencji dostawców i usług ICT oraz spójna ocena ryzyka dostawców.

Analiza odpowiedzi otwartych pokazuje, że skuteczne wdrażanie DORA opiera się nie na pojedynczych narzędziach technologicznych. Respondenci rekomendują podejście systemowe, w którym DORA jest traktowana jako program transformacyjny obejmujący całą organizację, proces długofalowy, element strategii zarządzania ryzykiem i odpornością operacyjną. Najbardziej powtarzalne dobre praktyki – centralizacja, silne umocowanie zarządcze, współpraca między działami w banku, standaryzacja relacji z dostawcami oraz mapowanie.

4.7 Potrzeby i oczekiwania

Uzyskane wyniki wskazują, że w procesie wdrażania DORA kluczowe znaczenie dla banków miało i nadal ma wsparcie zewnętrzne, zarówno ze strony organów nadzorczych, jak i dostawców ICT, przy czym zasadniczym problemem nie jest brak zaangażowania tych podmiotów, lecz niewystarczająca klarowność, standaryzacja oraz przewidywalność działań. Banki w największym stopniu oczekują jednoznacznych interpretacji regulacyjnych, usprawnionego dialogu z nadzorem oraz stabilnych i spójnych standardów wdrożeniowych, które pozwoliłyby ograniczyć ryzyko rozbieżnych interpretacji i konieczność kosztownych korekt wdrożeń.

Jednocześnie badanie pokazuje, że skuteczna implementacja DORA wykracza poza relację bank–regulator i obejmuje cały system finansowo-technologiczny, w którym istotną rolę odgrywają dostawcy ICT, standardy umowne, mechanizmy testowania odporności oraz jednolite podejście do raportowania i nadzoru nad usługami zewnętrznymi.

- Banki jednoznacznie wskazują, że największą barierą we wdrażaniu DORA nie jest brak gotowości organizacyjnej ani technologicznej, lecz niedostateczna klarowność interpretacyjna przepisów oraz opóźnienia w publikacji szczegółowych wytycznych.

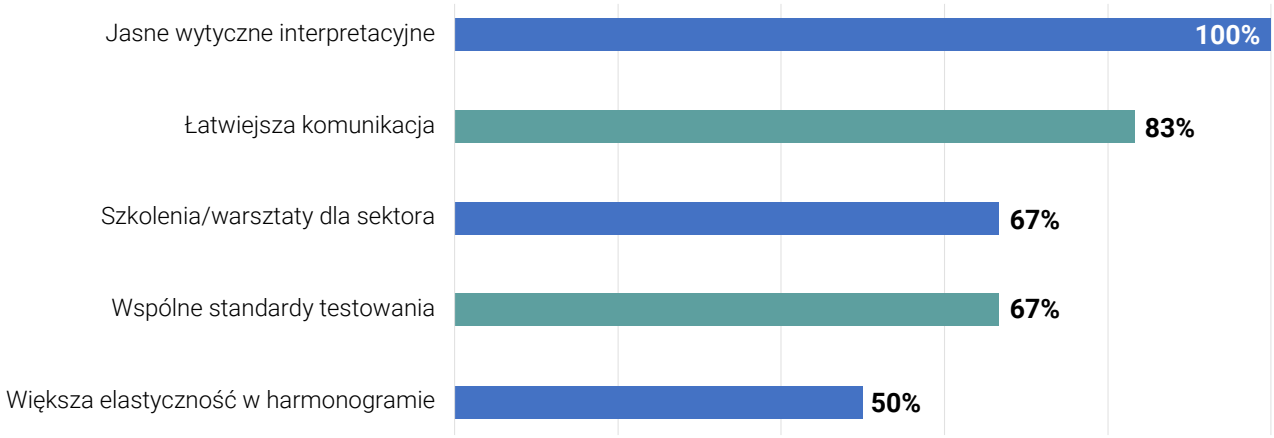
- Wsparcie regulatora jest postrzegane przede wszystkim w kategoriach merytorycznych i komunikacyjnych, a nie formalnych – kluczowe znaczenie mają jasne interpretacje, spójne stanowiska nadzorcze oraz możliwość bieżącego dialogu w trakcie trwania projektów wdrożeniowych.

- Banki oczekują standaryzacji praktyk rynkowych, w szczególności w obszarach testowania odporności operacyjnej, outsourcingu ICT, raportowania incydentów oraz kwalifikacji usług i dostawców, co pozwoliłoby ograniczyć ryzyko fragmentarycznych i niespójnych wdrożeń.

- Współpraca z dostawcami ICT pozostaje jednym z najbardziej wrażliwych elementów wdrożenia DORA, a brak elastyczności kontraktowej i jednolitych wzorców umownych znacząco zwiększa koszty oraz czas dostosowania po stronie banków.

Kluczowym oczekiwaniem banków wobec regulatora jest większa klarowność interpretacyjna przepisów DORA (wykres 4.12). Wszystkie badane instytucje (100% wskazań) uznały, że jasne wytyczne interpretacyjne byłyby najbardziej pomocną formą wsparcia. Wynik ten potwierdza wcześniejsze wnioski z pytań zamkniętych i otwartych, w których dominowały problemy związane z niejednoznacznością regulacji, szerokim polem interpretacyjnym oraz późnym publikowaniem szczegółowych wymagań. Drugim najczęściej wskazywanym obszarem wsparcia jest łatwiejsza i bardziej bezpośrednia komunikacja z regulatorem (83% odpowiedzi). Oczekiwanie to sugeruje potrzebę usprawnienia dialogu nadzorczego, w tym możliwości szybszego uzyskiwania jednoznacznych odpowiedzi na pytania interpretacyjne

Wykres 4.12. Oczekiwane przez banki wsparcie ze strony regulatora.



Pyt. Jakie wsparcie ze strony regulatora byłoby najbardziej pomocne? Można zaznaczyć kilka odpowiedzi.

Źródło: wyniki badań własnych.

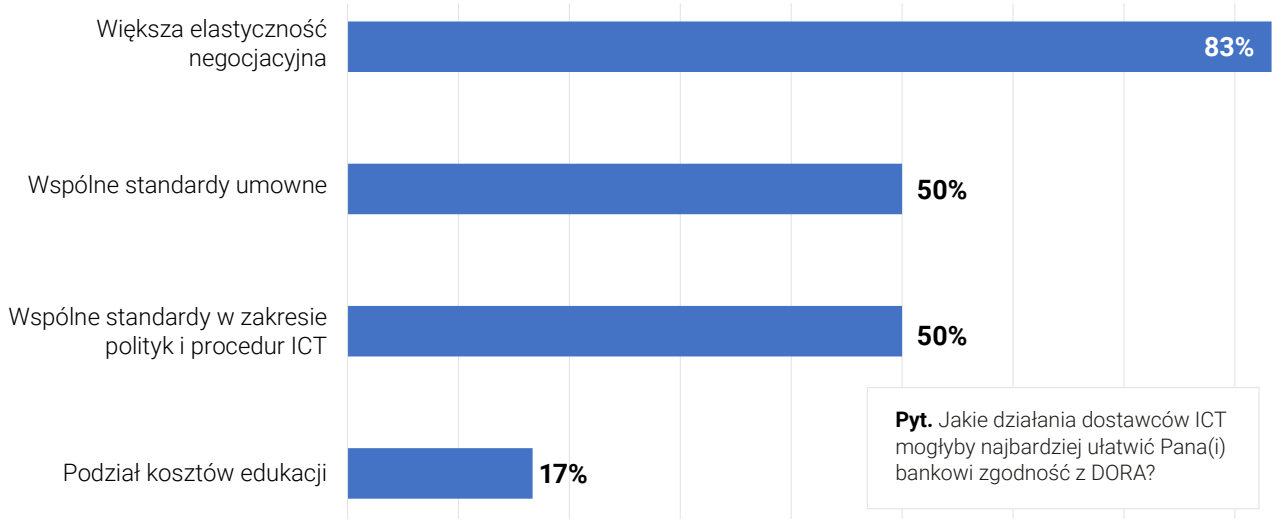
oraz bieżącego wyjaśniania wątpliwości pojawiających się w trakcie wdrażania DORA. Istotne znaczenie respondenci przypisują również działaniom edukacyjnym i standaryzacyjnym. 67% badanych wskazało na potrzebę szkoleń i warsztatów dla sektora, a taki sam odsetek uznał za pomocne wspólne standardy testowania odporności. Oznacza to, że banki nie tylko oczekują wyjaśnienia przepisów, ale również praktycznych, ujednoliconych wzorców ich stosowania, szczególnie w obszarach takich jak testowanie odporności operacyjnej, TLPT czy nadzór nad dostawcami ICT. Połowa badanych (50%) wskazała na potrzebę większej elastyczności w harmonogramie wdrażania wymogów. Wynik ten sugeruje, że tempo implementacji DORA – zwłaszcza w kontekście opóźnień aktów delegowanych i wytycznych – było dla części banków istotnym wyzwaniem organizacyjnym i operacyjnym.

Banki oczekują od regulatora przede wszystkim wsparcia interpretacyjnego i komunikacyjnego, a dopiero w dalszej kolejności zmian o charakterze formalnym lub organizacyjnym. Kluczowym problemem nie jest sama idea DORA, lecz sposób jej operacjonalizacji w warunkach niepełnej informacji, zmiennych interpretacji i presji czasowej.

Z perspektywy wdrażania DORA oznacza to, że największą wartość dla sektora finansowego przyniosłyby jednoznaczne i spójne wytyczne interpretacyjne, ustrukturyzowany dialog z nadzorem, wspólne standardy i dobre praktyki, działania edukacyjne skierowane do całego sektora. Takie podejście mogłoby istotnie ograniczyć ryzyko rozbieżnych interpretacji, zmniejszyć koszty dostosowania oraz przyspieszyć osiągnięcie realnej – a nie wyłącznie formalnej – odporności operacyjnej, która jest głównym celem regulacji DORA.

Odpowiedzi banków jednoznacznie wskazują, że największym wyzwaniem we współpracy banków z dostawcami ICT w kontekście DORA jest obszar negocjacyjno-kontraktowy (wykres 4.13). Zdecydowana większość badanych (83%) uznała, że większa elastyczność negocjacyjna po stronie dostawców ICT byłaby kluczowym czynnikiem ułatwiającym osiągnięcie zgodności z regulacją. Wynik ten potwierdza, że proces renegocjowania umów – szczególnie z dużymi, międzynarodowymi dostawcami usług ICT – stanowi jedno z najbardziej czasochłonnych i problematycznych ogniw wdrożenia DORA. Połowa respondentów (50%) wskazała na potrzebę wspólnych standardów umownych, które mogłyby ograniczyć konieczność indywidualnych negocjacji każdego kontraktu oraz zmniejszyć ryzyko rozbieżnych interpretacji wymagań DORA. Równocześnie taki sam odsetek badanych uznał za istotne wspólne standardy w zakresie polityk i procedur ICT, co sugeruje, że banki oczekują większego ujednolicenia podejścia dostawców do kwestii bezpieczeństwa, raportowania, testowania odporności oraz zarządzania ryzykiem. Znacznie rzadziej wskazywanym obszarem był podział kosztów edukacji (17% odpowiedzi). Może to oznaczać, że choć działania szkoleniowe i edukacyjne są postrzegane jako istotne, to nie stanowią kluczowej bariery w osiąganiu zgodności z DORA, w przeciwieństwie do kwestii formalnych, kontraktowych i proceduralnych.

Wykres 4.13. Działania dostawców ICT najbardziej ułatwiające bankowi zgodność z DORA.



Źródło: wyniki badań własnych.

Rola dostawców ICT w procesie wdrażania DORA jest równie istotna jak działania samych banków. Największe trudności nie wynikają z braku technologii, lecz z asymetrii negocjacyjnej, braku standaryzacji oraz ograniczonej gotowości dostawców do dostosowania się do specyfiki regulacyjnej sektora finansowego. Z perspektywy banków, największą wartość dodaną ze strony dostawców ICT przyniosłyby większa elastyczność w negocjacjach kontraktowych, ujednolicone wzorce umów zgodne z DORA, spójne standardy polityk i procedur ICT oraz gotowość do współodpowiedzialności za zgodność regulacyjną.

W szerszym ujęciu wyniki te sugerują, że osiągnięcie realnej odporności operacyjnej, będącej celem DORA, wymaga systemowego podejścia obejmującego cały system finansowo-technologiczny, a nie wyłącznie działania po stronie instytucji finansowych. Bez aktywnego zaangażowania i adaptacji dostawców ICT, pełna i trwała zgodność z DORA może pozostać kosztowna, czasochłonna i obarczona istotnym ryzykiem operacyjnym.

Analiza odpowiedzi otwartych wskazuje na wyraźną koncentrację problemów nie wokół celów regulacji DORA, lecz wokół jej operacjonalizacji, definicyjnej precyzji oraz stabilności standardów wykonawczych.[36] Wśród spontanicznych opinii, które obszary wymagają dalszych analiz lub standaryzacji w ramach wdrożenia DORA wymieniono następujące.

„Uszczegółowienie dodatkowych wytycznych /przykładów usług ICT, które powinny podlegać kwalifikacji od S01 – S19. Uszczegółowienie definicji usługi ICT by była bardziej klarowna. Podejścia do Body Leasingu i klasyfikacji JDG."

