

SPEEDNET

Metaanaliza

Koszty AI Governance

Utrzymanie i compliance w bankowości europejskiej

2024–2025

Spis treści

Executive Summary	3
Abstrakt	12
Metodyka	13
Wyniki	14
Wprowadzenie	16
Metodyka (Szczegółowa)	18
Ramy analityczne	21
Wyniki (Szczegółowe)	29
Koszty personelu i nadzoru ludzkiego	29
Dokumentacja i prowadzenie rejestrów	34
Testowanie i walidacja	38
Monitorowanie i bieżące utrzymanie	43
Zarządzanie danymi i infrastruktura technologiczna	48
Audyt i certyfikacja zgodności	53
Dyskusja	58
Wnioski końcowe	66

Executive Summary

Zakres i odbiorcy opracowania

Niniejsze streszczenie menedżerskie stanowi kompleksową syntezę obszernej metaanalizy dotyczącej kosztów zarządzania (governance), utrzymania cyklu życia oraz zapewnienia zgodności (compliance) systemów sztucznej inteligencji w sektorze bankowym Unii Europejskiej. Struktura dokumentu oraz przyjęte standardy dowodowe bezpośrednio opierają się na Wytycznych Tworzenia Metaanaliz, a wszystkie wnioski zostały ściśle przyporządkowane do kategorii zdefiniowanych w Mapie Kosztów Ładu AI (AI Governance Cost Map).

Wspomniane kategorie obejmują następujące obszary:

- Personel i nadzór ludzki (Human Oversight)
- Dokumentacja i prowadzenie rejestrów
- Testowanie i walidacja
- Monitorowanie i bieżące utrzymanie
- Zarządzanie danymi oraz dostrajanie (Fine-Tuning) i Infrastruktura
- Audyt i certyfikacja

Dowody ograniczają się wyłącznie do wiarygodnych źródeł akademickich, raportów wiodących firm doradczych oraz syntezy wynikającej z samej metaanalizy projektu.

Wnioski dla banków w UE

Roczny koszt operacyjny (run-rate) modelu wysokiego ryzyka

Z przeprowadzonej metaanalizy płynie kluczowy wniosek: roczny koszt utrzymania pojedynczego modelu w fazie stabilizacji (steady state) mieści się w przedziale **116–137 tys. euro.** Wynik ten oparto na weryfikacji krzyżowej (triangulacji) wymogów regulacyjnych UE oraz benchmarków rynkowych.

Zasady szacowania kosztów dla zbioru modeli

W procesie planowania strategicznego bankom zaleca się przyjęcie następującego przelicznika:

- **Gdy w grę wchodzi utrzymanie 10 modeli wysokiego ryzyka:** roczne wydatki operacyjne (OPEX) na nadzór (governance) wyniosą w przybliżeniu **1,16–1,37 mln euro.**
- **Wraz ze wzrostem skali do 20 modeli:** koszt ten rośnie proporcjonalnie do poziomu **≈ 2,32–2,74 mln euro.**

Szacunek ten wynika z przemnożenia kosztów jednostkowych przez liczebność modeli w danej puli.

Ścieżki oceny zgodności (Conformity Assessment)

Wyróżnić można dwie główne metody oceny zgodności, różniące się zasadniczo strukturą kosztów:

Ocena zewnętrzna (strona trzecia):

Wiąże się z wydatkiem rzędu **~16,8–23 tys. euro na model** (opłata jednorazowa, ponoszona przy każdej głównej aktualizacji systemu).

Wewnętrzny system QMS (Zarządzanie Jakością):

Wymaga jednorazowej inwestycji wdrożeniowej na poziomie **193–330 tys. euro** oraz rocznego utrzymania w kwocie ok. **~71,4 tys. euro** (koszt ten rozkłada się na wszystkie obsługiwane modele).

Kontekst budżetowy

Wiele organizacji planuje alokować **co najmniej 10% całkowitego budżetu przeznaczonego na AI** na działania związane z ładem korporacyjnym i compliance. Jest to strategia w pełni spójna z obserwowanym w sektorze bankowym sześciocyfrowym rocznym kosztem utrzymania (run-rate) w przeliczeniu na model.

Stawka regulacyjna

Unijny akt w sprawie sztucznej inteligencji (AI Act) nakłada rygorystyczne obowiązki w zakresie jakości danych, dokumentacji i prowadzenia rejestrów, a także przejrzystości, nadzoru ludzkiego oraz odporności i cyberbezpieczeństwa systemów. Brak zgodności niesie ze sobą realne ryzyko nałożenia dotkliwych kar administracyjnych.

Struktura kosztów (zmapowana do Mapy Kosztów Ładu AI)

Personel i nadzór ludzki (Personnel & Human Oversight)

Kategoria ta obejmuje pełną obsadę ról związanych z governance w ramach modelu trzech linii obrony (1LoD/2LoD/3LoD), angażuje walidatorów modeli, doradców prawnych i ds. etyki, a także uwzględnia przeglądy decyzji AI z udziałem człowieka (human-in-the-loop). Jest to zazwyczaj największy pojedynczy składnik kosztowy w całym zestawieniu.

Dokumentacja i prowadzenie rejestrów

Koszty w tym obszarze wiążą się z tworzeniem plików technicznych, przeprowadzaniem analiz ryzyka, opracowywaniem informacji dla użytkowników, a także utrzymywaniem gotowych do audytu logów i wersjonowania przez cały cykl życia systemu. Elementy te muszą być bezwzględnie aktualizowane po każdej istotnej zmianie w modelu.

Testowanie i walidacja (QA)

Obszar ten obejmuje testy odporności i dokładności, weryfikację pod kątem obciążeń (bias) i sprawiedliwości (fairness), cyberbezpieczeństwo i testy kontradyktoryjne (adversarial testing) oraz niezależną walidację przed wdrożeniem produkcyjnym (go-live) i po wprowadzonych zmianach.

Monitorowanie i bieżące utrzymanie

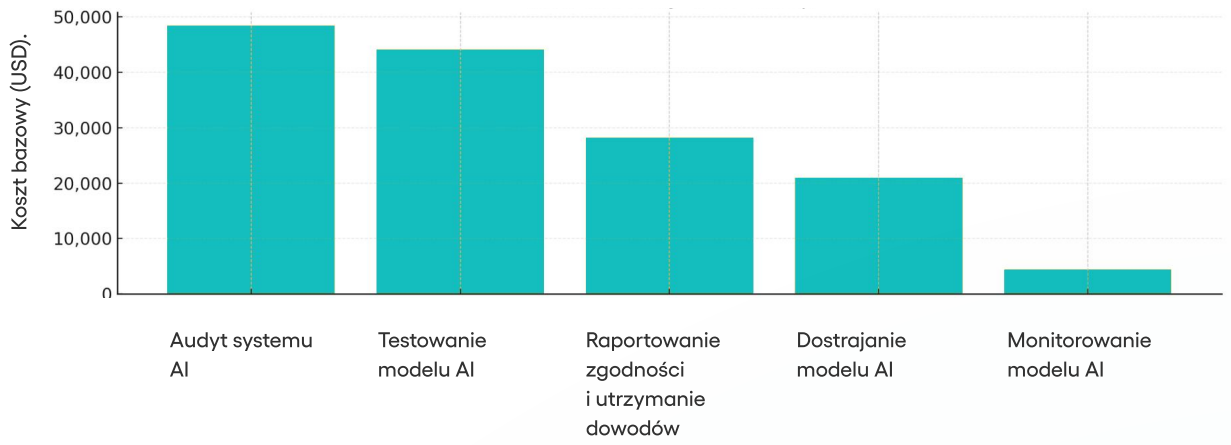
Są to wydatki związane z monitorowaniem systemów po wprowadzeniu na rynek (post-market monitoring), obsługą przepływów pracy w ramach nadzoru ludzkiego, zarządzaniem incydentami, wyzwalaczami ponownego trenowania (retraining triggers) oraz okresową rewalidacją wraz z towarzyszącymi obowiązkami sprawozdawczymi.

Zarządzanie danymi i dostrajanie / Infrastruktura

Obejmuje szeroko pojęty ład danych, w tym ich jakość, reprezentatywność i rodowód (lineage), a także retencję i logowanie, inwentaryzację modeli oraz automatyzację dokumentacji, platformy monitorujące i bezpieczne potoki danych (pipelines).

Audyt zgodności i certyfikacja (Compliance Auditing & Certification)

Koszty te są bezpośrednio powiązane z zewnętrznymi ocenami zgodności lub ocenami opartymi na wewnętrznym systemie QMS, audytami nadzoru, aktualizacjami rejestrów oraz integracją z wewnętrznymi cyklami audytowymi banku.



Rysunek ES-1 — Roczny koszt zarządzania i utrzymania (governance & maintenance) w przeliczeniu na model według grup kosztów (poziom bazowy). Wartość bazowa podana w USD; odpowiada przedziałom w EUR omawianym w tekście.

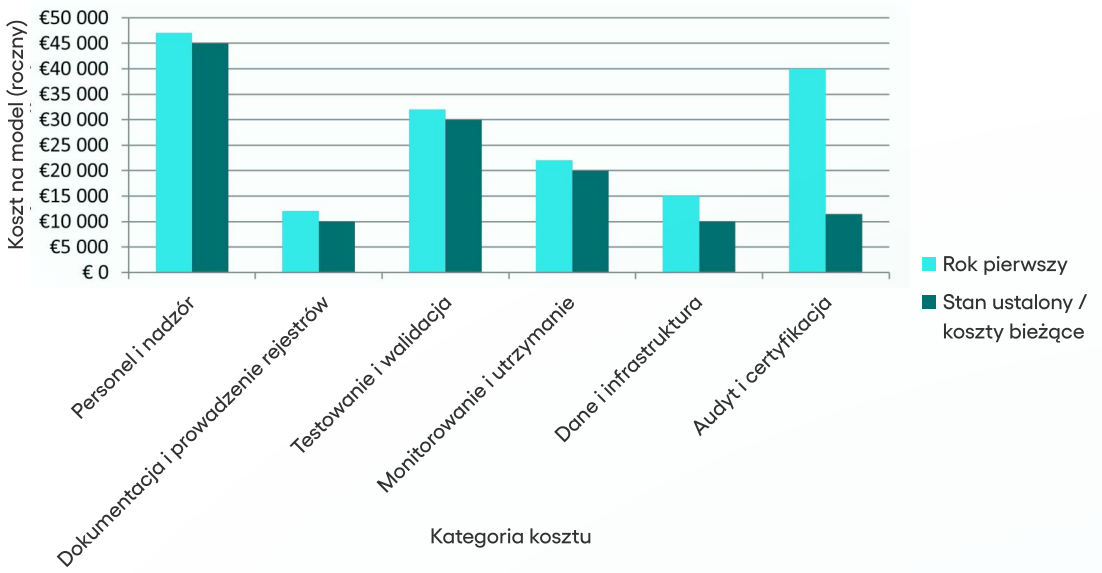
Przyczyny zróżnicowania szacunków (jak interpretować zakres)

Efekt skali

Koszty stałe, takie jak wdrożenie QMS i platformy technologiczne, maleją w przeliczeniu na model w przypadku większych portfeli. Koszty jednostkowe (per model) plasują się w dolnej granicy dla banków o charakterze uniwersalnym, natomiast w górnej granicy dla banków posiadających zaledwie kilka modeli wysokiego ryzyka.