„Testowanie odporności operacyjnej w tym kluczowych dostawców."

„Proporcjonalność środków i wymagań względem skali działania podmiotu."

„Zapewnienie zgodności dużych i międzynarodowych dostawców usług ICT."

„Analiza łańcucha poddostawców. Wdrożenie TIBER-PL. Monitorowanie ryzyka i bezpieczeństwa ICT Zarządzanie kluczowymi dostawcami."

„Jednolite standardy sprawozdawcze, niezmieniane dynamicznie w czasie. Jasne i spójne opisy standardów z definicjami pojęć."

„Poprawa systemy raportowania SDD."

„Lepsza komunikacja z KNF- SLA na odpowiedzi KNF."

36 Jakie obszary wymagają, według Państwa, dalszych analiz lub standaryzacji w ramach wdrożenia DORA?

Wypowiedzi respondentów układają się w kilka spójnych, powtarzalnych obszarów tematycznych.

1. Nieprecyzyjne definicje i zakres kwalifikacji usług ICT

Jednym z najczęściej wskazywanych problemów jest brak wystarczającej jednoznaczności w zakresie definicji usługi ICT, kwalifikacji usług do kategorii S01–S19 oraz podejścia do specyficznych modeli współpracy, takich jak body leasing czy klasyfikacja JDG. Respondenci podkreślają, że niejasności definicyjne prowadzą do rozbieżnych interpretacji pomiędzy bankami, a także do trudności w spójnym raportowaniu i klasyfikacji usług. Brak przykładów referencyjnych oraz jednoznacznych wytycznych powoduje, że instytucje finansowe zmuszone są do tworzenia własnych, często zachowawczych interpretacji, co zwiększa koszty wdrożenia i ryzyko regulacyjne.

2. Testowanie odporności operacyjnej i zasada proporcjonalności

Kolejnym kluczowym obszarem wymagającym dalszej standaryzacji jest testowanie odporności operacyjnej, w szczególności udział kluczowych dostawców ICT w testach, zakres i głębokość testów, proporcjonalność wymagań do skali działalności banku. Respondenci wskazują, że brak jednoznacznych wytycznych dotyczących proporcjonalności prowadzi do nadmiernych obciążeń organizacyjnych, zwłaszcza dla mniejszych instytucji, oraz utrudnia praktyczne wdrożenie testów obejmujących duże, międzynarodowe podmioty technologiczne.

3. Zarządzanie łańcuchem poddostawców i środowisko chmurowe

Wypowiedzi respondentów wskazują na potrzebę dalszych analiz w obszarze identyfikacji i monitorowania poddostawców ICT. Brak spójnych wytycznych w tym zakresie utrudnia bankom pełną ocenę ryzyka oraz integrację wymogów DORA z istniejącymi modelami i architekturą IT.

4. Standardy sprawozdawcze i narzędzia raportowe

Istotnym obszarem krytycznym są również kwestie sprawozdawczości, w tym brak stabilnych, jednolitych standardów raportowych, dynamiczne zmiany wymagań w czasie oraz problemy techniczne systemu raportowania SDD. Respondenci podkreślają, że zmienność standardów oraz błędy narzędzi raportowych znacząco zwiększają ryzyko operacyjne i organizacyjne, utrudniają automatyzację procesów oraz ograniczają możliwość długofalowego planowania.

5. Komunikacja z nadzorem i przewidywalność procesu regulacyjnego

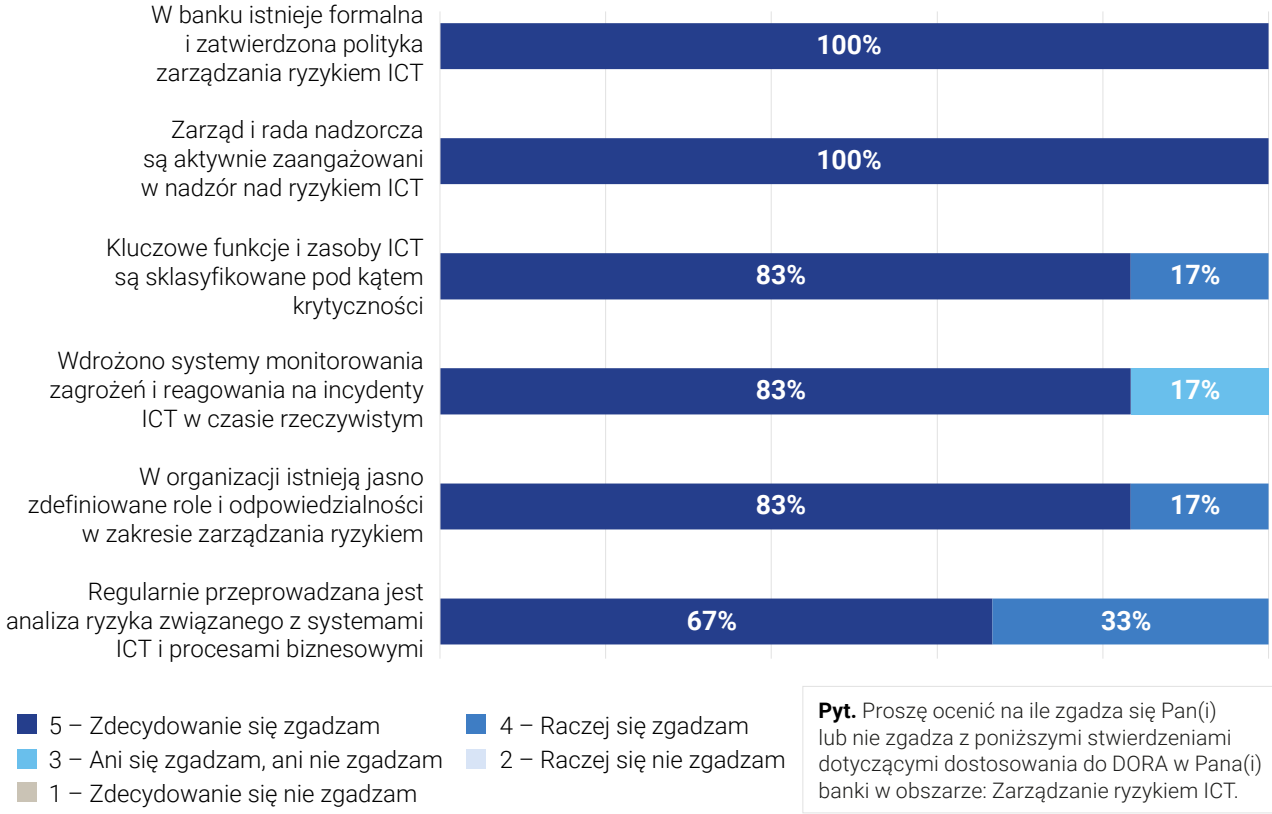
Ostatnim, silnie akcentowanym wątkiem jest potrzeba poprawy komunikacji z organami nadzorczymi, w szczególności poprzez wprowadzenie przewidywalnych zasad odpowiedzi, wcześniejsze publikowanie stabilnych wytycznych, ograniczenie zmian interpretacyjnych na późnych etapach wdrożenia. Respondenci wskazują, że brak przewidywalności komunikacyjnej zwiększa presję czasową i utrudnia skuteczne zarządzanie projektami regulacyjnymi.

Analiza odpowiedzi otwartych pokazuje, że największym wyzwaniem w dalszym wdrażaniu DORA nie są cele regulacji ani gotowość banków, lecz niedostateczna precyzja definicyjna, brak standaryzacji wykonawczej oraz ograniczona stabilność otoczenia regulacyjnego. Banki w dużej mierze osiągnęły zgodność formalną i organizacyjną, jednak pełna odporność cyfrowa jest utrudniona przez niejednoznaczności interpretacyjne, brak spójnych standardów oraz ograniczoną przewidywalność wymagań. W szerszym ujęciu badanie wskazuje, że DORA wchodzi w fazę, w której kluczowe znaczenie ma jakość implementacji, a nie sama deklaratywna zgodność.

4.8 Dostosowanie do DORA w obszarach

Analiza wyników badania dostosowania w poszczególnych obszarach tematycznych do DORA wskazuje, że banki osiągnęły wysoki poziom zgodności regulacyjnej oraz dojrzałości organizacyjnej, przy czym stopień tej dojrzałości jest zróżnicowany w zależności od charakteru danego obszaru. Najbardziej rozwinięte są obszary o ugruntowanych ramach regulacyjnych i operacyjnych, takie jak zarządzanie ryzykiem ICT oraz zgłaszanie i zarządzanie incydentami, gdzie DORA w dużej mierze uporządkowała i sformalizowała istniejące praktyki. Jednocześnie obszary wymagające silnej współpracy z podmiotami zewnętrznymi lub integracji, w szczególności testowanie odporności cyfrowej oraz zarządzanie ryzykiem stron trzecich ujawniają większe zróżnico-

Wykres 4.14. Ocena dostosowania banku do DORA w obszarze: zarządzanie ryzykiem ICT.



Pyt. Proszę ocenić na ile zgadza się Pan(i) lub nie zgadza z poniższymi stwierdzeniami dotyczącymi dostosowania do DORA w Pana(i) banki w obszarze: Zarządzanie ryzykiem ICT.

Źródło: wyniki badań własnych.

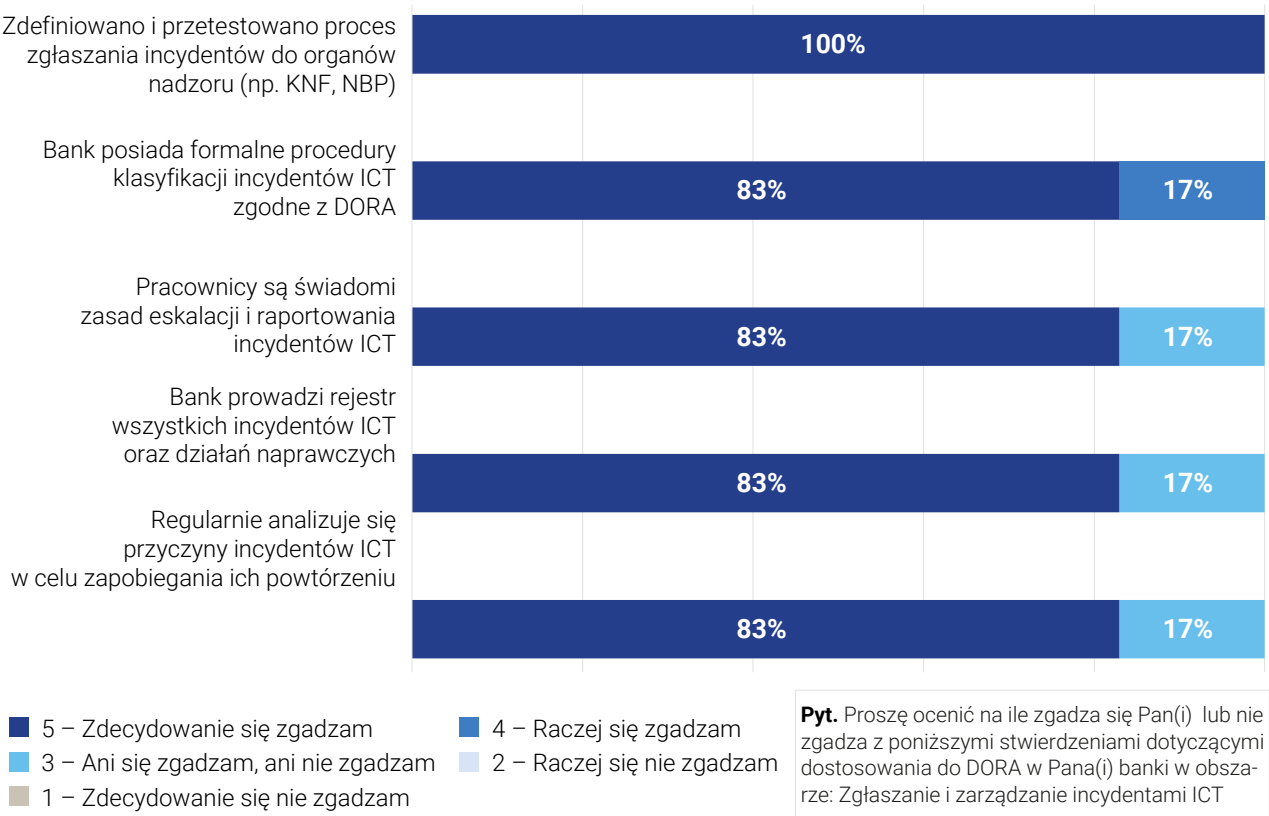
wanie poziomu dojrzałości i pozostają kluczowym polem dalszego rozwoju. Całościowo wyniki potwierdzają, że DORA nie funkcjonuje jako zbiór odrębnych wymogów, lecz jako systemowa regulacja, która testuje zdolność banków do integracji zarządzania ryzykiem ICT, ładu korporacyjnego, procesów operacyjnych oraz współpracy sektorowej.

Badane banki osiągnęły wysoki poziom zgodności strukturalnej i formalnej z wymogami DORA we wszystkich analizowanych obszarach, co potwierdza skuteczne zakorzenienie regulacji w ramach ładu korporacyjnego i systemów zarządzania. Największą dojrzałość wykazują obszary: zarządzania ryzykiem ICT, zgłaszania i zarządzania incydentami ICT, wymiany informacji i współpracy sektorowej, które charakteryzują się wysokim poziomem standaryzacji, jasnym przypisaniem odpowiedzialności oraz gotowością operacyjną. Obszary bardziej złożone organizacyjnie i relacyjnie — w szczególności testowanie odporności cyfrowej, zarządzanie ryzykiem stron trzecich, pozostają w fazie dojrzewania i wymagają dalszej integracji procesowej, standaryzacji oraz wsparcia interpretacyjnego.

Wyniki pokazują wyraźną różnicę pomiędzy zgodnością dokumentacyjną a dojrzałością operacyjną – fundamenty formalne są w dużej mierze zbudowane, natomiast pełna odporność cyfrowa wymaga konsekwentnego testowania, egzekwowania i doskonalenia mechanizmów w praktyce. Wysoki poziom zaangażowania zarządów oraz rosnąca integracja DORA z zarządzaniem ryzykiem operacyjnym potwierdzają, że regulacja ta jest postrzegana jako element strategiczny, a nie wyłącznie obowiązek compliance. Jednocześnie ujawnione ograniczenia zasobowe oraz nierównomierna dojrzałość w niektórych obszarach wskazują, że DORA jest procesem ciągłym, a nie zamkniętym projektem wdrożeniowym, którego skuteczność będzie w kolejnych latach zależna od stabilności zasobów, kompetencji oraz jakości współpracy z interesariuszami zewnętrznymi.

Uzyskane wyniki wskazują na wysoki poziom dojrzałości badanych banków w obszarze zarządzania ryzykiem ICT, szczególnie w zakresie formalnych ram organizacyjnych oraz zaangażowania najwyższego szczebla zarządczego (wykres 4.14). We wszystkich badanych bankach (100% odpowiedzi „zdecy-

Wykres 4.15. Ocena dostosowania banku do DORA w obszarze: Zgłaszanie i zarządzanie incydentami ICT.



Pyt. Proszę ocenić na ile zgadza się Pan(i) lub nie zgadza z poniższymi stwierdzeniami dotyczącymi dostosowania do DORA w Pana(i) banki w obszarze: Zgłaszanie i zarządzanie incydentami ICT

Źródło: wyniki badań własnych.

dowanie się zgadzam") potwierdzono istnienie formalnej, zatwierdzonej polityki zarządzania ryzykiem ICT, a także aktywne zaangażowanie zarządu i rady nadzorczej w nadzór nad tym obszarem. Wynik ten świadczy o tym, że kluczowe wymagania DORA dotyczące odpowiedzialności organów zarządzających zostały w pełni wdrożone i są realnie osadzone w strukturach ładu korporacyjnego banków.

Wysoki poziom zgodności odnotowano również w obszarach operacyjnych i organizacyjnych. 83% respondentów zdecydowanie zgadza się, że kluczowe funkcje i zasoby ICT zostały sklasyfikowane pod kątem krytyczności, wdrożono systemy monitorowania zagrożeń i reagowania na incydenty ICT w czasie rzeczywistym, a w organizacji jasno zdefiniowano role i odpowiedzialności w zakresie zarządzania ryzykiem ICT. Pozostałe 17% odpowiedzi „raczej się zgadzam" w tych obszarach sugeruje, że w części banków procesy te są jeszcze doprecyzowywane lub rozwijane, jednak kierunek zmian jest jednoznacznie zgodny z wymogami DORA. Relatywnie najsłabszym – choć nadal pozytywnie ocenianym – elementem jest regularność i zakres analiz ryzyka ICT powiązanego z systemami oraz procesami biznesowymi. W tym przypadku 67% respondentów zdecydowanie zgadza się, że takie analizy są prowadzone regularnie, natomiast 33% wskazało odpowiedź „raczej się zgadzam". Może to oznaczać, że w części banków analizy ryzyka są realizowane, lecz nie zawsze w pełni zintegrowane z cyklem zarządzania procesami biznesowymi lub nie obejmują jeszcze wszystkich obszarów wymaganych przez DORA.

Wyniki wskazują, że zarządzanie ryzykiem ICT jest jednym z najbardziej dojrzałych obszarów dostosowania do DORA w badanych bankach. Szczególnie silnie rozwinięte są formalne ramy zarządcze i polityki, odpowiedzialność i zaangażowanie zarządu oraz rady nadzorczej oraz podstawowe mechanizmy monitorowania i reagowania na incydenty.

Jednocześnie widoczna jest przestrzeń do dalszego doskonalenia w obszarze ciągłej, pogłębionej analizy ryzyka ICT w powiązaniu z procesami biznesowymi, co jest jednym z kluczowych elementów podejścia DORA, kładącego nacisk na integrację zarządzania ry-

zykiem technologicznym z całym modelem operacyjnym instytucji. Z perspektywy całego badania można stwierdzić, że banki w pierwszej kolejności osiągnęły zgodność strukturalno-formalną, natomiast kolejnym etapem rozwoju będzie pogłębianie jakościowe i operacyjne zarządzania ryzykiem ICT, w tym jego silniejsze powiązanie z testami odporności, zarządzaniem dostawcami ICT oraz ciągłością działania

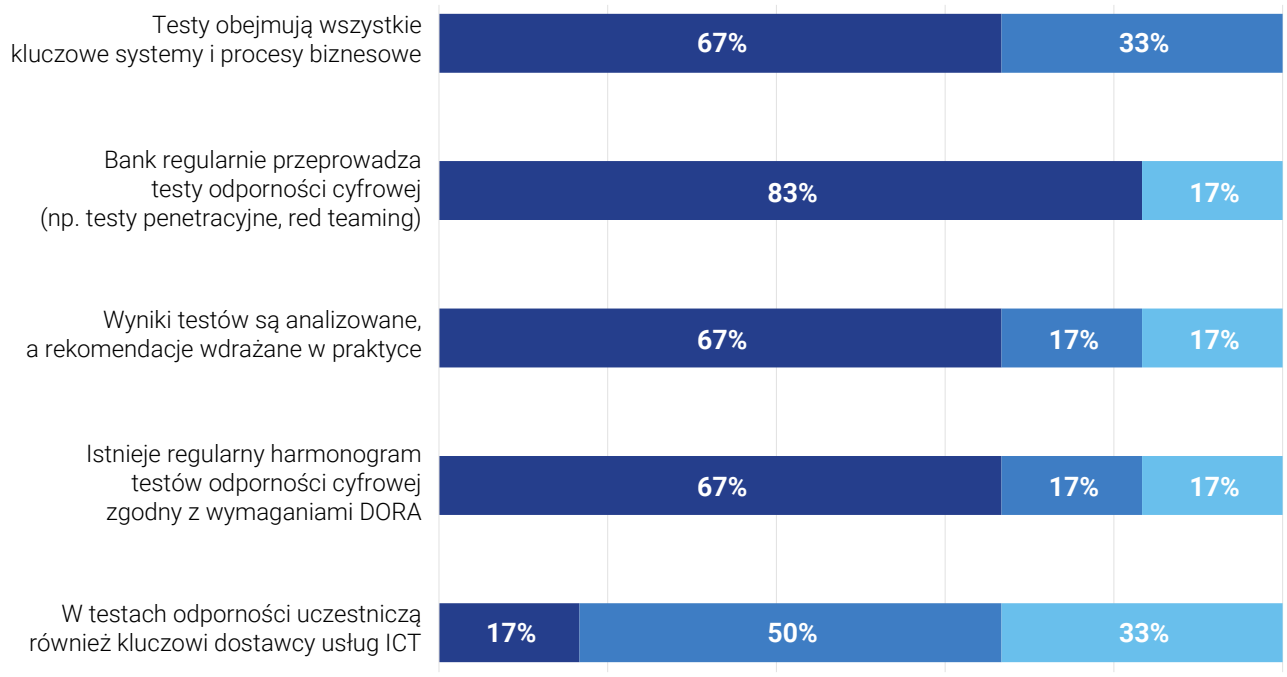
Wyniki badania wskazują na bardzo wysoki poziom przygotowania banków w obszarze zgłaszania i zarządzania incydentami ICT, który – obok zarządzania ryzykiem ICT – należy do najbardziej dojrzałych komponentów wdrożenia DORA (wykres 4.15). We wszystkich badanych bankach (100% odpowiedzi „zdecydowanie się zgadzam") potwierdzono, że proces zgłaszania incydentów do organów nadzoru został zarówno zdefiniowany, jak i przetestowany. Jest to szczególnie istotne z perspektywy DORA, która kładzie silny nacisk nie tylko na formalne posiadanie procedur, ale również na ich praktyczną sprawdzalność i gotowość operacyjną. W pozostałych kluczowych obszarach również odnotowano wysoki poziom zgodności:

- 83% respondentów zdecydowanie zgadza się, że bank posiada formalne procedury klasyfikacji incydentów ICT zgodne z DORA,
- 83% potwierdza wysoką świadomość pracowników w zakresie zasad eskalacji i raportowania incydentów,
- 83% wskazuje na prowadzenie rejestru wszystkich incydentów ICT oraz działań naprawczych,
- 83% deklaruje regularną analizę przyczyn incydentów ICT w celu zapobiegania ich powtórzeniom.

Pozostałe 17% odpowiedzi „ani się zgadzam, ani nie zgadzam" w tych obszarach może sugerować, że w części banków procesy te funkcjonują, jednak nie są jeszcze w pełni ustandaryzowane w całej organizacji.

Analizowany obszar należy ocenić jako jeden z najlepiej zaimplementowanych elementów DORA w badanych bankach. Szczególnie pozytywnie wyróżnia

Wykres 4.16. Ocena dostosowania banku do DORA w obszarze: testowanie odporności cyfrowej.



Pyt. Proszę ocenić na ile zgadza się Pan(i) lub nie zgadza z poniższymi stwierdzeniami dotyczącymi dostosowania do DORA w Pana(i) banki w obszarze: Testowanie odporności cyfrowej.

Źródło: wyniki badań własnych.

się gotowość operacyjna do raportowania incydentów do organów nadzoru, istnienie formalnych procedur klasyfikacji i eskalacji incydentów, wysoki poziom świadomości pracowników, systematyczne podejście do rejestrowania incydentów oraz analiz przyczynowych. W szerszym kontekście badania DORA można stwierdzić, że banki osiągnęły wysoką zgodność regulacyjną w obszarach reaktywnych (incydenty, raportowanie), co tworzy solidną bazę do dalszego rozwoju bardziej zaawansowanych elementów odporności cyfrowej, takich jak testowanie odporności operacyjnej (TLPT) czy zarządzanie ryzykiem dostawców ICT.

Testowanie odporności cyfrowej jest w bankach wdrażane w sposób zaawansowany, lecz nierównomierny, a ten obszar pozostaje bardziej wymagający organizacyjnie i operacyjnie niż zarządzanie ryzykiem ICT czy obsługa incydentów (wykres 4.16). Najwyższy poziom dojrzałości widoczny jest w zakresie regularności prowadzenia testów 83% respondentów zdecydowanie zgadza się, że bank regularnie przeprowadza testy odporności cyfrowej, co potwierdza, że testowanie zostało już osadzone w cyklu zarządczym organizacji, pozostałe 17% deklaruje postawę neutralną, co może wynikać z różnic w zakresie częstotliwości lub formy testów pomiędzy jednostkami.

W odniesieniu do zakresu testów 67% respondentów zdecydowanie zgadza się, że testy obejmują wszystkie kluczowe systemy i procesy biznesowe, 33% wskazuje raczej na zgodność, co sugeruje, że choć zakres testów jest szeroki, w części banków może on być jeszcze rozwijany lub stopniowo rozszerzany.

Podobny obraz wyłania się w obszarze analizy wyników testów i wdrażania rekomendacji 67% badanych zdecydowanie potwierdza, że wyniki testów są analizowane, a rekomendacje wdrażane w praktyce, pozostałe odpowiedzi wskazują na częściową zgodność lub neutralność, co może oznaczać, że proces domykania testów nie zawsze jest jeszcze w pełni sformalizowany.

Również w zakresie posiadania regularnego harmonogramu testów odporności cyfrowej zgodnego z wymaganiami DORA 67% respondentów zdecydowanie się zgadza, 17% raczej się zgadza, 17% pozostaje neutralnych, co może sugerować, że harmonogramy istnieją, ale są nadal dostosowywane do nowych wytycznych lub aktów delegowanych.

Najniższy poziom dojrzałości i jednocześnie największe wyzwanie wdrożeniowe – dotyczy udziału kluczowych dostawców usług ICT w testach odporności. Tylko 17% respondentów zdecydowanie potwierdza udział dostawców ICT, 50% wskazuje na częściową zgodność, aż 33% respondentów zajmuje postawę neutralną, co pokazuje, że w wielu bankach ten element pozostaje jeszcze na etapie koncepcyjnym lub pilotażowym.