Punkt wyjścia

Banki dysponujące dojrzałymi systemami zarządzania ryzykiem modelu (standard Bazylei) mogą z powodzeniem zaadaptować funkcjonujące już procesy governance. Zdecydowanie wyższe koszty w pierwszym roku generuje natomiast budowanie zgodności od podstaw (podejście greenfield compliance).



Rysunek ES-2 — Wzrost nakładów w pierwszym roku (konfiguracja/QMS i narzędzia) w porównaniu do ustabilizowanego tempa operacyjnego (run-rate) w przeliczeniu na model.

Wybory dotyczące zakresu

Rozwiązania typu „minimum viable" są tańsze, ale rodzą ryzyko związane z zastrzeniami ze strony autyrorów. Programy kompleksowe wymagają wyższych nakładów – obejmujące automatyzację analizy biasu czy gęstsze próbkowanie – w zamian jednak skutecznie mitygują ryzyko rezydualne.

Zakres regulacyjny

Jako systemy wysokiego ryzyka zakwalifikowana zostanie tylko niewielka część rozwiązań AI. Dlatego planując budżet dla wszystkich modeli, należy wziąć pod uwagę rzeczywisty zakres zastosowań krytycznych

Rekomendacje dla CFO: Planowanie w fazie stabilizacji (steady state)

OPEX na model

W tym przypadku trzeba się liczyć z rocznym kosztem rzędu **116–137 tys. euro**, pokrywającym zarówno nadzór (governance), jak i utrzymanie cyklu życia.

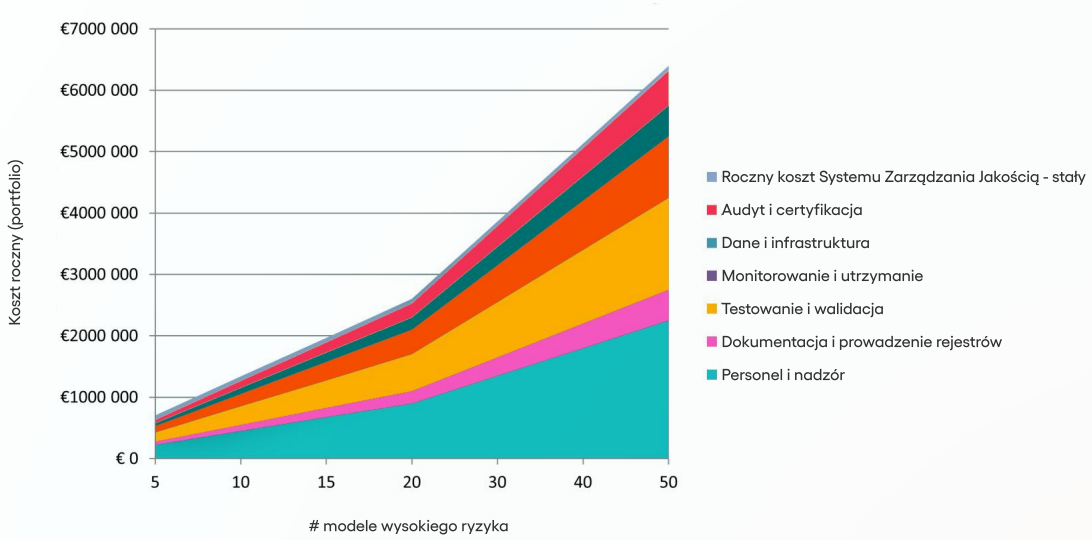
Ocena zgodności

Jednorazowy audyt zewnętrzny to wydatek rzędu **16,8–23 tys. euro za model**. Alternatywą jest wewnętrzny system QMS – tu bariera wejścia wynosi **193–330 tys. euro** (wdrożenie), a roczne utrzymanie pochłania ok. **71,4 tys. euro** (koszt ten ulega amortyzacji).

Alokacja środków

W praktyce na działania z zakresu governance i compliance rezerwować należy co najmniej **10% całkowitego budżetu AI**.

Wielkość portfela (Liczba modeli wysokiego ryzyka)	Roczny OPEX na Governance (niski–wysoki)	Uwagi
10	1,16 mln € – 1,37 mln €	Dolicz koszt utrzymania QMS (~71,4 tys. €/rok), jeśli dotyczy
20	2,32 mln € – 2,74 mln €	Utrzymanie QMS amortyzuje się do poziomu ~3,6 tys. €/model/rok przy 20 modelach



Rysunek ES-3 — OPEX portfela a liczba modeli wysokiego ryzyka; amortyzacja kosztów stałych wraz ze wzrostem portfela.

Plan na najbliższe 6–12 miesięcy: kontrola kosztów i bezpieczeństwo regulacyjne

Inwentaryzacja i stratyfikacja ryzyka (Risk Tiering)

Aby precyzyjnie wyznaczyć obszary wysokiego ryzyka, niezbędne jest stworzenie kompletnego, ogólnobankowego rejestru modeli oraz wdrożenie klasyfikacji zgodnej z wymogami AI Act.

Strategia certyfikacji

Konieczne jest wybranie optymalnej ścieżki weryfikacji – poprzez zewnętrznego audytora bądź w ramach wewnętrznego QMS – oraz zdefiniowanie zasad amortyzacji kosztów dla wszystkich modeli.

Uszczelnienie dokumentacji (Hardening)

Standardy dokumentowania i logowania – obejmujące szablony, pakiety dowodowe, retencję oraz wersjonowanie – muszą zostać wzmocnione tak, by systemy były z definicji gotowe na audyt (audit-ready).

Industrializacja testowania

Konieczne jest uprzemysłowienie procesów testowania i walidacji, w tym wdrożenie zautomatyzowanych zestawów testów na bias i odporność, niezależnej walidacji oraz retestów wyzwalanych zmianami.

Operacjonalizacja monitoringu

Należy wdrożyć monitoring porynkowy (post-market) poprzez wskaźniki KPI, wykrywanie dryfu, plany próbkowania dla nadzoru ludzkiego oraz podręczniki zarządzania incydentami.

Szkolenia i ponowne wykorzystanie procesów

Wymagane jest przeszkolenie trzech linii obrony w zakresie obowiązków specyficznych dla AI oraz ponowne wykorzystanie istniejących procesów zarządzania ryzykiem modelu i ochrony danych w celu uniknięcia duplikacji działań.

Wskaźniki, które powinien śledzić Zarząd

Pokrycie i kondycja procesów

Procent modeli AI z przypisanym poziomem ryzyka, przydzielonymi kontrolami nadzoru, kompletnymi plikami technicznymi i aktywnymi pulpitami monitorującymi; czas do uzyskania certyfikacji.

Jakość i sprawiedliwość (Fairness)

Wskaźniki zaliczenia walidacji, metryki biasu w granicach ustalonych progów, wskaźniki MTTD/MTTR dla dryfu (średni czas wykrycia/rozwiązania).

Wyniki zapewnienia jakości (Assurance)

Liczba ustaleń audytowych na model i czas ich zamknięcia; zewnętrzne niezgodności.

Dyscyplina kosztowa

Bieżący OPEX na model (run-rate), amortyzacja platformy na model oraz procent budżetu AI przeznaczony na governance w stosunku do wydatków na rozwój.

Kategoria kosztów	Przyjęcie przypadku użycia	Projektowanie (Design)	Budowa (Build)	Walidacja	Wdrożenie (Deploy)	Po wdrożeniu (Post-market)
Personel i Nadzór	2	2	2	2	2	3
Dokumentacja i Rejestry	1	2	2	3	2	2
Testowanie i Walidacja	1	1	2	3	2	2
Monitoring i Utrzymanie	1	1	1	2	2	3
Dane i Infrastruktura	2	2	2	2	2	2
Audyt i Certyfikacja	0	0	0	2	2	2

Rysunek ES-4 — Heatmapa pokrycia cyklu życia (intensywność 0–3 w podziale na etapy cyklu życia i kategorie kosztów).

Kategoria Kosztów	1LoD	2LoD	3LoD	Prawne	Bezpieczeństwo IT
Personel i Nadzór	40%	30%	10%	10%	10%
Dokumentacja i Rejestry	15%	30%	5%	30%	20%
Testowanie i Walidacja	10%	10%	40%	5%	35%
Monitoring i Utrzymanie	30%	20%	10%	10%	30%
Dane i Infrastruktura	20%	15%	5%	10%	50%
Audyt i Certyfikacja	5%	15%	50%	20%	10%

Rysunek ES5 — Heatmapa: kategoria kosztów a interesariusze.

Jakość materiału dowodowego i zastrzeżenia

Wskaźnik run-rate na poziomie 116 tys. – 137 tys. euro jest syntezą opracowaną w ramach metaanalizy na podstawie kosztów składowych zawartych w materiałach regulacyjnych UE oraz dowodów dotyczących udziału w budżecie pochodzących z badań firm doradczych. Reprezentuje on roczne koszty w fazie stabilizacji (steady state) dla modeli AI wysokiego ryzyka, przy uwzględnieniu wszystkich głównych składników kosztowych (personel, dokumentacja, testowanie, monitorowanie, dane/infrastruktura, audyt/certyfikacja). Należy wyraźnie podkreślić, że koszty w pierwszym roku mogą być wyższe w przypadkach, gdy banki muszą ustanowić nowe ramy działania, platformy lub zdolności w zakresie QMS.