Obszar testowania odporności cyfrowej należy uznać za jedno z kluczowych pól dalszego dojrzewania wdrożenia DORA. Banki posiadają już regularne testy i szeroki zakres scenariuszy, coraz częściej analizują wyniki i wdrażają rekomendacje, budują harmonogramy testowe zgodne z wymaganiami regulacyjnymi. Jednocześnie badanie jasno pokazuje, że integracja testów z łańcuchem dostaw ICT pozostaje największym wyzwaniem. Jest to obszar wymagający zarówno standaryzacji podejścia sektorowego, jak i współpracy z dostawcami oraz wsparcia interpretacyjnego regulatora.

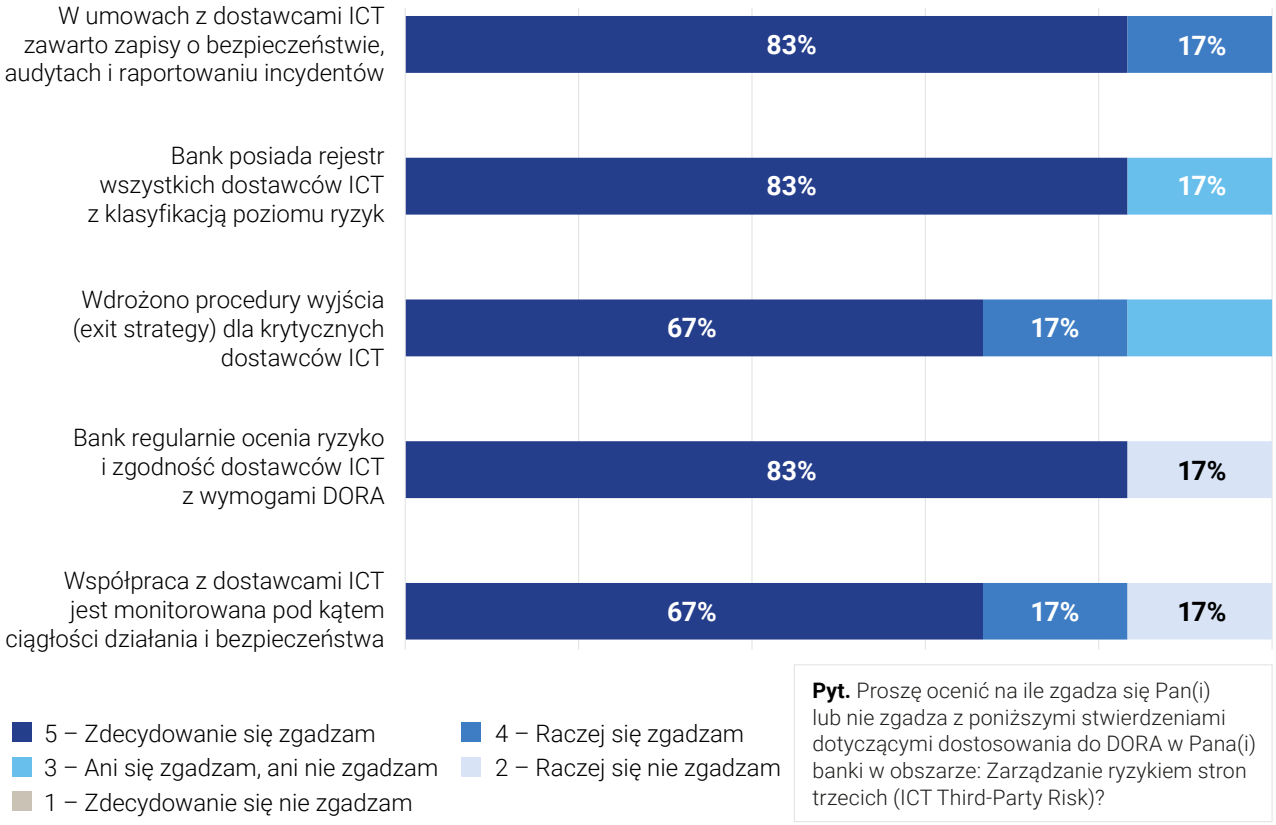
W szerszym kontekście DORA oznacza to, że banki są dobrze przygotowane na testowanie własnej odporności, natomiast pełne przejście do modelu, obejmującego również podmioty trzecie, będzie kolejnym, bardziej złożonym etapem wdrożenia regulacji.

Zarządzanie ryzykiem dostawców ICT jest jednym z bardziej zaawansowanych obszarów wdrożenia DORA, choć – podobnie jak w przypadku testowania odporności cyfrowej – nie wszystkie elementy osiągnęły jeszcze pełną dojrzałość (wykres 4.17). Najwyższy poziom zgodności respondenci deklarują w obszarach formalnych i kontraktowych:

- 83% badanych zdecydowanie zgadza się, że w umowach z dostawcami ICT zawarto zapisy dotyczące bezpieczeństwa, audytów i raportowania zgodnie z wymaganiami DORA,
- 83% respondentów zdecydowanie potwierdza, że bank posiada rejestr wszystkich dostawców ICT wraz z klasyfikacją poziomu ryzyka,
- 83% wskazuje również na regularną ocenę ryzyka i zgodności dostawców ICT z wymogami DORA.

Nieco niższy, choć nadal wysoki, poziom dojrzałości widoczny jest w obszarach operacyjnych, 67% respondentów zdecydowanie zgadza się, że wdrożono procedury wyjścia (exit strategy) dla krytycz-

Wykres 4.17. Ocena dostosowania banku do DORA w obszarze: zarządzanie ryzykiem stron trzecich (ICT Third-Party Risk).



Pyt. Proszę ocenić na ile zgadza się Pan(i) lub nie zgadza z poniższymi stwierdzeniami dotyczącymi dostosowania do DORA w Pana(i) banki w obszarze: Zarządzanie ryzykiem stron trzecich (ICT Third-Party Risk)?

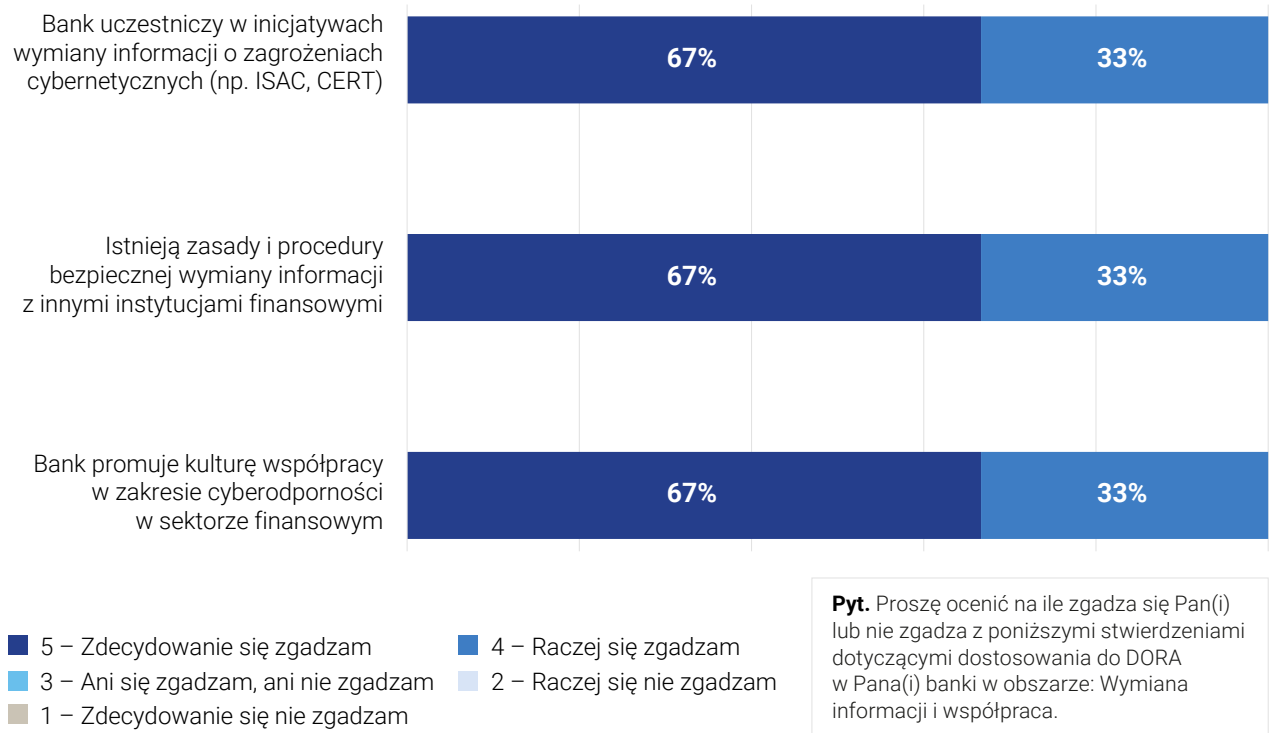
Źródło: wyniki badań własnych.

nych dostawców ICT, kolejne 17% raczej się zgadza, a 17% pozostaje neutralnych, co może oznaczać, że w części banków exit strategy są jeszcze testowane lub wymagają dalszego doprecyzowania. Podobna struktura odpowiedzi dotyczy monitorowania współpracy z dostawcami ICT pod kątem ciągłości działania, gdzie 67% respondentów deklaruje pełną zgodność, a pozostałe odpowiedzi wskazują na częściową implementację lub etap przejściowy.

Zarządzanie ryzykiem stron trzecich w bankach objętych badaniem można ocenić jako obszar relatywnie dojrzały, szczególnie w zakresie formalizacji relacji z dostawcami ICT, inwentaryzacji i klasyfikacji ryzyka oraz cyklicznej oceny zgodności z wymaganiami regulacyjnymi. Jednocześnie wyniki pokazują, że największym wyzwaniem pozostają elementy dynamiczne, wymagające praktycznego testowania procedur wyjścia, bieżącego monitorowania zdolności dostawców do zapewnienia ciągłości działania oraz integracji zarządzania Third-Party Risk z testami odporności cyfrowej oraz planami ciągłości działania banku. W kontekście DORA oznacza to, że banki w dużym stopniu zbudowały fundamenty formalne, natomiast kolejnym etapem będzie przejście od zgodności dokumentacyjnej do pełnej odporności operacyjnej łańcucha dostaw ICT, zwłaszcza wobec dostawców krytycznych i międzynarodowych.

Wyniki badania wskazują na spójny poziom zgodności deklarowanej w całym analizowanym obszarze, bez występowania odpowiedzi neutralnych lub negatywnych. We wszystkich trzech analizowanych stwierdzeniach respondenci potwierdzili zgodność w stopniu pełnym lub bardzo wysokim (wykres 4.18). Po 67% respondentów zdecydowanie zgadza się, że bank uczestniczy w inicjatywach wymiany informacji o zagrożeniach cybernetycznych, takich jak ISAC czy CERT, że w organizacji istnieją formalne zasady i procedury bezpiecznej wymiany informacji z innymi instytucjami finansowymi oraz że bank aktywnie promuje kulturę współpracy w zakresie cyberodporności w sektorze finansowym. Pozostałe 33% respondentów w każdym z przypadków raczej się zgadza, co oznacza, że we wszystkich badanych instytucjach działania w tym obszarze są wdrożone, choć w części banków mogą mieć charakter bardziej selektywny lub rozwijany etapowo.

Wykres 4.18. Ocena dostosowania banku do DORA w obszarze: wymiana informacji i współpraca.



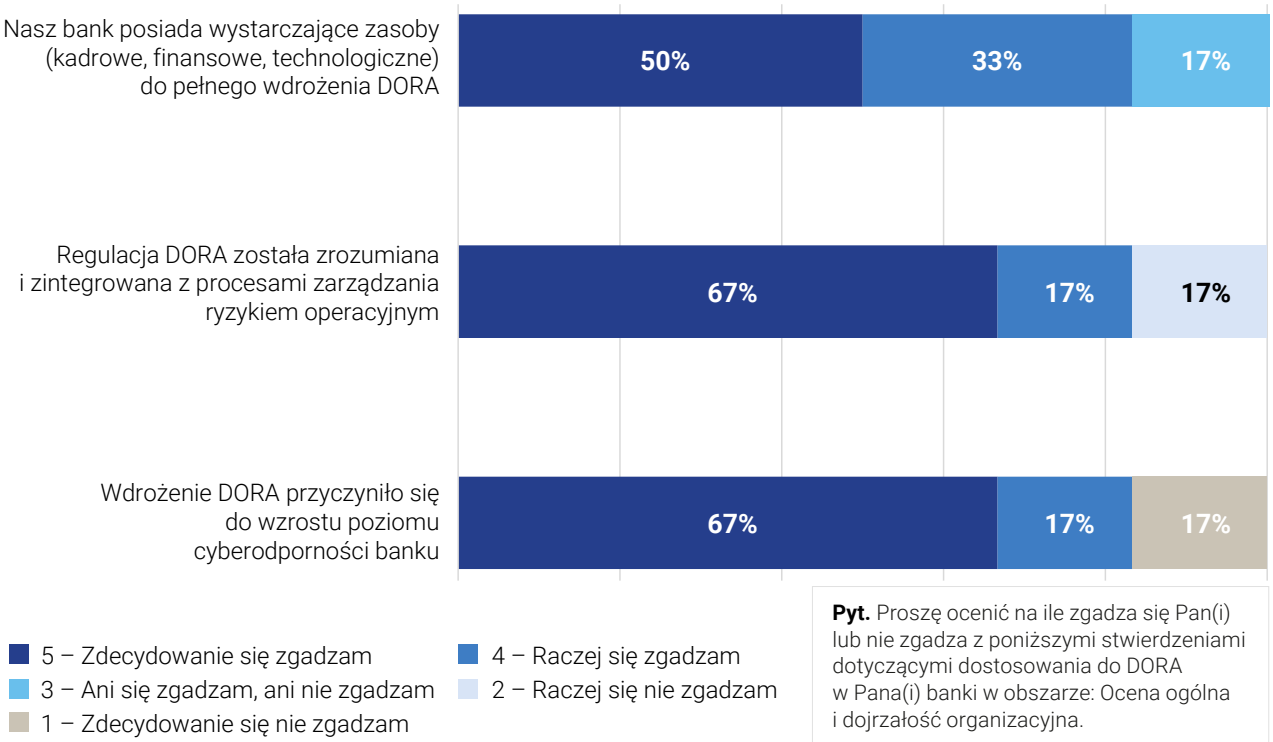
Pyt. Proszę ocenić na ile zgadza się Pan(i) lub nie zgadza z poniższymi stwierdzeniami dotyczącymi dostosowania do DORA w Pana(i) banki w obszarze: Wymiana informacji i współpraca.