Wniosek strategiczny

Dla banków w UE zarządzanie sztuczną inteligencją (governance) oznacza sześciocyfrowy roczny wydatek operacyjny (OPEX) na każdy model wysokiego ryzyka – jest to cena zaufania, bezpieczeństwa i regulacyjnej przepustki do skalowania. Ład korporacyjny należy traktować jako kluczową infrastrukturę dla AI działającej w dużej skali, a nie jako dodatek wdrażany po fakcie (afterthought). Decyzje na poziomie portfela (amortyzacja QMS, ponowne wykorzystanie procesów oraz selektywna automatyzacja) mogą utrzymać wskaźnik run-rate w dolnej granicy szacowanego zakresu, nie obniżając przy tym poziomu zapewnienia jakości.

Abstrakt

Europejskie banki stoją w obliczu konieczności ponoszenia znacznych, bieżących kosztów związanych z zarządzaniem (governance) i utrzymaniem systemów sztucznej inteligencji wysokiego ryzyka, co wynika z nowo wprowadzanych regulacji prawnych.

Niniejsza metaanaliza dokonuje syntezy danych pochodzących z ocen skutków regulacji UE oraz wiodących raportów firm doradczych, w celu oszacowania rocznego kosztu zgodności (compliance) przypadającego na pojedynczy model AI w sektorze bankowym Unii Europejskiej.

Tło

Wcześniejsze badania wskazywały na istnienie wielu kategorii kosztowych – począwszy od personelu i nadzoru, poprzez dokumentację, testowanie, monitorowanie, infrastrukturę danych, aż po audyt i certyfikację – uznając je za kluczowe czynniki kosztotwórcze (key cost drivers).

Metodyka

Zakres przeglądu

W ramach niniejszego opracowania dokonaliśmy przeglądu **ponad 20 źródeł,** w tym badań Komisji Europejskiej dotyczącego wpływu Aktu o AI, analiz przeprowadzonych przez ośrodek CEPS, a także raportów firm takich jak Accenture, Deloitte, EY, KPMG, McKinsey oraz branżowych studiów przypadków (np. CostPerform, Ethos.ai). Do analizy zakwalifikowano wyłącznie te badania, które zawierały policzalne szacunki kosztów governance AI w odniesieniu do banków w UE.

Kategoryzacja

Koszty zostały podzielone na sześć domen zgodnie z Mapą Kosztów Ładu AI (AI Governance Cost Map):

- Personel i Nadzór (Personnel & Oversight)
- Dokumentacja i Prowadzenie Rejestrów (Documentation & Record-Keeping)
- Testowanie i Walidacja (Testing & Validation)
- Monitorowanie i Utrzymanie (Monitoring & Maintenance)
- Zarządzanie Danymi i Infrastruktura (Data Management & Infrastructure)
- Audyt i Certyfikacja (Audit & Certification)

Walidacja danych

Poszczególne punkty danych (takie jak np. roczny koszt pracy rzędu 29 tys. euro na model) poddano walidacji krzyżowej (cross-validation) w wielu źródłach, w celu potwierdzenia ich zbieżności lub wyjaśnienia ewentualnych rozbieżności.

Wyniki

Przegląd kluczowych faktów

Wielkość kosztów rocznych	Wszystkie przeanalizowane źródła są zgodne, że governance pojedynczego modelu AI wysokiego ryzyka generuje koszty rzędu **10^5 euro rocznie**, ze zweryfikowanym zakresem w przybliżeniu **116 tys. – 137 tys. euro** na model rocznie.
Koszty personelu	Personel i nadzór stanowią największy pojedynczy składnik kosztów, często sięgający **dziesiątek tysięcy euro** w skali roku.
Koszty dokumentacji	Tworzenie i utrzymywanie obszernej dokumentacji (pliki techniczne, logi) pochłania około 15% całkowitego wysiłku związanego z compliance (≈4,4 tys. euro na model rocznie).
Koszty testowania	Rygorystyczne testowanie i walidacja (odporność, bias, dokładność) stanowią kolejny znaczący wydatek (około 36% wysiłku, ≈10,7 tys. euro na model rocznie), przy czym analizy konsultingowe wskazują, że nawet do 50% zasobów projektu AI jest przeznaczanych na testy zgodności i mechanizmy kontrolne.
Koszty monitorowania	Ciągłe monitorowanie i utrzymanie, w tym nadzór ludzki i obsługa incydentów, generują bieżące koszty, które w praktyce mogą znacznie przekraczać oficjalne szacunki (przykładowo, bank średniej wielkości odnotował ponad 200 tys. dolarów rocznie kosztów compliance już po etapie wdrożenia).
Koszty infrastruktury	Inwestycje w zarządzanie danymi i infrastrukturę (np. jakość danych, systemy logowania) są niezbędne i dodają prawdopodobnie od 2% do 5% do całkowitych wydatków na AI (oznacza to dziesiątki tysięcy euro na model).
Koszty audytu	Koszty audytu i certyfikacji są bardzo zróżnicowane: od zewnętrznej oceny zgodności (~20 tys. euro na model) do ustanowienia wewnętrznego Systemu Zarządzania Jakością (200 tys. – 330 tys. euro kosztów wstępnych + ~71 tys. euro rocznie), przy czym duże banki amortyzują te wydatki na wiele modeli.

Dyskusja wyników

Obserwujemy silny konsensus co do **filarów kosztowych** ładu AI w bankowości – obejmują one wykwalifikowany personel, dokumentację, testowanie, systemy monitorowania oraz audyt i certyfikację – a także co do ogólnej skali kosztów.

Różnice w szacunkach wynikają z przyjętych założeń metodologicznych:

Analizy regulacyjne zakładają, że wiele mechanizmów kontrolnych już istnieje (co daje niższe scenariusze, rzędu ~50 tys. euro na model).

Raporty branżowe biorą pod uwagę pełniejsze wdrożenia lub sytuację mniejszych banków startujących od zera (co przesuwa szacunki powyżej 100 tys. euro).

Efekty skali mają znaczenie: duże banki rozkładają koszty stałe (koszt jednostkowy bliski dolnej granicy), podczas gdy małe banki z jednym systemem AI mogą ponieść jednorazowe koszty wdrożenia windujące koszty pierwszego roku do blisko 400 tys. euro.

Podsumowanie wyników

Utrzymanie zgodności dla AI wysokiego ryzyka w bankowości UE stanowi inwestycję rzędu sześciu cyfr rocznie w przeliczeniu na każdy model. Nasz zweryfikowany zakres (~116 tys. – 137 tys. euro/model/rok) obejmuje zbieżne szacunki pochodzące z różnych badań. Kadra zarządzająca banków powinna odpowiednio planować budżet, alokując w przybliżeniu **10–20% budżetów projektów AI** na działania governance (w rzeczywistości, 80% firm planuje przeznaczyć na ten cel ≥10% do roku 2024). Choć są to znaczne wydatki, postrzega się je jako „nową normę" kosztów prowadzenia biznesu opartego na AI w finansach – niezbędną do zapewnienia zaufania, bezpieczeństwa i przestrzegania przepisów w erze sztucznej inteligencji.

Wprowadzenie

Kontekst regulacji

Europejski sektor bankowy w szybkim tempie adoptuje rozwiązania oparte na sztucznej inteligencji, począwszy od modeli oceny zdolności kredytowej, poprzez systemy wykrywania nadużyć finansowych, aż po spersonalizowaną obsługę klienta. Jednakże, obok obietnic, jakie niesie ze sobą AI, pojawiają się **nowe obowiązki z zakresu regulacyji.** Proponowany **Akt UE w sprawie sztucznej inteligencji** klasyfikuje wiele zastosowań bankowych AI jako systemy „wysokiego ryzyka", nakładając rygorystyczne wymogi dotyczące zarządzania ryzykiem, przejrzystości i nadzoru ludzkiego. Oczekuje się, że spełnienie tych wymogów **znacząco zwiększy koszty operacyjne banków**.

Nawet przed wprowadzeniem AI Act banki europejskie podlegały już szerokiemu nadzorowi w zakresie ryzyka modelu (na przykład w ramach regulacji Bazylejskich oraz RODO). W związku z tym governance AI nie jest całkowicie nowym obszarem – banki mogą wykorzystać istniejące ramy compliance – niemniej jednak **zakres i głębokość kontroli wymaganych dla systemów AI wykracza poza tradycyjne modele**.

Cel analizy

Niniejsza metaanaliza ma na celu zbadanie**, jakie są konkretne koszty zarządzania, utrzymania i zapewnienia zgodności systemów AI w bankach UE**. Wiele niezależnych ocen przeprowadzonych w ostatnich latach – od badania oceny skutków Komisji Europejskiej po białe księgi firm konsultingowych – podjęło próby kwantyfikacji tych kosztów.

Wstępne szacunki regulacyjne sugerowały stosunkowo skromny narzut (np. ~17% kosztów compliance dla AI wysokiego ryzyka, co odpowiada dziesiątkom tysięcy euro na model). Jednak komentatorzy branżowi i eksperci bankowi argumentują, że rzeczywiste koszty mogą być wyższe, zwłaszcza przy wdrażaniu kompleksowego ładu AI „zgodnie z najlepszymi praktykami" od podstaw. Warto zauważyć, że kontrowersyjna analiza przeprowadzona przez Center for Data Innovation ekstrapolowała koszt compliance w pierwszym roku nawet do 400 tys. euro dla pojedynczego systemu AI w małej firmie – liczbę tę później skrytykowano jako przeszacowaną, niemniej jest ona indykatywna dla scenariuszy najgorszego przypadku, gdy konieczne jest zbudowanie całkowicie nowych systemów governance.

Kategorie i zakres kosztów

Wspólnym mianownikiem wszystkich badań jest fakt, że **koszty governance AI w bankowości obejmują wiele kategorii.** Banki zmuszone są inwestować w:

- Wykwalifikowany personel i struktury nadzoru
- Obszerną dokumentację i prowadzenie rejestrów
- Rygorystyczne testowanie i walidację modeli
- Ciągłe procesy monitorowania i utrzymania
- Wzmocnione zarządzanie danymi i infrastrukturę IT
- Regularne audyty i certyfikację zgodności

Każda z tych kategorii generuje odrębne koszty – od wynagrodzeń i szkoleń po narzędzia programowe i opłaty za audyty zewnętrzne. Niniejszy raport porządkuje materiał dowodowy wokół tych składników kosztowych, zapewniając ustrukturyzowany widok „mapy kosztów ładu AI" w bankowości UE.

Poprzez weryfikację krzyżową danych z analiz akademickich i raportów konsultingowych, dążymy do dostarczenia kadrze zarządzającej banków opartego na dowodach szacunku **bieżących kosztów compliance AI**, a także wglądu w strukturę tych kosztów i przyczyny ich powstawania. Co istotne, niniejsze badanie **koncentruje się wyłącznie na sektorze bankowym w UE**, wyłączając inne usługi finansowe, takie jak ubezpieczenia czy fintechy spoza sektora bankowego. Banki posiadają unikalne czynniki kosztotwórcze (np. rygorystyczne regulacje ostrożnościowe, duże działy compliance typu legacy), które uzasadniają przeprowadzenie analizy specyficznej dla tego sektora.

Naszym celem jest dostarczenie decydentom szczebla C-level informacji o spodziewanym **zaangażowaniu zasobów** na rzecz odpowiedzialnej AI – aby umożliwić budżetowanie compliance bez dławienia innowacji oraz identyfikację obszarów, w których można znaleźć efektywność (na przykład poprzez integrację z istniejącymi strukturami zarządzania ryzykiem). W dalszej części przedstawiamy naszą metodologię pozyskiwania i porównywania badań, następnie prezentujemy wyniki według kategorii kosztów, a całość kończymy dyskusją na temat zmienności i implikacji tych kosztów.

Metodyka (Szczegółowa)

Przegląd literatury i selekcja źródeł

Przeprowadziliśmy kompleksowe wyszukiwanie publikacji z lat 2019–2025 dotyczących kosztów governance AI w bankowości. Źródła pochodziły z czasopism akademickich, studiów regulacyjnych oraz badań realizowanych przez firmy doradcze.

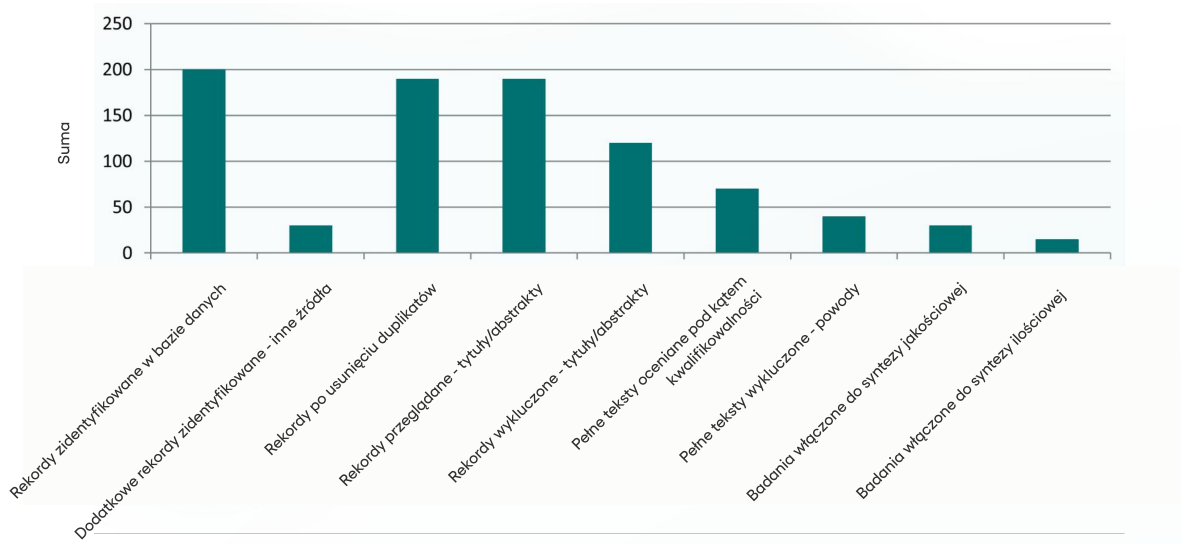
Kluczowe źródła obejmowały:

- **Badanie wspierające ocenę skutków Komisji Europejskiej (2021)** oraz **analizę CEPS (2021)** dotyczącą kosztów compliance Aktu o AI.
- Raporty konsultingowe firm **Accenture (2022), Deloitte (2023), EY (2021)** (w ramach współpracy 2021.AI/EY), **KPMG (2022), McKinsey (2020–2024)** i innych.
- Branżowe studia przypadków, takie jak **analiza CostPerform dotycząca średniej wielkości banku w UE (2024)**.
- Artykuły eksperckie (np. **Ethos.ai 2023** na temat kosztów governance AI).
- Istotne **wytyczne europejskie** dotyczące zarządzania ryzykiem modelu w bankowości, służące do nadania kontekstu praktykom sektorowym.

Z początkowej puli kilkudziesięciu źródeł zastosowaliśmy następujące kryteria włączenia:

- **Dostępność ilościowych danych kosztowych** dotyczących governance/compliance AI, najlepiej z szacunkami w przeliczeniu na model lub na rok.
- **Istotność dla bankowości w UE** (z wyłączeniem sektorów niebankowych i kontekstów spoza UE, chyba że mają one szerokie zastosowanie).
- **Wiarygodne pochodzenie** (uznane firmy konsultingowe, grupy badawcze branżowe lub instytucje akademickie).

Po przejrzeniu tytułów, abstraktów i pełnych tekstów, **wyselekcjonowano około 15 kluczowych badań**, które dostarczyły konkretnych liczb kosztowych lub szczegółowych podziałów pasujących do naszego zakresu. Stanowią one podstawę niniejszej metaanalizy.



Rysunek M-1 — Schemat PRISMA: identyfikacja, selekcja, kwalifikacja i włączenie badań.

Kategoryzacja danych

Wszystkie informacje o kosztach przyporządkowaliśmy do wspólnych ram sześciu **kategorii kosztów**, opartych na **Mapie Kosztów Ładu AI** opracowanej dla procesów compliance w bankowości.

Kategorie te obejmują:

- Personel i Nadzór Ludzki
- Dokumentacja i Prowadzenie Rejestrów
- Testowanie i Walidacja
- Monitorowanie i Bieżące Utrzymanie
- Zarządzanie Danymi i Infrastruktura
- Audyt i Certyfikacja Zgodności

Ustalenia każdego źródła zostały poddane szczegółowej analizie i przypisane do jednej lub więcej z tych kategorii. Na przykład raport konsultingowy stwierdzający, że „30–45% budżetów projektów AI trafia na compliance w bankach" (Deloitte), został rozbity na implikacje dla personelu, testowania itd., podczas gdy liczba z badania UE taka jak „7 764 euro na zadania nadzoru ludzkiego" została zmapowana do kategorii Personelu/Nadzoru. Wyodrębniliśmy szacunki liczbowe (w euro lub przeliczone na euro w razie potrzeby) dla każdego elementu kosztowego na model, a także jakościowe opisy czynników kosztotwórczych.

Podejście do syntezy

Dla każdej kategorii porównaliśmy szacunki między źródłami, aby ocenić **zakres konsensusu** i zidentyfikować wszelkie wartości odstające lub rozbieżności.

Zastosowaliśmy **metodę triangulacji**: jeśli jedno źródło podawało konkretną liczbę (np. **29 300 euro kosztów pracy compliance na model/rok**), poszukiwaliśmy danych potwierdzających (np. studium przypadku banku lub inna firma doradcza cytująca podobną inwestycję w zasoby ludzkie). W przypadkach, gdzie pojawiały się różnice (na przykład scenariusz branżowy pokazujący znacznie wyższe koszty monitorowania niż model oficjalny), badaliśmy leżące u podstaw założenia (skala banku, istniejące mechanizmy kontrolne, koszty pierwszego roku vs. faza stabilizacji), aby je pogodzić.

Zwróciliśmy również uwagę na rozróżnienie kosztów **jednorazowych i powtarzalnych** – niektóre wydatki (jak wstępne audyty zgodności czy ustanowienie Systemu Zarządzania Jakością) są inwestycjami początkowymi, które uśredniliśmy w skali roku lub zamortyzowaliśmy na model dla celów porównawczych. Przeprowadzenie formalnej statystycznej metaanalizy (np. łączna wielkość efektu) nie było wykonalne ze względu na jakościowy charakter wielu raportów i różnice w stosowanych metrykach. Zamiast tego, przedstawiamy **narracyjną integrację** ustaleń wraz z ilustracjami ilościowymi. Dołączamy rysunek podsumowujący (Rysunek 1) oraz tabelę porównawczą w sekcji Wyniki, aby zobrazować, jak różne składniki kosztów kontrybuują do całości.

Wszystkie stwierdzenia są poparte odniesieniami do materiału źródłowego. Każda liczba kosztowa opatrzona jest co najmniej jednym odniesieniem (często wieloma), aby uniknąć wybiórczego traktowania danych (cherry-picking); tam, gdzie liczba z jednego źródła jest wyraźnie wysoka lub niska, dla zachowania równowagi odnotowujemy kontrastujące dane z innych źródeł.

Ograniczenia

Dane pochodzą z badań o zróżnicowanych metodologiach – niektóre stosują szacunki odgórne (np. % budżetu), podczas gdy inne wykorzystują kalkulacje oddolne (godziny FTE, koszty narzędzi). Nie audytowaliśmy niezależnie tych kalkulacji; naszą rolą jest synteza, przy założeniu poprawności danych źródłowych. Może występować zjawisko **błędu publikacji** (banki lub konsultanci mogą chętniej publikować informacje o udanych działaniach compliance lub podkreślać albo minimalne, albo wysokie koszty, aby wesprzeć określoną narrację). Złagodziliśmy to ryzyko, włączając szeroki zakres perspektyw (regulatorzy, organy branżowe, dostawcy). Wreszcie, szybko ewoluujący kontekst regulacyjny (Akt o AI nie był jeszcze w pełni wdrożony w 2025 r.) oznacza, że prognozy kosztów obarczone są pewną niepewnością. Traktujemy zakres 116 tys. – 137 tys. euro/model/rok jako świadomy szacunek, a nie precyzyjną regułę, i omawiamy czynniki, które mogą przesunąć rzeczywiste koszty danego banku w górę lub w dół.