Źródło: wyniki badań własnych.

Obszar wymiany informacji i współpracy należy uznać za jeden z jednolicie rozwiniętych elementów dostosowania do DORA w badanych bankach. Brak odpowiedzi neutralnych i negatywnych wskazuje, że znaczenie współdzielenia informacji o zagrożeniach cybernetycznych jest powszechnie rozumiane, a banki postrzegają cyberodporność nie tylko jako kwestię wewnętrzną, lecz również jako element odpowiedzialności sektorowej. Z perspektywy DORA wyniki te są szczególnie istotne, ponieważ regulacja ta wprost zakłada, że odporność cyfrowa sektora finansowego ma charakter systemowy, a nie indywidualny. Aktywne uczestnictwo w inicjatywach wymiany informacji, istnienie bezpiecznych procedur komunikacji oraz promowanie kultury współpracy wzmacniają zdolność sektora do wcześniejszego wykrywania zagrożeń, szybszego reagowania na incydenty oraz ograniczania efektów rozprzestrzeniania się ryzyk operacyjnych pomiędzy instytucjami. Jednocześnie przewaga odpowiedzi „zdecydowanie się zgadzam" sugeruje, że ten obszar może stanowić punkt odniesienia (good practice) dla dalszego rozwoju bardziej złożonych elementów DORA, takich jak testowanie odporności czy zarządzanie ryzykiem dostawców ICT.

Wyniki wskazują na ogólnie pozytywną ocenę wpływu DORA na funkcjonowanie banków, przy jednoczesnym ujawnieniu pewnych ograniczeń zasobowych, które mogą wpływać na tempo i zakres dalszego doskonalenia (wykres 4.19). 67% respondentów zdecydowanie zgadza się, że wdrożenie DORA przyczyniło się do wzrostu poziomu cyberodporności banku, kolejne 17% raczej się zgadza, a 17% zajmuje postawę neutralną. Analogiczny rozkład odpowiedzi dotyczy stwierdzenia, że regulacja DORA została zrozumiana i zintegrowana z procesami zarządzania ryzykiem operacyjnym. Oznacza to, że w większości banków DORA nie funkcjonuje wyłącznie jako odrębny obowiązek regulacyjny, lecz została włączona w istniejące ramy zarządcze. Postawy neutralne mogą jednak wskazywać, że w części organizacji proces integracji nadal trwa lub nie jest jeszcze w pełni ugruntowany we wszystkich jednostkach. Najbardziej zróżnicowane odpowiedzi dotyczą stwierdzenia o wystarczających zasobach do pełnego wdrożenia DORA. 50% respondentów zdecydowanie się zgadza, 33% raczej się zgadza, a 17% zdecydowanie się nie zgadza. Jest to jedyne stwierdzenie w całym zestawie, w którym pojawia się wyraźna odpowiedź negatyw-

Wykres 4.19. Ocena dostosowania banku do DORA w obszarze: ocena ogólna i dojrzałość organizacyjna.



Pyt. Proszę ocenić na ile zgadza się Pan(i) lub nie zgadza z poniższymi stwierdzeniami dotyczącymi dostosowania do DORA w Pana(i) banki w obszarze: Ocena ogólna i dojrzałość organizacyjna.

Źródło: wyniki badań własnych.

na. Wskazuje to, że mimo ogólnej dojrzałości organizacyjnej i postrzeganego pozytywnego wpływu DORA, część banków odczuwa realne ograniczenia kadrowe, finansowe lub technologiczne.

Wyniki potwierdzają, że DORA jest postrzegana jako regulacja wzmacniająca dojrzałość organizacyjną i cyberodporność banków, a nie jedynie jako dodatkowe obciążenie regulacyjne. Wysoki poziom zgody co do poprawy odporności cyfrowej oraz integracji z zarządzaniem ryzykiem świadczy o rosnącej świadomości strategicznego znaczenia odporności operacyjnej oraz skutecznym osadzeniu DORA w strukturach zarządczych banków. Jednocześnie zidentyfikowane ograniczenia zasobowe sugerują, że kolejna faza dojrzałości DORA będzie wymagała nie tylko utrzymania zgodności, lecz także dalszych inwestycji – zwłaszcza w obszarach kompetencyjnych, technologicznych i integracyjnych. Z perspektywy całego badania obszar oceny ogólnej potwierdza wniosek, że DORA działa jako katalizator zmian organizacyjnych, ale pełna stabilizacja i optymalizacja wdrożenia zależy od zdolności banków do trwałego zabezpieczenia odpowiednich zasobów.

5. Kluczowe wyzwania we wdrażaniu DORA

5.1 Integracja z istniejącymi systemami zarządzania ryzykiem ICT

Integracja wymogów rozporządzenia DORA z istniejącymi systemami zarządzania ryzykiem ICT stanowi jedno z najbardziej złożonych i wielowymiarowych wyzwań wdrożeniowych po stronie banków oraz innych instytucji finansowych. Podmioty te od wielu lat rozwijają własne ramy zarządzania ryzykiem technologii informacyjno-komunikacyjnych, często w oparciu o uznane międzynarodowe standardy i dobre praktyki, takie jak ISO/IEC 27001, COBIT, ITIL czy wytyczne Europejskiego Urzędu Nadzoru Bankowego (EBA/GL/2019/04). Rozporządzenie DORA nie zastępuje tych istniejących rozwiązań, lecz nakłada obowiązek ich ujednolicenia, formalizacji oraz ścisłego powiązania z całościowym systemem zarządzania ryzykiem operacyjnym na poziomie całej organizacji.

W praktyce oznacza to konieczność dostosowania dotychczasowych ram zarządzania ryzykiem ICT do jednolitego, spójnego modelu odporności operacyjnej, obejmującego identyfikację, ocenę, monitorowanie oraz ograniczanie ryzyk związanych z wykorzystaniem technologii informacyjnych. Kluczowym elementem tego procesu jest przeprowadzenie kompleksowej analizy luk regulacyjnych (gap analysis), która powinna obejmować zarówno aspekty procesowe, jak i organizacyjne oraz technologiczne. Analiza ta pozwala zidentyfikować obszary niezgodności z wymogami DORA, w szczególności w zakresie zarządzania incydentami ICT, testowania odporności cyfrowej, ciągłości działania oraz nadzoru nad dostawcami zewnętrznymi usług ICT.

Szczególnym wyzwaniem pozostaje zapewnienie spójnej i jednolitej klasyfikacji incydentów ICT, zgodnej z kryteriami określonymi w DORA, a także ustanowienie jasnych zasad ich eskalacji i raportowania do właściwych organów nadzorczych. W wielu bankach procesy te funkcjonowały dotychczas w sposób rozproszony, często w ramach odrębnych struktur IT, bezpieczeństwa informacji lub ryzyka operacyjnego. Taki model utrudnia nie tylko szybkie reagowanie na incydenty, lecz także spełnienie wymogów regulacyjnych dotyczących terminowości, kompletności i jakości raportowania.

Integracja wymogów DORA wymaga również wzmocnienia ładu korporacyjnego w obszarze ICT. Oznacza to konieczność jednoznacznego określenia ról i odpowiedzialności, w tym zwiększonego zaangażowania organów zarządzających w nadzór nad ryzykiem ICT oraz odpornością operacyjną. Zarząd i rada nadzorcza powinny posiadać odpowiedni poziom wiedzy umożliwiający podejmowanie świadomych decyzji w tym zakresie, a także zapewnić, że strategia ICT jest spójna z ogólną strategią zarządzania ryzykiem instytucji.

Dodatkowo skuteczna integracja wymaga ścisłej i trwałej współpracy pomiędzy kluczowymi jednostkami organizacyjnymi, takimi jak IT, bezpieczeństwo informacji, ryzyko operacyjne, compliance oraz audyt wewnętrzny. Brak odpowiedniej koordynacji pomiędzy tymi obszarami może prowadzić do powstawania silosów informacyjnych, niespójności w dokumentacji oraz dublowania działań, co pozostaje w sprzeczności z holistycznym i zintegrowanym podejściem promowanym przez DORA.

W dłuższej perspektywie skuteczna integracja systemów zarządzania ryzykiem ICT z wymogami DORA może jednak przynieść istotne korzyści organizacyjne. Należą do nich zwiększona przejrzystość profilu ryzyka, lepsza jakość danych zarządczych, usprawnienie procesów decyzyjnych oraz realne wzmocnienie odporności operacyjnej banku na zakłócenia technologiczne i cyberzagrożenia. Tym samym DORA, mimo wysokich wymagań wdrożeniowych, może stać się impulsem do dojrzałego i bardziej efektywnego zarządzania ryzykiem ICT w sektorze bankowym.

5.2 Zarządzanie relacjami z dostawcami zewnętrznymi (Third-Party Risk)

Rozporządzenie DORA znacząco rozszerza oraz uszczegóławia obowiązki instytucji finansowych w zakresie zarządzania ryzykiem związanym z dostawcami zewnętrznymi usług ICT. W odróżnieniu od wcześniejszych regulacji, które koncentrowały się głównie na samym procesie outsourcingu, DORA wprowadza kompleksowe podejście do zarządzania ryzykiem stron trzecich (Third-Party Risk Management), obejmujące cały cykl życia relacji z dostawcą – od etapu wyboru, poprzez bieżące monitorowanie, aż po zakończenie współpracy. Banki są zobowiązane do systematycznej identyfikacji, oceny oraz ciągłego nadzoru nad wszystkimi relacjami outsourcingowymi, w tym w szczególności nad usługami chmurowymi, centrami przetwarzania danych oraz dostawcami oprogramowania i infrastruktury uznanych za krytyczne lub istotne.

Jednym z kluczowych wyzwań wdrożeniowych jest skala oraz złożoność relacji zewnętrznych. Duże in-

stytucje finansowe współpracują często z setkami, a nawet tysiącami dostawców, różniących się zakresem świadczonych usług, poziomem krytyczności oraz lokalizacją geograficzną. Wymaga to wdrożenia zaawansowanych mechanizmów klasyfikacji dostawców oraz standaryzowanych metod oceny ryzyka, uwzględniających m.in. wpływ danego dostawcy na ciągłość działania banku, poziom zależności technologicznej, ryzyko koncentracji oraz odporność operacyjną samego dostawcy. DORA kładzie szczególny nacisk na identyfikację tzw. krytycznych lub istotnych funkcji wspieranych przez strony trzecie, co bezpośrednio wpływa na zakres i intensywność nadzoru nad daną relacją outsourcingową.

Istotnym elementem zarządzania ryzykiem stron trzecich jest również zapewnienie odpowiednich zapisów umownych. Rozporządzenie DORA precyzyjnie określa minimalny zakres klauzul, jakie powinny znaleźć się w umowach z dostawcami ICT, w tym m.in. prawo do audytu i inspekcji, obowiązki informacyjne i raportowe, wymogi dotyczące bezpieczeństwa informacji, podwykonawstwa oraz planów ciągłości działania. Szczególne znaczenie mają również tzw. strategie wyjścia (exit strategies), które mają na celu umożliwienie bankowi bezpiecznego i uporządkowanego zakończenia współpracy z dostawcą, bez istotnego zakłócenia działalności operacyjnej lub naruszenia ciągłości świadczenia usług.

W praktyce jednym z największych wyzwań pozostaje renegocjacja istniejących umów outsourcingowych, zawartych przed wejściem w życie DORA. Proces ten bywa długotrwały, kosztowny i obarczony ryzykiem, zwłaszcza w relacjach z globalnymi dostawcami technologii, którzy często stosują wystandaryzowane wzorce umowne i mają ograniczoną elastyczność negocjacyjną. Banki muszą w takich przypadkach znaleźć równowagę pomiędzy spełnieniem restrykcyjnych wymogów regulacyjnych a utrzymaniem stabilnych i długofalowych relacji biznesowych, kluczowych dla funkcjonowania nowoczesnej infrastruktury ICT.