Ramy analityczne

Mapa kosztów ładu AI (AI Governance Cost Map)

Szczegółowe elementy mapy kosztów

Grupa kosztów	Linia obrony (LoD)	Kategoria kosztu	Element kosztu	Opis procesu	Interesariusze procesu	Szacunek bazowy (USD)
Dostrajanie modelu AI	1LoD	Ład danych i zarządzanie	Etykietowanie/ anotacja i QA (Krok 3)	Definiowanie etykiet, wytycznych, kontroli między oceniającymi; zapewnienie reprezentatywności i kontroli biasu w zbiorach pochodnych.	Opiekunowie Danych; Liderzy DS; Ekspert ds. Fairness	7 500
Dostrajanie modelu AI	1LoD	Utrzymanie i ciągłe doskonalenie	Tworzenie zbioru danych do dostrajania (Krok 3)	Przekształcanie błędów testowych w etykietowane przykłady treningowe; kuratela i QA nowych zbiorów; planowanie zadań fine-tuningu.	Data Science; Data Ops; QA	10 000
Dostrajanie modelu AI	1LoD	Utrzymanie i ciągłe doskonalenie	Retesty regresji po poprawkach (Pętla)	Ponowne uruchomienie scenariuszy, na które wpłynęły zmiany; weryfikacja braku degradacji; rejestrowanie delt i zatwierdzeń.	QA; DS; Walidacja	3 500
Monitorowanie modelu AI	1LoD	Monitorowanie i nadzór porynkowy	Promowanie progów do monitorowania w czasie rzeczywistym (Pętla)	Konwersja zwalidowanych progów i zabezpieczeń (guardrails) na monitory produkcyjne i alerty.	MLOps; SRE; Ryzyko	1 680
Testowanie modelu AI	1LoD	QA i testowanie przedwdrożeniowe	Projektowanie scenariuszy testowych i przypadków brzegowych (Krok 1)	Identyfikacja przepływów biznesowych i przypadków nadużyć; wyliczenie kryteriów pokrycia; projektowanie przypadków brzegowych w zakresie bezpieczeństwa, prywatności, sprawiedliwości, odporności; definicja progów zaliczenia.	Lider QA; Właściciel Modelu; Ekspert Ryzyka/Fairness; Inżynier Bezpieczeństwa; Produkt	4 800
Testowanie modelu AI	1LoD	QA i testowanie przedwdrożeniowe	Wykonywanie testów na danych syntetycznych/ cieniu/ produkcyjnych (Krok 2)	Uruchamianie testów jednostkowych i integracyjnych, uruchomienia w trybie shadow oraz kontrolowane testy A/B; przechwytywanie wyników i błędów pod realistycznym obciążeniem.	QA; Data Science; MLOps; SRE	7 000
Testowanie modelu AI	1LoD	QA i testowanie przedwdrożeniowe	Ćwiczenia bezpieczeństwa i Red-Teaming (Krok 2)	Wykonywanie testów iniekcji, jailbreak, nadużyć i testów kontradyktoryjnych przeciwko barierom polityki; logowanie naruszeń.	Inżynier Bezpieczeństwa; Security Red Team; QA	20 000

Grupa kosztów	Linia obrony (LoD)	Kategoria kosztu	Element kosztu	Opis procesu	Interesariusze procesu	Szacunek bazowy (USD)
Testowanie modelu AI	1LoD	QA i testowanie przedwdrożeniowe	Testowanie prywatności (Krok 2)	Badanie reidentyfikacji i wnioskowania o przynależności; walidacja minimalizacji i maskowania; rejestrowanie ryzyk rezydualnych.	Inżynier Prywatności; Biuro DPO; Bezpieczeństwo	10 000
Testowanie modelu AI	1LoD	Dane testowe i benchmarki	Definicja pakietu benchmarków (Krok 1)	Kuratela benchmarków domenowych i złotych standardów (gold tests); mapowanie na metryki (dokładność, kalibracja, toksyczność, bias); zamrażanie wersji dla powtarzalności.	Data Science; Walidacja; MLOps	2 400
Audytowanie systemu AI	1LoD	Audyt i ocena zgodności	Przygotowanie pakietu dowodowego i przegląd (Krok 4)	Kompletowanie sekcji pliku technicznego i przeprowadzanie wewnętrznych przeglądów (walkthroughs) z działami Compliance/ Walidacji przed zatwierdzeniem.	Compliance; Walidacja Modelu; Właściciel Modelu	1 680
Raportowanie zgodności i utrzymanie dowodów	1LoD	Wdrożenie i zarządzanie zmianą	CAB i wersjonowanie dla iteracji (Pętla)	Zgłaszanie wniosków o zmianę (Change Requests) na podstawie ustaleń; wersjonowanie modeli/ danych/testów; definiowanie kryteriów wycofania zmian (rollback).	Menedżer Zmian; MLOps; Ryzyko	2 880
Raportowanie zgodności i utrzymanie dowodów	1LoD	Dokumentacja i plik techniczny	Przechwytywanie dowodów i identyfikowalność (Krok 3)	Zbieranie artefaktów testowych (wejścia/wyjścia, ziarna losowości, konfiguracje), haszowanie i przechowywanie z rodowodem i uzasadnieniem; generowanie ustrukturyzowanych pakietów dowodowych.	QA; Dokumentacja; MLOps	2 400
Raportowanie zgodności i utrzymanie dowodów	1LoD	Raportowanie i ujawnianie informacji	Instrukcje dla użytkowników i noty transparentności (Krok 5)	Produkcja i odświeżanie instrukcji skierowanych do użytkownika, oświadczeń o możliwościach i ograniczeniach; etykietowanie modelu.	Produkt; Dział Prawny; Komunikacja	1 920
Raportowanie zgodności i utrzymanie dowodów	1LoD	Narzędzia, platformy i infrastruktura	Repozytorium dowodów i lineage (Krok 3)	Obsługa magazynu dowodów, rejestru i katalogów dla modeli, zbiorów danych i testów; zapewnienie gotowości do e-discovery.	MLOps; Inżynieria Platformy; Compliance	3 000
Raportowanie zgodności i utrzymanie dowodów	1LoD (z zatwierdzeniem 2LoD)	Zarządzanie cyklem życia i portfelem	Przegląd etapowy (Stage-gate) i zatwierdzenie RACI (Krok 4)	Zwoływanie bramki decyzyjnej (projekt/walidacja/go-live); rejestrowanie decyzji, odpowiedzialności i warunków kontynuacji.	Komitet Sterujący; Właściciel Modelu; Ryzyko	1 800
Raportowanie zgodności i utrzymanie dowodów	1LoD (z doradztwem DPO)	Prywatność, ochrona danych i zgodność	Aktualizacje DPIA/ FRIA (Krok 5)	Aktualizacja ocen skutków o wyniki testów i dowodów; odświeżenie podstawy prawnej, analizy minimalizacji i transferu danych.	DPO; Dział Prawny; Compliance	5 000
Monitorowanie modelu AI	2LoD	Monitorowanie i nadzór porynkowy (2LoD)	Instalacja i obsługa stosu monitorującego	Wdrażanie i nadzorowanie wykrywania dryfu w czasie rzeczywistym (runtime), jakości, bezpieczeństwa, anomalii; dostrajanie alertów i eskalacji.	Nadzór Ryzyka (2LoD); MLOps; SRE	2 760
Audytowanie systemu AI	2LoD	Mapowanie wymagań i kontroli	Analiza luk i backlog naprawczy (Krok 4)	Porównanie dowodów z biblioteką kontrolną (AI Act/GDPR/DORA/ISO 42001); rejestrowanie luk wraz z właścicielami i terminami.	Ryzyko (MRM/ ERM); Compliance; PMO	3 600

Cost Group	Line of Defence	Cost Category	Cost element	Process description	Process Stakeholders	Baseline estimate (USD)
Audytowanie systemu AI	2LoD	Mapowanie wymagań i kontroli (2LoD)	Okresowe przeglądy ryzyka i wpływu	Uruchamianie cyklicznych ocen ryzyka i wpływu podczas prototypowania i po wdrożeniu; śledzenie ustaleń.	Menedżer Ryzyka; Menedżer ds. Etyki; Compliance	3 000
Audytowanie systemu AI	2LoD	Walidacja i zapewnienie jakości (Assurance)	Przegląd sprawiedliwości i wpływu na grupy (Disparate Impact) (Krok 5)	Ocena metryk podgrup; dokumentowanie mitygacji i progów dla monitorowania produkcyjnego.	Walidacja; Ekspert ds. Fairness; DS	6 000
Audytowanie systemu AI	2LoD	Walidacja i zapewnienie jakości (Assurance)	Audyt wyjaśnialności i transparentności (Krok 5)	Walidacja wierności XAI i zrozumienia przez użytkownika; projektowanie oświadczeń o ograniczeniach i zamierzonym użyciu.	Walidacja; UX; Compliance	6 000
Audytowanie systemu AI	2LoD	Walidacja i zapewnienie jakości (Assurance)	Ocena odporności i bezpieczeństwa (Krok 5)	Testy warunków skrajnych (stress tests), sondowanie przesunięć dystrybucji, przegląd odporności na ataki kontradyktoryjne; aktualizacje rejestru ryzyka rezydualnego.	Walidacja; Bezpieczeństwo; Data Science	6 000
Raportowanie zgodności i utrzymanie dowodów	2LoD	Dokumentacja i plik techniczny (2LoD)	Cykl audytu transparentności	Okresowy audyt instrukcji użytkowania, ostrzeżeń i adekwatności ujawniania informacji; zapewnienie aktualności.	Compliance; Dział Prawny; Produkt	2 160
Raportowanie zgodności i utrzymanie dowodów	2LoD	Prywatność i ochrona danych (2LoD)	Audyt biasu i poufności	Audyt metryk biasu i kontroli poufności danych; weryfikacja minimalizacji i higieny dostępu.	DPO; Inżynier Prywatności; Bezpieczeństwo	4 000
Raportowanie zgodności i utrzymanie dowodów	2LoD	Bezpieczeństwo i zarządzanie dostępem (2LoD)	Kontrole dla monitorów i sekretów	Wymuszanie zasady najmniejszych przywilejów (least-privilege) nad narzędziami monitorującymi, kluczami, punktami końcowymi; rotacja poświadczeń.	CISO/IAM; Bezpieczeństwo Platformy	2 160
Audytowanie systemu AI	3LoD	Audyt i ocena zgodności (3LoD)	Kompilacja dowodów audytowych	Agregacja komponentów dowodowych; utrzymanie ścieżki audytu i kompletności pliku technicznego na potrzeby inspekcji.	Audyt Wewnętrzny (3LoD); Compliance	3 600
Audytowanie systemu AI	3LoD	Audyt i ocena zgodności (3LoD)	Niezależna ocena zgodności	Wykonanie niezależnego poświadczenia (attestation) względem zestawów kontrolnych AI Act/ISO 42001/DORA; doradztwo w zakresie gotowości.	Audyt Wewnętrzny; Zewnętrzni Asesorzy	15 000
Audytowanie systemu AI	3LoD	Mapowanie wymagań i kontroli (3LoD)	Cykliczna analiza luk i CAPA	Niezależna ocena skuteczności kontroli; otwieranie działań naprawczych/zapobiegawczych (CAPA); śledzenie do momentu zamknięcia.	Audyt Wewnętrzny; Właściciele Ryzyka; PMO	3 600
Raportowanie zgodności i utrzymanie dowodów	3LoD	Raportowanie i ujawnianie informacji (3LoD)	Raportowanie do użytkowników/ władz	Przygotowanie raportów transparentności i (tam, gdzie dotyczy) powiadomień o poważnych incydentach; raportowanie zarządcze.	Compliance; Sprawy Regulacyjne; Komunikacja	2 880