DORA wzmacnia również rolę nadzoru regulacyjnego nad dostawcami krytycznych usług ICT, wprowadzając mechanizmy bezpośredniego nadzoru nad wybranymi podmiotami trzecimi na poziomie Unii Europejskiej. Z perspektywy banków oznacza to konieczność uwzględnienia dodatkowych wymogów informacyjnych oraz ścisłej współpracy z dostawcami w zakresie spełniania oczekiwań organów nadzorczych. W dłuższej perspektywie skuteczne zarządzanie ryzykiem stron trzecich, zgodne z DORA, może przyczynić się do zwiększenia stabilności operacyjnej sektora finansowego oraz ograniczenia ryzyka systemowego wynikającego z nadmiernej koncentracji usług ICT u niewielkiej liczby dostawców.

5.3 Zapewnienie odporności operacyjnej w całym łańcuchu dostaw

Rozporządzenie DORA kładzie szczególny nacisk na zapewnienie odporności operacyjnej nie tylko na poziomie pojedynczych instytucji finansowych, lecz całego ekosystemu finansowego, w którym funkcjonują one w ścisłej zależności od złożonego łańcucha dostaw usług ICT. Oznacza to konieczność systemowego podejścia do identyfikacji, oceny oraz ograniczania ryzyk wynikających zarówno z koncentracji dostawców, jak i z powiązań technologicznych pomiędzy podmiotami sektora finansowego oraz ich kluczowymi partnerami zewnętrznymi. DORA wychodzi tym samym poza tradycyjne, instytucjonalne podejście do zarządzania ryzykiem, promując perspektywę sektorową i makroostrożnościową.

Jednym z najistotniejszych wyzwań w tym obszarze jest identyfikacja punktów krytycznych w łańcuchu dostaw ICT, których awaria mogłaby prowadzić do zakłóceń o charakterze systemowym. Szczególne ryzyko wiąże się z wysokim poziomem koncentracji usług u niewielkiej liczby globalnych dostawców technologii, zwłaszcza w obszarze przetwarzania w chmurze, infrastruktury sieciowej czy specjalistycznego oprogramowania bankowego. Powszechne wykorzystywanie tych samych platform technologicznych przez wiele instytucji finansowych zwiększa prawdopodobieństwo wystąpienia tzw. efektu domina, w którym pojedynczy incydent techniczny lub cyberatak może jednocześnie oddziaływać na znaczną część sektora bankowego.

DORA wymaga od instytucji finansowych systematycznego mapowania zależności technologicznych oraz analizowania potencjalnych scenariuszy zakłóceń, w tym również tych o niskim prawdopodobieństwie, lecz wysokim wpływie. Elementem tego podejścia jest obowiązek regularnego testowania odporności operacyjnej, obejmującego zarówno podstawowe testy ciągłości działania, jak i zaawansowane testy odporności cyfrowej. Szczególne znaczenie mają testy penetracyjne oparte na symulowanych scenariuszach zagrożeń (Threat-Led Penetration Testing – TLPT), które pozwalają na realistyczną ocenę zdolności instytucji do wykrywa-

nia, reagowania i odzyskiwania sprawności po złożonych incydentach cybernetycznych.

Organizacja i przeprowadzenie testów TLPT stanowi istotne wyzwanie operacyjne i organizacyjne. Wymaga bowiem wysokiego poziomu dojrzałości procesów zarządzania bezpieczeństwem, zaangażowania wyspecjalizowanych zespołów oraz ścisłej współpracy z dostawcami zewnętrznymi, którzy często są integralną częścią testowanych środowisk technologicznych. Dodatkowym utrudnieniem mogą być kwestie kontraktowe, ograniczenia prawne oraz obawy dostawców dotyczące bezpieczeństwa własnych systemów. Mimo to DORA jednoznacznie wskazuje, że brak współpracy w tym zakresie nie może stanowić przeszkody w realizacji obowiązków regulacyjnych instytucji finansowych.

Pomimo wysokich kosztów oraz znacznego nakładu zasobów, regularne testowanie odporności operacyjnej w całym łańcuchu dostaw stanowi kluczowy element budowania długoterminowej stabilności sektora finansowego. Pozwala ono nie tylko na identyfikację słabych punktów infrastruktury ICT, lecz także na doskonalenie procedur reagowania kryzysowego, poprawę koordynacji pomiędzy podmiotami oraz zwiększenie świadomości ryzyk na poziomie strategicznym. W efekcie DORA przyczynia się do wzmocnienia odporności operacyjnej banków oraz ograniczenia ryzyka systemowego wynikającego z rosnącej zależności sektora finansowego od zewnętrznych dostawców technologii.

5.4 Wyzwania organizacyjne i kompetencyjne

Jednym z najpoważniejszych ograniczeń skutecznego wdrożenia rozporządzenia DORA są wyzwania o charakterze organizacyjnym i kompetencyjnym. Wymogi regulacyjne w obszarze odporności cyfrowej nakładają na instytucje finansowe obowiązek posiadania wysoko wyspecjalizowanych kompetencji z zakresu cyberbezpieczeństwa, zarządzania ryzykiem ICT, ciągłości działania oraz zgodności regulacyjnej. Tymczasem rynek pracy w tych obszarach charakteryzuje się istotnym deficytem wykwalifikowanych specjalistów, co prowadzi do rosnącej konkurencji o talenty, wzrostu kosztów zatrudnienia oraz zwiększonego ryzyka rotacji kluczowych pracowników.

DORA wymaga zaangażowania znacznie szerszego grona interesariuszy niż dotychczasowe regulacje dotyczące ICT. Odpowiedzialność za odporność cyfrową została jednoznacznie przypisana organom zarządzającym, co oznacza konieczność aktywnego udziału zarządu i rady nadzorczej w nadzorze nad ryzykiem ICT. W praktyce wymusza to podnoszenie kompetencji regulacyjnych i technologicznych na najwyższym szczeblu decyzyjnym, tak aby kadra zarządzająca była w stanie właściwie oceniać ryzyka, podejmować świadome decyzje strategiczne oraz skutecznie nadzorować realizację wymogów DORA. Brak odpowiedniej wiedzy w tym zakresie może prowadzić do nadmiernego polegania na raportach technicznych bez pełnego zrozumienia ich implikacji biznesowych.

Istotnym wyzwaniem organizacyjnym jest również konieczność integracji wymogów DORA z działalnością jednostek biznesowych, które często postrzegają kwestie odporności cyfrowej jako domenę działów IT lub bezpieczeństwa informacji. Tymczasem regulacja ta wymaga, aby zarządzanie ryzykiem ICT było elementem codziennych procesów biznesowych, takich jak rozwój produktów, zarządzanie relacjami z klientami czy współpraca z dostawcami zewnętrznymi. Oznacza to potrzebę redefinicji ról i odpowiedzialności oraz dostosowania struktury organizacyjnej w sposób umożliwiający skuteczną współpracę pomiędzy obszarami technicznymi i biznesowymi.

Brak dojrzałej kultury zarządzania ryzykiem cyfrowym może prowadzić do sytuacji, w której spełnienie wymogów DORA ma charakter wyłącznie formalny, ograniczający się do tworzenia dokumentacji i procedur bez realnego wpływu na praktykę operacyjną. Aby temu zapobiec, kluczowe znaczenie mają systematyczne szkolenia, programy podnoszenia świadomości oraz inicjatywy edukacyjne skierowane do pracowników na wszystkich poziomach organizacji. Szczególną rolę odgrywa tu budowanie świadomości zagrożeń cyfrowych oraz zrozumienie, w jaki sposób codzienne decyzje operacyjne mogą wpływać na poziom odporności całej instytucji.

W dłuższej perspektywie skuteczne zarządzanie wyzwaniami organizacyjnymi i kompetencyjnymi może stać się jednym z kluczowych czynników sukcesu we wdrażaniu DORA. Inwestycje w rozwój kompetencji, wzmocnienie ładu organizacyjnego oraz budowanie kultury odpowiedzialności za odporność cyfrową nie tylko ułatwiają spełnienie wymogów regulacyjnych, lecz także zwiększają zdolność banków do reagowania na dynamicznie zmieniające się zagrożenia technologiczne i cybernetyczne.

5.5 Koszty wdrożenia i ich wpływ na działalność banków

Wdrożenie rozporządzenia DORA wiąże się z istotnymi kosztami finansowymi, które stanowią jedno z kluczowych wyzwań dla sektora bankowego. Koszty te obejmują zarówno nakłady inwestycyjne o charakterze jednorazowym, jak i trwałe koszty operacyjne związane z utrzymaniem zgodności regulacyjnej. Do najważniejszych kategorii wydatków należą modernizacja i rozbudowa infrastruktury ICT, wdrożenie zaawansowanych narzędzi do zarządzania i monitorowania ryzyka ICT, przeprowadzanie regularnych audytów wewnętrznych i zewnętrznych, testów odporności operacyjnej – w tym testów TLPT – a także szeroko zakrojone programy szkoleniowe dla pracowników.

Znaczącą pozycję kosztową stanowią również wydatki związane z zarządzaniem relacjami z dostawcami zewnętrznymi. Renegocjacja umów outsourcingowych, zapewnienie zgodności zapisów kontraktowych z wymogami DORA, a także bieżący nadzór nad dostawcami krytycznych usług ICT generują dodatkowe obciążenia finansowe i organizacyjne. W wielu przypadkach banki zmuszone są do korzystania z usług wyspecjalizowanych doradców prawnych, firm audytorskich oraz podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, co dodatkowo zwiększa całkowity koszt wdrożenia regulacji.

Skala wpływu kosztów wdrożeniowych różni się istotnie w zależności od wielkości i profilu działalności instytucji. Dla dużych banków o rozbudowanej infrastrukturze technologicznej koszty te mogą sięgać milionów euro rocznie, jednak relatywnie łatwiej jest im je absorbować dzięki efektowi skali oraz większym możliwościom inwestycyjnym. Z kolei dla mniejszych banków i instytucji finansowych koszty wdrożenia DORA stanowią znacznie większe obciążenie względne, co może wpływać na ich rentowność oraz zdolność do konkurowania z większymi podmiotami na rynku.

Istnieje również ryzyko, że nadmierne obciążenia regulacyjne mogą ograniczać zdolność banków do innowacji oraz rozwoju nowych produktów i usług cyfrowych. Środki finansowe oraz zasoby organizacyjne, które mogłyby zostać przeznaczone na rozwój technologiczny lub poprawę doświadczenia klienta, są w części kierowane na działania o charakterze stricte regulacyjnym. W krótkim okresie może to prowadzić do spowolnienia tempa transformacji cyfrowej, zwłaszcza w mniejszych instytucjach.

Z drugiej strony inwestycje ponoszone w ramach wdrażania DORA mogą przynieść istotne korzyści długoterminowe. Wzmocnienie odporności operacyjnej, poprawa jakości zarządzania ryzykiem ICT oraz lepsze przygotowanie na incydenty cybernetyczne mogą przyczynić się do zmniejszenia liczby zakłóceń operacyjnych, ograniczenia strat finansowych oraz redukcji kosztów związanych z usuwaniem skutków awarii. Dodatkowo wyższy poziom odporności cyfrowej sprzyja budowaniu zaufania klientów, inwestorów oraz organów nadzorczych, co w dłuższej perspektywie może pozytywnie wpływać na stabilność i reputację banku.

W konsekwencji, mimo znacznych kosztów wdrożenia, DORA może być postrzegana nie tylko jako obciążenie regulacyjne, lecz także jako impuls do modernizacji infrastruktury ICT oraz podniesienia dojrzałości organizacyjnej banków w obszarze zarządzania ryzykiem cyfrowym.

Dyskusji wymaga czy rozwiązania zaproponowane w rozporządzeniu DORA są rzeczywiście niezbędne, szczególnie dla banków spółdzielczych zgodnie z zasadą proporcjonalności zwłaszcza w odniesieniu do polskich instytucji finansowych, których działalność w dużym stopniu ma charakter lokalny a nie transgraniczny, zatem istnieje ryzyko, że poniosą koszty nowych rozwiązań, nie odnosząc korzyści związanych z ich ujednoliceniem na poziomie unijnym.[37]

5.6 Wątpliwości interpretacyjne związane z rozporządzeniem DORA

Pomimo wysokiego poziomu szczegółowości oraz rozbudowanej struktury normatywnej, rozporządzenie DORA pozostawia wiele istotnych kwestii otwartych na interpretację, co stanowi dodatkowe wyzwanie dla instytucji finansowych na etapie wdrażania regulacji. Wątpliwości interpretacyjne dotyczą w szczególności definicji usług krytycznych lub istotnych, zakresu stosowania zasady proporcjonalności, a także odpowiedzialności organów zarządzających za zapewnienie odporności operacyjnej. Nieprecyzyjne granice pomiędzy tymi pojęciami mogą prowadzić do zróżnicowanego podejścia instytucji finansowych, a w konsekwencji do ryzyka rozbieżności w ocenie zgodności regulacyjnej przez organy nadzorcze.