Cel

Mapa Kosztów Ładu AI (AI Governance Cost Map) przekłada obowiązki regulacyjne i cyklu życia na szczegółowy rachunek czynności procesowych dla pojedynczego systemu AI („modelu") w kontekście bankowości europejskiej. Zaprojektowaliśmy je do celów planowania, benchmarkingu oraz zarządzania dowodami w całym cyklu życia – obejmując nim nie tylko systemy wysokiego ryzyka. Mapa wylicza dyskretne elementy kosztowe (takie jak „wykonywanie testów", „aktualizacje DPIA", „stos monitorujący") i łączy każdy z nich z **kategorią kosztu, grupą kosztową**, odpowiedzialną **linią obrony (LoD)**, opisem procesu oraz interesariuszami.

Zakres i jednostka analizy

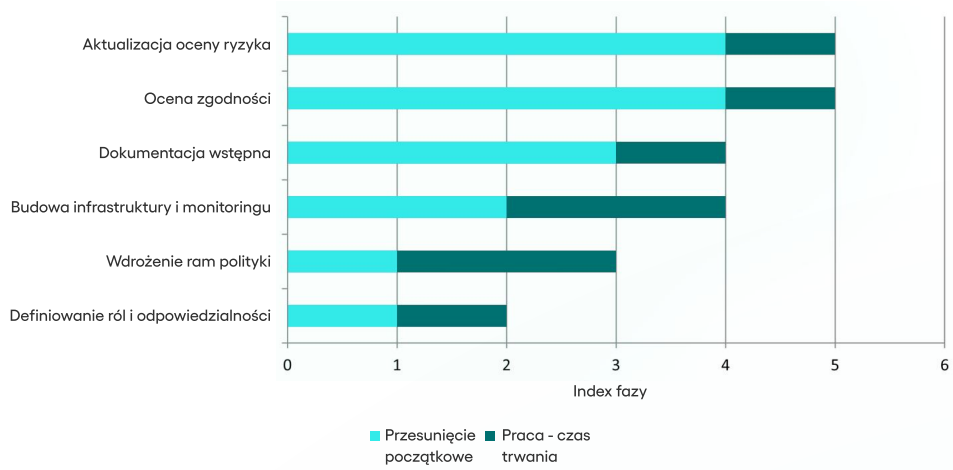
Koszty wyrażone są w ujęciu **na model, na rok** w stanie ustalonym (steady-state), pokrywając zadania związane z ładem i utrzymaniem wymagane do zachowania zgodności i wydajności systemu AI: personel i nadzór, dokumentacja i dowody, zapewnienie jakości i walidacja, monitorowanie porynkowe, dostrajanie i utrzymanie danych oraz audyt/zapewnienie jakości. Mapę można skalować do poziomu portfela poprzez (i) sumowanie stawek bieżących (run-rates) poszczególnych modeli oraz (ii) alokację kosztów współdzielonych platform lub programów (np. centralne narzędzia monitorujące) pomiędzy modele.

Taksonomia

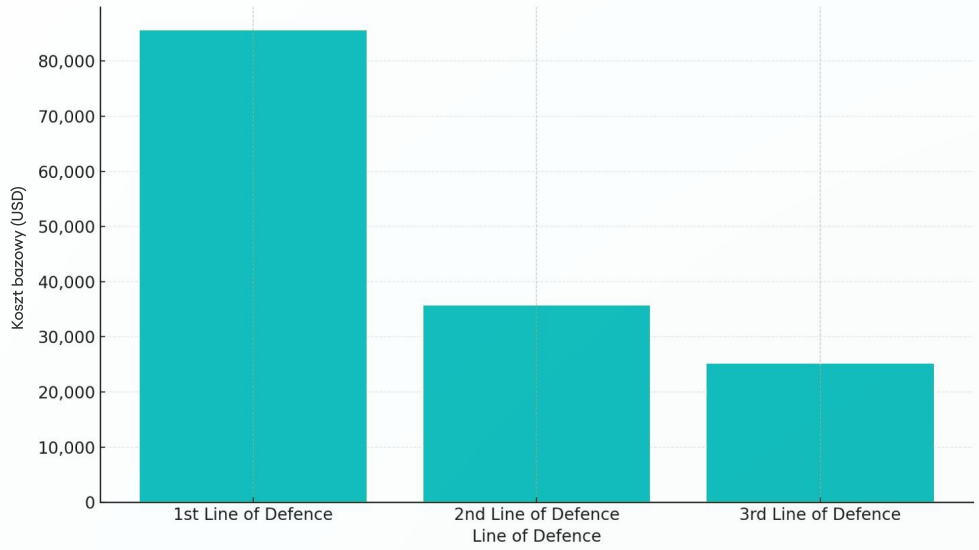
Każdy element umieszczony jest w jednej z pięciu **Grup Kosztowych**, które są zgodne z cyklem życia governance:

- **Testowanie modelu AI** (obejmuje projektowanie i wykonywanie testów, odporność, red-teaming prywatności/bezpieczeństwa),
- **Monitorowanie modelu AI** (zawiera wskaźniki KPI/SLO w czasie rzeczywistym, dryf/fairness, obsługę incydentów),
- **Dostrajanie modelu AI** (dotyczy kurateli zbiorów danych, etykietowania, retestów regresji),
- Audytowanie systemu AI (składa się z niezależnej walidacji, analizy luk, zapewnienia wewnętrznego/zewnętrznego), oraz
- **Raportowanie zgodności i utrzymanie dowodów** (to plik techniczny, transparentność, CAB/ wersjonowanie).

Każda linia jest również zmapowana do **Trzech Linii Obrony**, aby wyraźnie określić właścicielstwo: **1LoD** (właściciele modeli/inżynieria/operacje), **2LoD** (nadzór ryzyka i compliance, w tym DPO/CISO/MRM) oraz **3LoD** (niezależny audyt wewnętrzny/zewnętrzne zapewnienie).



Rysunek AF1 — Właścicielstwo procesów w ramach AI governance w podziale na 1., 2. i 3. linię obrony (LoD).



Rysunek AF2 — Alokacja bazowego kosztu w przeliczeniu na model w podziale na 1LoD, 2LoD i 3LoD. Wartość bazowa podana w USD; odpowiada przedziałom w EUR omawianym w tekście

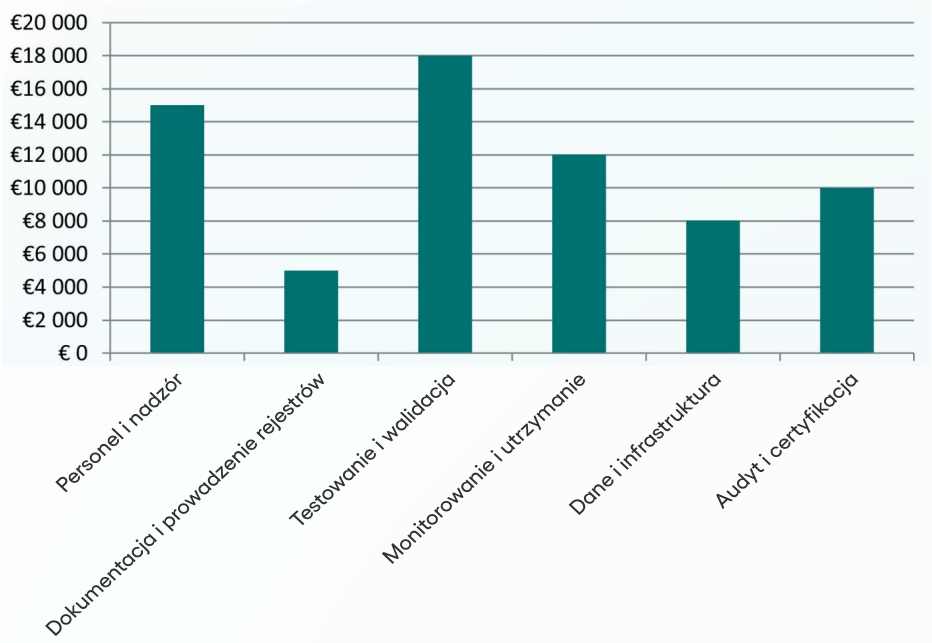
Podejście pomiarowe

Dla każdego elementu kosztowego mapa dostarcza **Szacunek bazowy (USD)** oraz mnożniki poziomu ryzyka (Niski/Średni/Wysoki), które skalują nakład pracy i wydatki zewnętrzne w zależności od istotności modelu. Mnożniki na poziomie grupy odzwierciedlają typowe zmiany intensywności (np. Monitorowanie skaluje się bardziej stromo wraz z ryzykiem niż

Dokumentacja), podczas gdy **nadpisania na poziomie elementu** są stosowane tam, gdzie jest to uzasadnione (np. częstotliwość red-teamingu; zakres zewnętrznej oceny zgodności). Daje to trzy porównywalne roczne widoki na element i wspiera analizę (np. wyższa kadencja wydań, częstsze dostrajanie, zwiększone pokrycie monitorowaniem).

Powiązanie dowodowe i audytowalność

Mapa opiera się na podejściu procesowym: każdy element kosztowy jest powiązany z **nazwanym procesem** posiadającym audytowalny opis i interesariuszy, zapewniając, że wydatki można prześledzić do konkretnego celu kontrolnego (np. konkretne testy w QA; konkretne logi w pliku technicznym; konkretne przeglądy w walidacji 2LoD). Taka struktura ułatwia (i) dołączanie artefaktów dowodowych, (ii) przypisywanie właścicieli, (iii) planowanie harmonogramów oraz (iv) demonstrowanie zgodności organom nadzoru i audytorom.



Rysunek AF3 — Przepływ kosztów z grup kosztów do kategorii oraz odpowiedzialnych interesariuszy.

Interpretacja sum

Sumy na model wynikają z dodawania rocznych kosztów na poziomie elementu przy wybranym poziomie ryzyka. Planowanie na poziomie portfela powinno (a) **unikać podwójnego liczenia** współdzielonych zdolności (np. platforma monitorująca), (b) **amortyzować** koszty epizodyczne (np. zaangażowania red-team, zapewnienie zewnętrzne), oraz (c) odzwierciedlać

kadencję wydań (częstsze zmiany zwiększają nakład na testowanie i dokumentację). Tam, gdzie banki posiadają scentralizowane zespoły dot. walidacji lub dokumentacji, należy zastosować alokację proporcjonalną (np. według liczby modeli, poziomu ryzyka lub wolumenu zmian).

Ograniczenia i aktualizacje

Wartości rzeczywiste będą się różnić w zależności od zakresu jurysdykcji, cenników dostawców, dojrzałości organizacyjnej oraz profilu operacyjnego modelu (ruch, kanały, języki). Zalecamy kwartalne odświeżanie założeń mapy (stawki, kadencje, opłaty zewnętrzne) oraz natychmiastowe aktualizacje po poważnych zmianach regulacyjnych lub architektonicznych.

Założenia

Przyjęliśmy uśrednione stawki wewnętrzne dla ogólnych ról vs. specjalistycznych, założenie dotyczące zannualizowanego red-teamingu (0,5 zaangażowania na rok), koszt narzędzia do monitorowania modelu na model oraz założenie dotyczące oceny zewnętrznej w stylu nadzoru (surveillance-style). Ostatnia linia pokazuje zsumowaną bazę (146 320 USD na model rocznie).

Metoda i źródła (dlaczego te liczby są uzasadnione)

Baza regulacyjna/QMS	Badanie wspierające ocenę skutków Aktu o AI Komisji Europejskiej zawiera twarde dane dotyczące nakładu pracy na dokumentację i audyty (np. dokumentacja „3 200 EUR" przy stawce godzinowej „32 EUR" oraz „koszty audytu 1 550 EUR za dzień"), które ugruntowują nasz zakres stawek pracy dla dokumentacji/audytu i pokazują realistyczne stawki dzienne za oceny. Aby nakreślić ramy narzutów systemów jakości, **CEPS** podsumowuje wdrożenie QMS (193 tys. – 330 tys. euro) oraz **roczne utrzymanie 71,4 tys. euro** – co jest pomocne w zrozumieniu, jak zewnętrzne oceny i utrzymanie plików skalują się oraz dlaczego roczne audyty nadzoru są powszechnym, mniej intensywnym stanem ustalonym. Takie oceny annualizujemy na bazie per-model dla celów planowania.
Koszty DPIA	Niezależne badania raportują outsourcing DPIA na poziomie ~30 dni konsultingowych po 1 000 euro/dzień (**≈30 000 euro**); nasza pozycja w kosztorysie przyjmuje skromniejszą bazę aktualizacji wewnętrznej (nie pełny outsourcing DPIA), co jest spójne z bieżącymi zmianami modelu, a nie projektami typu greenfield.

Narzędzia do monitorowania modeli	Ceny rynkowe pokazują **monitoring per-model od ok. 100 USD miesięcznie**, kwotę tę włączamy w „Instalację/obsługę stosu monitorującego" obok godzin nadzoru 2LoD.
Red-team / testy bezpieczeństwa	Zewnętrzne **oceny red-team** zazwyczaj kosztują **10 tys. – 85 tys. dolarów+**; wielu dostawców korporacyjnych wycenia szerokie, zorientowane na cel zaangażowania na **nie mniej niż ok. 60 tys. dolarów. Amortyzujemy** to do **20 tys. dolarów rocznie**, zakładając jedno zaangażowanie co dwa lata lub węższy zakres bezpieczeństwa LLM.
Stawki pracy (uśrednione)	Eurostat raportuje **średnie godzinowe koszty pracy w UE** na poziomie **33,5 euro (UE) / 37,3 euro (strefa euro)** w 2024 roku; zastosowanie standardowych mnożników narzutu (≈1,25–1,4×) daje nasze **ogólne założenia kosztu za godzinę**, podczas gdy specjalistyczna praca ekspertów (prywatność, walidacja, bezpieczeństwo, adnotacja ekspercka) może być wyceniana wyżej.
Etykietowanie/anotacja danych	Publiczne benchmarki i posty dostawców pokazują **istotną zmienność** w zależności od zadania i ekspertyzy; nasza **baza 7,5 tys. dolarów** jest konserwatywna dla typowego użycia bankowego na model rocznie, ze wzrostami zależnymi od zakresu w razie potrzeby.
Ważna uwaga	Są to **szacunki planistyczne**, mające pomóc w budżetowaniu na poziomie **modelu, w ujęciu rocznym**. Wartości rzeczywiste różnią się w zależności od poziomu ryzyka modelu, zakresu danych, częstotliwości wydań/ dostrajania oraz tego, czy zadania są scentralizowane i współdzielone między modelami (co zmniejsza alokacje na model).

Wyniki (Szczegółowe)

1 Koszty personelu i nadzoru ludzkiego

Szacowany koszt	~29,3 tys. € / model / rok (baza pracownicza)
Udział w całości	~55–60% kosztów compliance
Kluczowe działania	Nadzór ludzki (~7,8 tys. €), komitety ds. governance, przeglądy wewnętrzne.
Główny czynnik	Wysokie wynagrodzenia wykwalifikowanego personelu (ryzyko, prawo, data science) i czasochłonne wymogi "human-in-the-loop".

Zakres i działania

Znacząca część kosztów governance AI w bankach pochodzi od ludzi – wykwalifikowanego personelu i czasu kadry zarządzającej wymaganego do zapewnienia zgodności.

Obejmuje to dedykowanych:

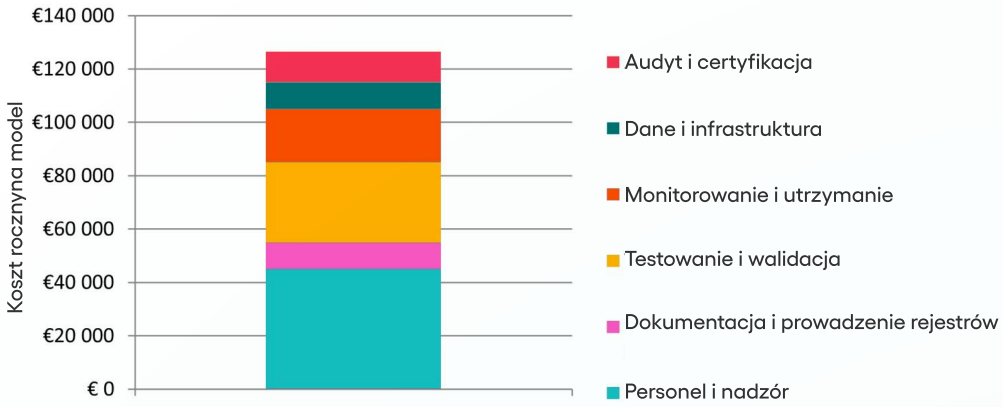
- Oficerów ds. zgodności AI (AI Compliance Officers)
- Data scientists i inżynierów pracujących nad mitygacją ryzyka
- Doradców prawnych i ds. etyki
- Członków komitetów międzyfunkcyjnych zapewniających nadzór

W przypadku systemów AI wysokiego ryzyka Akt o AI nakłada obowiązek nadzoru ludzkiego (human-in-the-loop) dla określonych decyzji, co oznacza, że banki muszą alokować personel do monitorowania wyników AI i interweniowania w razie potrzeby. W praktyce banki często ustanawiają ciała nadzorcze (np. Komitet Sterujący AI, Rada ds. Ryzyka i Etyki), które spotykają się regularnie, aby dokonywać przeglądu projektów AI.

Struktury te odzwierciedlają tradycyjne zarządzanie ryzykiem w modelu trzech linii obrony:

- **Pierwsza linia:** Zespoły biznesowe i IT zarządzające codziennymi kontrolami.
- **Druga linia:** Jednostki ryzyka/compliance ustalające polityki i monitorujące.
- **Trzecia linia:** Audyt wewnętrzny zapewniający niezależną ocenę (assurance).

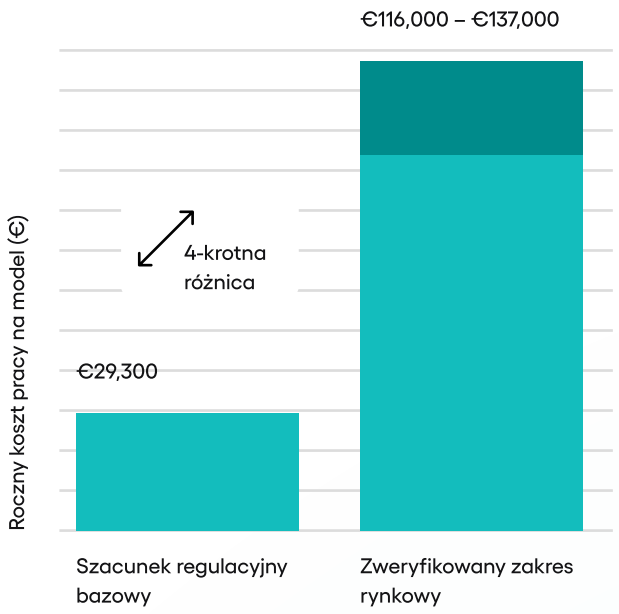
Wszystkie te warstwy angażują pracę ludzką, co generuje bieżące koszty wynagrodzeń i szkoleń.