37 P. Pelc, Wpływ planowanych przez UE działań i regulacji na instytucje finansowe w Polsce, Cybersecurity and Law, nr 20/2021

Szczególnym obszarem niepewności jest identyfikacja funkcji i usług uznawanych za krytyczne, których zakłócenie mogłoby mieć istotny wpływ na stabilność operacyjną banku lub całego systemu finansowego. Brak jednoznacznych kryteriów powoduje, że instytucje często przyjmują podejście zachowawcze, kwalifikując szeroki zakres procesów jako krytyczne, co z kolei prowadzi do zwiększenia zakresu obowiązków oraz kosztów wdrożeniowych. Z drugiej strony zbyt wąska interpretacja może skutkować niedostosowaniem się do oczekiwań nadzorczych i potencjalnymi sankcjami regulacyjnymi.

Dodatkowym wyzwaniem jest etapowe publikowanie technicznych standardów regulacyjnych oraz wykonawczych (RTS i ITS), które doprecyzowują wymagania określone w DORA. Proces ten wymaga od banków bieżącego monitorowania zmian regulacyjnych oraz elastycznego dostosowywania już wdrażanych rozwiązań organizacyjnych i technologicznych. W praktyce oznacza to konieczność podejmowania decyzji w warunkach niepełnej jasności regulacyjnej, co zwiększa ryzyko zarówno nadinterpretacji przepisów, prowadzącej do nieproporcjonalnych działań, jak i niedostosowania się do przyszłych oczekiwań nadzorczych.

Wątpliwości interpretacyjne dotyczą również zakresu odpowiedzialności organów zarządzających, w szczególności w kontekście osobistej odpowiedzialności członków zarządu za niedociągnięcia w obszarze odporności cyfrowej. DORA podkreśla rolę najwyższego kierownictwa w nadzorze nad ryzykiem ICT, jednak nie zawsze precyzuje granice pomiędzy odpowiedzialnością strategiczną a operacyjną. Może to prowadzić do ostrożności decyzyjnej, wydłużenia procesów decyzyjnych oraz zwiększonego formalizmu w zarządzaniu ryzykiem.

W praktyce skuteczne zarządzanie ryzykiem interpretacyjnym wymaga aktywnego i proaktywnego podejścia ze strony instytucji finansowych. Kluczowe znaczenie ma ścisła współpraca z organami nadzoru, udział w konsultacjach publicznych dotyczących projektów RTS i ITS oraz bieżące monitorowanie stanowisk i wytycznych publikowanych przez Europejski Urząd Nadzoru Bankowego (EBA) oraz Komisję Nadzoru Finansowego (KNF). Istotnym elementem jest również wymiana doświadczeń w ramach sektora bankowego oraz korzystanie z interpretacji i dobrych praktyk wypracowywanych przez organizacje branżowe.

Podsumowując, wątpliwości interpretacyjne związane z rozporządzeniem DORA stanowią nieodłączny element procesu wdrażania nowej regulacji o tak szerokim zakresie. Odpowiednie zarządzanie tym obszarem, oparte na dialogu z nadzorcą, elastyczności organizacyjnej oraz świadomym podejmowaniu decyzji, może jednak ograniczyć ryzyko regulacyjne i przyczynić się do bardziej efektywnego oraz spójnego wdrożenia wymogów odporności cyfrowej w sektorze bankowym.

PROGRAM ANALITYCZNO BADAWCZY

6. Dobre praktyki we wdrażaniu DORA

6.1. Narzędzia i rozwiązania ICT wspierające zgodność z DORA

Wobec rosnącej liczby obowiązków po stronie adresatów DORA pojawiły się też liczne standardy i narzędzia, które mają pomóc uporać się im z tymi obowiązkami w sposób efektywny.

Związek Banków Polski ze swoim partnerem opracował m.in. Standard DORA stanowiący Rekomendację ZBP dotyczącą wdrażania Rozporządzenia DORA oraz ujednolicenie rynkowych rozwiązań dotyczących relacji dostawców usług ICT z sektorem finansowym w zakresie odporności cyfrowej. Dokumentowi towarzyszą załączniki, zawierające gotowe propozycje dokumentów, możliwych do wdrożenia w wewnętrznych procesach. Sam dokument nie jest dostępny publicznie.

Standard DORA został opracowany także w ramach fundacji FinTech Poland.

Jeżeli chodzi o narzędzia, które mają wspierać w stosowaniu przepisów DORA to na rynku dostępne są głównie rozwiązania wspierające zarządzanie ryzykiem czy też prowadzenie rejestrów umów[38][39]. Ważnym obszarem jest też raportowanie[40], które dla wielu podmiotów może być problematyczne ze względu nie tylko na format i strukturę raportów, ale także sposób ich przekazywania KNF.

Podkreślenia wymaga, że w wielu przypadkach zaangażowanie dostawców tego typu narzędzi będzie wiązało się z koniecznością uwzględnienia kwestii outsourcingu (także bankowego), jak również samej DORA, gdyż będą to zewnętrzni dostawcy usług ICT.

Obserwując rozwój rynku RegTech można przyjąć, że zarówno ilość, jak i jakość dostępnych narzędzi wspierających zgodność z DORA będzie rosła. Wymagać będzie to jednak również po stronie banków podejmowania działań w zakresie „porządkowania" danych (praktyki data governance oraz data management), bowiem przykładowo prawidłowemu wykonaniu obowiązków raportowych wymaga, aby dostarczane dane były wysokiej jakości.

Innymi słowy, sama dostępność narzędzi po stronie zewnętrznych dostawców usług ICT będzie niewystarczająca, jeżeli banki nie zadbają o to jakie dane są dostarczane. Zauważalne jest zwiększanie zdolności (technicznych oraz kompetencji) w zakresie analityki danych po stronie KNF, co oznacza, że zwiększą się też oczekiwania co do wspomnianej jakości danych.

Te kwestie powinny stanowić jeden z priorytetów i celów strategicznych banków, które dzięki temu zapewnią nie tylko zgodność z przepisami oraz oczekiwaniami regulacyjnymi, ale także poprawią swoją efektywność operacyjną.

6.2. Praktyki w zakresie testowania odporności cyfrowej

Jeżeli chodzi o praktyki w zakresie testowania odporności cyfrowej w kontekście DORA to należy wskazać, że jest to obszar rozwojowy, który z pewnością będzie nabierał na znaczeniu. Dzisiaj trudno mówić o standaryzacji w zakresie testowania odporności stricte odnoszącej się do DORA.

Wydaje się jednak, że takiej potrzeby po prostu nie ma. Obszar testowania w kontekście zarządzania systemem bezpieczeństwa informacji jest zasadniczo wystandaryzowany i z powodzeniem może być przenoszony na obszar działalności instytucji finansowych, w tym banków. Tak zresztą dzieje się i dzisiaj.

Należy przy tym zaznaczyć, że rozporządzenie delegowane Komisji (UE) 2025/1190[41] dość szczegółowo określa wymagania w zakresie przeprowadzania chociażby testów penetracyjnych, w tym wymagania stawiane podmiotom, które za nie odpowiadają. W wielu miejscach rozporządzenia znajdziemy odniesienia do standardów rynkowych, które już funkcjonują lub zostaną opracowane w przyszłości. Branża cyberbezpieczeństwa jest dobrze wystandaryzowana, także w zakresie niezbędnych certyfikatów, które posiadać muszą specjaliści w tym obszarze.

38 https://www.1global.com/ (dostęp: 18.01.2026 r.).

39 https://redintogreen.pl/en/solutions/security/ (dostęp: 18.01.2026 r.).

40 https://authoritysoftware.co.uk/authority-suite/dpm-authority/dora/?gad_source=1&gad_campaignid=21951806128&gbraid=0AAAADEQNVicT0Pi9h0LO0hfySpdMQfEN&gclid=Cj0KCQiAprLLBhCMARIsAEDhdPfbrgaUsXbmLL0G_CaC_PuLqjlkT2R6TFJBl5wuRUL22gHT_HC5Vv0aAmEAEALw_wcB (dostęp: 18.01.2026 r.).

41 https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L_202501190 (dostęp: 18.01.2026 r.)

Niemniej jednak można wskazać na pewne dobre praktyki i standardy, które mogą mieć zastosowanie w obszarze DORA. Należą do nich:

- framework TIBER-EU opracowany przez ekspertów Europejskiego Banku Centralnego[42], który określa zasady przeprowadzania testów penetracyjnych,
- standardy ISO, w szczególności 27001, 27002 oraz 22301,
- NIST SP 800-115[43] oraz NIST SP 800-53[44] i 800-53A[45] oraz
- standard PCI Security dla obszaru przede wszystkim płatniczego[46]
- W przypadku niektórych obszarów zastosowanie mogą mieć również inne standardy i dobre praktyki, w szczególności rekomendowane przez specjalistów odpowiedzialnych za przeprowadzanie testów. Te aspekty są również przedmiotem stosownych polityk bezpieczeństwa informacji, jak i towarzyszących im procedur, wytycznych oraz instrukcji.

6.3. Modelowe podejścia do zarządzania ryzykiem ICT

Trudno jednoznacznie wskazać standard zarządzania ryzykiem ICT, który będzie modelowy i do zastosowania zawsze w każdym przypadku. W kontekście DORA punktem wyjścia powinno być rozporządzenie delegowane Komisji (UE) 2024/1774[47], które wskazuje właśnie na taki modelowy system.

Poza tym funkcjonują również standardy uznane za powszechne, jak np. ISO 27005[48] odnoszący się do zarządzania ryzykiem bezpieczeństwa informacji czy COBIT Risk Management[49], a także standard NIST[50]. Opracowując lub modyfikując swoje systemy zarządzania ryzykiem banki muszą uwzględniać też ewentualne wytyczne (w tym wymienione już wytyczne EBA) europejskich i krajowych organów oraz obowiązujące przepisy.

W kontekście tworzenia takich ram niezwykle istotne jest uwzględnienie specyfiki danej organizacji. Nie ma rozwiązań typu „one-size-fits-all", a jedną z kluczowych kwestii jest operacjonalizacja tych rozwiązań, co wymaga budowania świadomości, kompetencji oraz stosowania odpowiednich narzędzi do zarządzania ryzykiem.

42 https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.en.pdf?0309990e5e167a47ca4748370a949064 (dostęp: 18.01.2026 r.).

43 https://www.nist.gov/privacy-framework/nist-sp-800-115 (dostęp: 18.01.2026 r.).

44 https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (dostęp: 18.01.2026 r.).

45 https://csrc.nist.gov/pubs/sp/800/53/a/r5/final (dostęp: 18.01.2026 r.).

46 https://www.pcisecuritystandards.org/standards/ (dostęp: 18.01.2026 r.).

47 https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L_202401774 (dostęp: 18.01.2026 r.).

48 https://www.iso.org/standard/80585.html (dostęp: 18.01.2026 r.).

49 https://www.itsm-docs.com/blogs/cobit/cobit-risk-management (dostęp: 18.01.2026 r.).

50 https://csrc.nist.gov/projects/risk-management (dostęp: 18.01.2026 r.).

7. Wnioski i rekomendacje

Rozporządzenie DORA stanowi istotny punkt zwrotny w podejściu do zarządzania ryzykiem ICT i odpornością operacyjną w sektorze finansowym. Analiza doświadczeń banków komercyjnych w Polsce wskazuje, że skuteczne wdrożenie regulacji wymaga skoordynowanych działań po stronie wszystkich interesariuszy: instytucji finansowych, organów nadzorczych oraz dostawców usług ICT. Poniżej przedstawiono kluczowe wnioski i rekomendacje, pogrupowane według perspektywy poszczególnych uczestników ekosystemu DORA.

7.1 Dla banków: jak skutecznie zarządzać wdrażaniem DORA

Banki powinny postrzegać DORA nie jako jednorazowy projekt compliance, lecz jako **długofalowy proces transformacji zarządzania ryzykiem ICT i odpornością operacyjną**. Kluczowe znaczenie ma trwałe osadzenie wymogów regulacyjnych w strategii instytucji, strukturach ładu korporacyjnego oraz codziennych procesach operacyjnych.

Rekomenduje się, aby banki:

- integrowały zarządzanie ryzykiem ICT z całościowym systemem zarządzania ryzykiem, unikając tworzenia odrębnych, silosowych struktur dedykowanych wyłącznie DORA;
- wzmacniały rolę zarządów i rad nadzorczych w nadzorze nad odpornością cyfrową, w tym poprzez regularne raportowanie ryzyk ICT, wyników testów odporności oraz stanu relacji z kluczowymi dostawcami ICT;
- inwestowały w rozwój kompetencji kadry kierowniczej i specjalistów w obszarze cyberbezpieczeństwa, testowania odporności operacyjnej oraz zarządzania incydentami ICT;
- stosowały podejście oparte na ryzyku i zasadzie proporcjonalności, koncentrując największe zasoby na funkcjach krytycznych lub istotnych oraz usługach ICT o najwyższym znaczeniu dla ciągłości działania;
- standaryzowały procesy zarządzania relacjami z dostawcami ICT, w tym klasyfikację usług, ocenę koncentracji ryzyka oraz podejście kontraktowe, wykorzystując dobre praktyki sektorowe i wzorce umowne.