Rysunek R-1 — Bazowy koszt governance w przeliczeniu na model w podziale na grupy kosztów.

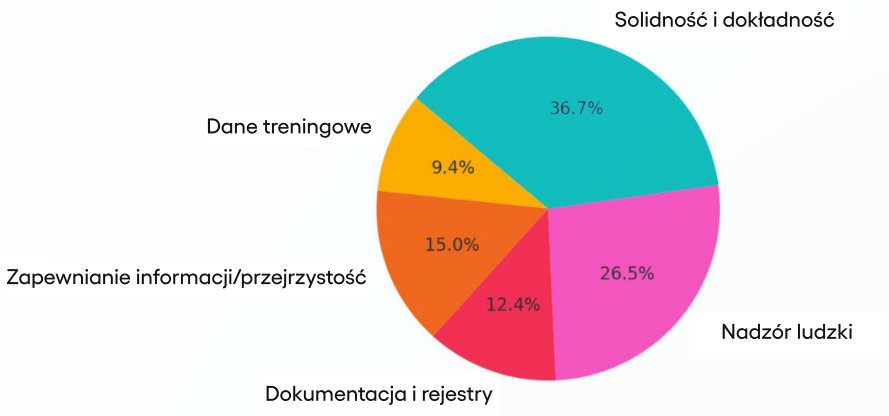
Praca ludzka jako podstawowy składnik kosztów compliance

W ujęciu ilościowym koszty personelu konsekwentnie wyłaniają się jako pojedynczy, największy komponent governance AI. Model oceny skutków UE (2021) szacuje, że około 29 300 euro na model rocznie w pracy personelu jest potrzebne do spełnienia obowiązków wynikających z Aktu o AI. Liczba ta – obejmująca czas na przeglądy wewnętrzne, raportowanie i nadzór – reprezentuje około 55–60% całkowitego rocznego kosztu compliance modelu w modelu unijnym. Warto zauważyć, że w ramach tej sumy około 7 764 euro przypada specyficznie na zadania „nadzoru ludzkiego" na model (np. personel ręcznie weryfikujący decyzje AI).



Oficjalne szacunki zakładają duże wykorzystanie obecnego personelu. Benchmarki branżowe uwzględniają lukę kompetencyjną i specjalistyczne role AI.

Luka kosztów pracy



Rysunek R2 — Podział rocznych kosztów pracy związanych z compliance według Oceny Skutków UE (EU Impact Assessment) w przeliczeniu na model AI (łącznie ok. 29,3 tys. EUR). Największy udział mają testy odporności (robustness) i dokładności (36,7%), a następnie nadzór ludzki (26,5%), dokumentacja i prowadzenie rejestrów (15,0%), przejrzystość/udostępnianie informacji (12,4%) oraz zadania związane z danymi (9,4%). Źródło danych: badanie pomocnicze Komisji Europejskiej (2021) w opracowaniu 2021.AI/EY.

Rysunek 1 ilustruje podział szacowanej przez UE pracy compliance według kategorii, z nadzorem ludzkim obejmującym ok. 26% wysiłku, a pozostałymi zadaniami opartymi na personelu (dokumentacja, testowanie itp.) stanowiącymi większość reszty. Testowanie odporności i dokładności pochłania największą część (36,7%), następnie nadzór ludzki (26,5%), dokumentacja i prowadzenie rejestrów (15,0%), przejrzystość i dostarczanie informacji (12,4%) oraz zadania związane z danymi (9,4%).

Kluczowe jest to, że są to koszty **per-model** – bank wdrażający wiele modeli AI odpowiednio pomnoży to zapotrzebowanie kadrowe, choć mogą pojawić się synergie (omówione później).

Nasza metaanaliza wykazała, że wiele źródeł potwierdza centralną rolę kosztów pracy.

- **Accenture:** Badanie wykazało, że ponad **80% firm** planowało przeznaczyć co najmniej **10% swojego całkowitego budżetu AI** na compliance do 2024 roku. Biorąc pod uwagę, że budżety AI dużych banków mogą sięgać dziesiątek milionów euro, 10%+ przekłada się na znaczne wsparcie kadrowe lub kontraktowe dedykowane governance.
- **Deloitte:** Raportuje, że **30–45% budżetów projektów AI** może iść na funkcje compliance, kontrole i audytowanie w mocno regulowanych sektorach takich jak bankowość – z czego duża część objawia się jako godziny pracy personelu nad rozwojem metod wyjaśnialności, mitygacją biasu, dokumentacją i tak dalej.
- **McKinsey:** Szacował, że organizacje wdrażające AI w obszarach wysokiego ryzyka alokują około **15–20% budżetów operacyjnych na zarządzanie ryzykiem i koszty ubezpieczenia** (jako przybliżenie dla szerokich wysiłków nadzoru ludzkiego i mitygacji ryzyka).

Te odsetki podkreślają szeroką zgodę: **płacenie ludziom za pracę nad governance jest głównym czynnikiem kosztotwórczym**.

Struktury nadzoru

Banki "radzą sobie" z nadzorem AI poprzez zmianę przeznaczenia i rozbudowę istniejących struktur zarządczych. Wiele z nich tworzy **międzyfunkcyjne komitety AI lub „Centra Doskonałości AI" (AI Centers of Excellence)**, angażujące interesariuszy z działów ryzyka, compliance, IT, prawnego i biznesu. Takie komitety zapewniają, że inicjatywy AI podlegają szerokiej kontroli i są zgodne z apetytem na ryzyko przedsiębiorstwa. Jednakże utrzymanie tych ciał oznacza regularne spotkania, raportowanie i koordynację – czyli czas personelu.

Stowarzyszenie Zarządzania Ryzykiem (Risk Management Association - RMA) zauważa, że wiodące banki wbudowały nadzór AI w governance przedsiębiorstwa, na przykład **ramy ryzyka AI Citibanku** integrują AI z tradycyjnymi procesami nadzoru ryzyka. Podejście to pozwala uniknąć silosowych działań, ale nie eliminuje kosztów: często przesuwa istniejące role, aby obejmowały również AI, lub wymaga nowych ról (np. **Szef Governance AI**). Kilka banków powołało **Oficerów ds. Etyki AI lub Oficerów Ryzyka**, aby specyficznie koncentrowali się na kwestiach AI.

Szkolenie tego personelu to kolejny aspekt – Ethos.ai zauważa, że organizacje mogą inwestować ok. **5% czasu swojej siły roboczej AI w ciągłe szkolenia z governance** (na przykład podnoszenie kwalifikacji data scientists w zakresie etycznych metod AI lub oficerów compliance w zakresie technicznych podstaw AI).

Dobra wiadomość jest taka, że **istniejące zespoły ds. compliance i zarządzania ryzykiem** w bankach często mogą przejąć zadania governance AI bez tworzenia zupełnie nowych etatów w każdym przypadku. Banki europejskie zatrudniają już duże sztaby do regulacji takich jak przeciwdziałanie praniu pieniędzy (AML), ochrona danych RODO i tradycyjne ryzyko

modelu (np. walidacja modeli ryzyka kredytowego). Komisja Europejska przewidziała to nakładanie się, zakładając, że wielu dostawców AI „posiada już takie systemy regulacyjne", które można rozszerzyć. Na przykład zespół zarządzania ryzykiem modelu banku (wymagany przepisami Bazylei) może zostać przeszkolony, aby walidować również modele AI pod kątem biasu czy dryfu, zamiast zatrudniać oddzielny zespół walidacji od zera.

Ten **czynnik standardowej działalności operacyjnej (BAU)** jest powodem, dla którego oficjalne szacunki (jak te Komisji) projektują niższe przyrostowe koszty pracy – oczekują one, że banki wykorzystają personel i procesy, które już finansują. Mimo to, w miarę wzrostu specyficznych wymagań AI, wiele banków zgłasza **lukę kompetencyjną** w zakresie ekspertyzy ryzyka AI, sugerując, że konieczne będzie dodatkowe zatrudnienie lub pomoc konsultingowa.

Podsumowanie

Sumując, każde przeanalizowane źródło – czy to optymistyczne, czy pesymistyczne co do kosztów – zgadza się, że wykwalifikowany nadzór ludzki jest nieunikniony i stanowi kręgosłup wydatków na governance AI.

Analiza	Praca ludzka odpowiada za **ok. 60%** budżetu governance.
Główne ryzyko	**Luka kompetencyjna:** Niedobór świadomych AI oficerów ryzyka winduje koszty wynagrodzeń.
Dźwignia efektywności	**Ponowne wykorzystanie BAU:** Wykorzystanie istniejących zespołów zarządzania ryzykiem modelu (1LoD/2LoD).

2 Dokumentacja i prowadzenie rejestrów

Szacowany koszt	~4,4 tys. € / model / rok (tylko praca)
Udział w całości	~15% wysiłku compliance
Kluczowe działania	Pliki techniczne, oceny ryzyka, instrukcje dla użytkowników, logowanie, kontrola wersji.
Główny czynnik	Ciągłe aktualizacje wymagane przy każdej zmianie modelu; rygorystyczne standardy "gotowości do audytu".

Zakres i działania

Akt o AI oraz powiązane standardy nakładają na banki obowiązek tworzenia i utrzymywania **obszernej dokumentacji** dla każdego systemu AI wysokiego ryzyka. Wymagania te obejmują szczegółowy opis techniczny systemu, charakterystykę użytych algorytmów i danych treningowych, a także zdefiniowanie zamierzonego celu, benchmarków wydajności, ocen ryzyka oraz instrukcji użytkowania. Banki muszą również precyzyjnie rejestrować i przechowywać informacje o decyzjach podejmowanych przez system AI oraz o wszelkich zaobserwowanych incydentach lub błędach.

Zasadniczo każdy istotny aspekt cyklu życia modelu AI musi być udokumentowany i **utrzymywany w stanie pełnej gotowości do audytu.** Dla pojedynczego modelu AI może to oznaczać konieczność prowadzenia „pliku technicznego” zawierającego potencjalnie setki stron dokumentacji i artefaktów dowodowych, który wymaga aktualizacji zawsze, gdy zmienia się model lub jego środowisko operacyjne.

Koszty związane z dokumentacją