Skuteczne wdrożenie DORA powinno prowadzić nie tylko do formalnej zgodności regulacyjnej, lecz przede wszystkim do **realnego zwiększenia zdolności banków do zapobiegania zakłóceniom, reagowania na incydenty oraz szybkiego przywracania ciągłości działania**.

7.2 Dla regulatorów: jak wspierać sektor w osiągnięciu zgodności

Doświadczenia banków wskazują, że jednym z kluczowych czynników ryzyka we wdrażaniu DORA była **niepewność interpretacyjna** wynikająca z ogólnego charakteru części przepisów oraz opóźnionego publikowania aktów wykonawczych. Rola regulatorów w tym procesie powinna wykraczać poza egzekwowanie formalnej zgodności. Rekomenduje się, aby organy nadzorcze:

- aktywnie wspierały sektor bankowy poprzez publikację praktycznych wyjaśnień, zestawów pytań i odpowiedzi (Q&A) oraz przykładów dobrych praktyk, zwłaszcza w obszarach takich jak Third-Party Risk, klasyfikacja incydentów ICT i rejestry umów;
- konsekwentnie stosowały zasadę proporcjonalności w praktyce nadzorczej, uwzględniając skalę działalności, profil ryzyka i znaczenie systemowe poszczególnych instytucji;
- prowadziły stały dialog z sektorem finansowym, w tym poprzez konsultacje, warsztaty i inicjatywy edukacyjne, sprzyjające jednolitemu rozumieniu wymogów DORA;
- dążyły do koordynacji podejścia regulacyjnego w obszarach styku DORA z innymi regulacjami (np. NIS2), tak aby ograniczyć ryzyko dublowania obowiązków i nadmiernych obciążeń administracyjnych.

Takie podejście pozwoli regulatorom pełnić rolę nie tylko organów kontrolnych, lecz także **partnerów wspierających budowę odpornego i stabilnego sektora finansowego**.

7.3 Dla dostawców ICT: jak współpracować z bankami w duchu DORA

DORA w sposób istotny zmienia pozycję dostawców ICT w ekosystemie finansowym, czyniąc ich

pośrednimi adresatami wymogów regulacyjnych. Skuteczne wdrożenie regulacji nie jest możliwe bez aktywnego zaangażowania tej grupy interesariuszy. Rekomenduje się, aby dostawcy ICT:

- traktowali wymogi DORA jako nowy standard rynkowy i element długoterminowej strategii, a nie wyłącznie jako koszt narzucony przez klientów z sektora finansowego;
- zwiększali transparentność w obszarze bezpieczeństwa, ciągłości działania, testów odporności oraz zarządzania incydentami, ułatwiając bankom realizację obowiązków regulacyjnych;
- rozwijali kompetencje organizacyjne i prawne umożliwiające sprawne negocjowanie umów zgodnych z DORA, w tym w zakresie audytów, praw dostępu i planów wyjścia (exit strategies);
- budowali partnerskie relacje z bankami, oparte na wspólnym rozumieniu ryzyk i odpowiedzialności za odporność całego łańcucha dostaw ICT.

Dostawcy, którzy będą w stanie efektywnie wspierać banki w realizacji wymogów DORA, mogą uzyskać **trwałą przewagę konkurencyjną** na rynku usług technologicznych dla sektora finansowego.

7.4 Obszary wymagające dalszych analiz i standaryzacji

Analiza doświadczeń wdrożeniowych wskazuje na szereg obszarów, które wymagają dalszych prac analitycznych, doprecyzowania interpretacyjnego lub standaryzacji na poziomie sektorowym i regulacyjnym. Należą do nich w szczególności:

- jednolite podejście do klasyfikacji usług ICT oraz oceny ich krytyczności, w tym relacji między zasadą proporcjonalności a faktycznym ryzykiem systemowym;
- standardy w zakresie testowania odporności operacyjnej, w szczególności częstotliwości, zakresu i metodologii testów TLPT;
- praktyczne modele zarządzania koncentracją ryzyka u dostawców ICT, zwłaszcza w kontekście usług chmurowych;
- relacje i granice pomiędzy obowiązkami wynikającymi z DORA a innymi regulacjami dotyczącymi cyberbezpieczeństwa i odporności operacyjnej;
- rozwój wspólnych narzędzi i benchmarków sektorowych umożliwiających ocenę dojrzałości odporności cyfrowej.

Dalsze prace mogłyby obejmować analizę na większej, reprezentatywnej próbie banków, a także zastosowanie metod pozwalających na bezpośrednią ocenę operacyjnej odporności cyfrowej, w tym testy odporności operacyjnej, audyty ICT aby istotnie przyczynić się do **zwiększenia spójności regulacyjnej, ograniczenia kosztów wdrożeniowych oraz wzmocnienia faktycznej odporności operacyjnej sektora finansowego**.

8. Literatura

1. Basel Committee on Banking Supervision, *Principles for operational resilience*, Bank for International Settlements, Basel, 2021.
2. Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. Working Paper, International Monetary Fund
3. COBIT – zarządzanie ryzykiem ICT, https://www.itsm-docs.com/blogs/cobit/cobit-risk-management, dostęp: 18.01.2026 r.
4. Deloitte, Digital Operational Resilience Act (DORA): Impact and implementation challenges for financial institutions.
5. Dyrektywa (UE) 2022/2555 (NIS2) – wersja PL, https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=pl, dostęp: 18.01.2026 r.
6. Dyrektywa (UE) 2022/2555 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii (NIS 2).
7. Dyrektywa (UE) 2022/2556 – wersja PL (PDF), https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022L2556, dostęp: 18.01.2026 r.
8. Dyrektywa (UE) 2022/2556 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. zmieniająca dyrektywy 2009/65/WE, 2009/138/WE oraz 2011/61/UE w odniesieniu do cyfrowej odporności operacyjnej.
9. ENISA, Threat Landscape for the Financial Sector, European Union Agency for Cybersecurity, Ateny, wydania cykliczne.
10. European Banking Authority, Discussion Paper on the Digital Operational Resilience Act, EBA, 2020.
11. European Banking Authority, Final Report on draft Regulatory Technical Standards under DORA, EBA, 2023–2024.
12. European Banking Authority, Guidelines on ICT and security risk management (EBA/GL/2019/04), EBA, 2019.
13. Guidelines on ICT and security risk management (2019). European Banking Authority.
14. Informacja o DORA – strona EIOPA, https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en, dostęp: 18.01.2026 r.
15. Informacja o zmianach wytycznych dotyczących ryzyka ICT, https://www.eba.europa.eu/publications-and-media/press-releases/eba-amends-its-guidelines-ict-and-security-risk-management-measures-context-dora-application, dostęp: 18.01.2026 r.
16. Informacje nt. zgłaszania incydentów ICT zgodnie z DORA, https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Incydenty_DORA, dostęp: 16.01.2026 r.
17. Informacje ogólne KNF dotyczące DORA, https://www.knf.gov.pl/dla_rynku/dora, dostęp: 12.01.2026 r.
18. ISACA, COBIT® 2019 Framework: Governance and Management Objectives, ISACA, Rolling Meadows, 2019.
19. ISO/IEC, ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection, International Organization for Standardization, Geneva.
20. Komisja Nadzoru Finansowego, Stanowiska i komunikaty dotyczące ryzyka ICT i cyberbezpieczeństwa w sektorze bankowym, KNF, Warszawa.
21. Komunikat dotyczący przetwarzania informacji w chmurze obliczeniowej, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf, dostęp: 12.01.2026 r.
22. Konsultacje nt. zarządzania ryzykiem stron trzecich, https://www.eba.europa.eu/publications-and-media/press-releases/eba-launches-consultation-its-draft-guidelines-third-party-risk-management-regard-non-ict-related, dostęp: 18.01.2026 r.
23. Kopp, E., Kaffenberger, L., Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability. Working Paper, International Monetary Fund.
24. Lachosik, A., DORA jako prawny instrument ochrony cyfrowego bezpieczeństwa rynku finansowego, Studia Prawnoustrojowe, nr 62/2023.
25. Lista kluczowych dostawców usług ICT (CTPPs), https://www.esma.europa.eu/sites/default/files/2025-11/List_of_designated_CTPPs.pdf, dostęp: 13.01.2026 r.
26. NIST Risk Management Framework, https://csrc.nist.gov/projects/risk-management, dostęp: 18.01.2026 r.
27. NIST SP 800-115 – przewodnik po testach bezpieczeństwa, https://www.nist.gov/privacy-framework/nist-sp-800-115, dostęp: 18.01.2026 r.
28. NIST SP 800-53 Rev. 5 – kontrole bezpieczeństwa i prywatności, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final, dostęp: 18.01.2026 r.
29. Norma ISO/IEC 27001:2022, https://www.iso.org/standard/80585.html, dostęp: 18.01.2026 r.
30. Obowiązki sprawozdawcze wynikające z DORA, https://www.knf.gov.pl/dla_rynku/dora/sprawozdawczosc/obowiazki_sprawozdawcze_w_zwiazku_z_rozporzadzeniem_dora, dostęp: 12.01.2026 r.

31. Operational Resilience and Digital Security in Financial Services (2021). OECD Publishing…
32. Pelc P., Wpływ planowanych przez UE działań i regulacji na instytucje finansowe w Polsce, Cybersecurity and Law, nr 20/2021
33. PCI DSS – standardy bezpieczeństwa kart płatniczych, https://www.pcisecuritystandards.org/standards/, dostęp: 18.01.2026 r.
34. Proczka K., Groniewski M., Krajobraz cyberbezpieczeństwa rynku finansowego w Polsce a poziom edukacji fi nansowej – perspektywa organu nadzoru nad rynkiem finansowym oraz jego interesariuszy, Studia Politologiczne, nr 77/2025
35. PwC, Operational resilience and third-party risk management under DORA, raport branżowy.
36. Q&A wspólnego komitetu organów nadzorczych, https://www.eiopa.europa.eu/about/governance-structure/joint-committee/joint-qas_en, dostęp: 18.01.2026 r.
37. Raport roczny CSIRT KNF za 2024 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_Roczny_CSIRT_KNF_2024_93226.pdf, dostęp: 12.01.2026 r.
38. Raportowanie incydentów PSD2 – informacje archiwalne, https://www.knf.gov.pl/dla_rynku/Informacje_dla_podmiotow_nadzorowanych/Sektor_bankowy/raportowanie_incydentow_PSD2, dostęp: 18.01.2026 r.
39. Rozporządzenia delegowane i wykonawcze Komisji uzupełniające rozporządzenie (UE) 2022/2554 w sprawie cyfrowej odporności operacyjnej sektora finansowego (2024–2025). *Dziennik Urzędowy Unii Europejskiej, Unia Europejska*.
40. *Rozporządzenie delegowane Komisji (UE) 2024/1772 – kryteria klasyfikacji incydentów, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1772, dostęp: 14.01.2026 r.*
41. *Rozporządzenie delegowane Komisji (UE) 2024/1774, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774, dostęp: 14.01.2026 r.*
42. *Rozporządzenie delegowane Komisji (UE) 2025/301*, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:L_202500301, dostęp: 16.01.2026 r.
43. Rozporządzenie delegowane Komisji (UE) 2025/302, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:L_202500302, dostęp: 16.01.2026 r.
44. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA) oraz zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) nr 909/2014.
45. Rozporządzenie wykonawcze (UE) 2024/2956 Komisji ustanawiające wykonawcze standardy techniczne dotyczące rejestru informacji na potrzeby stosowania rozporządzenia (UE) 2022/2554.
46. Testy TLPT – nowe podejście nadzorcze, https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/testy_TLPT_nowe_podejscie, dostęp: 16.01.2026 r.
47. Threat Landscape for the Financial Sector (2023). European Union Agency for Cybersecurity (ENISA).
48. TIBER-EU Framework 2025, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.en.pdf, dostęp: 18.01.2026 r.
49. Uchylenie wytycznych dot. raportowania incydentów PSD2, https://www.eba.europa.eu/publications-and-media/press-releases/eba-repeals-guidelines-major-incident-reporting-under-revised-payment-services-directive, dostęp: 18.01.2026 r.
50. Ustawa z dnia 25 czerwca 2025 r. – tekst aktu prawnego, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20250001069, dostęp: 14.01.2026 r.
51. Ustawa z dnia 25 czerwca 2025 r. o zmianie ustaw w związku ze stosowaniem rozporządzenia (UE) 2022/2554 w sprawie cyfrowej odporności operacyjnej sektora finansowego. .
52. Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. z późn. zm.).
53. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z późn. zm.).
54. Wytyczne dot. kosztów i strat w ramach DORA, https://www.eiopa.europa.eu/document/download/f92c9ae0-889f-45ed-89bc-7123012e0417_en, dostęp: 18.01.2026 r.
55. Wymagania rozporządzenia DORA dla podmiotów stosujących uproszczone ramy zarządzania ryzykiem związanym z ICT, KNF, 2025, https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/wymagania_rozporzadzenia_dora_dla_podmiotow_stosujacych_uproszczone_ramy_zarzadzania_zwiazanym_z_ryzykiem_ICT?articleId=91236&p_id=18 (dostęp 3.02.2026)

PROGRAM
ANALITYCZNO
BADAWCZY

Raport opracowany na zlecenie
Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości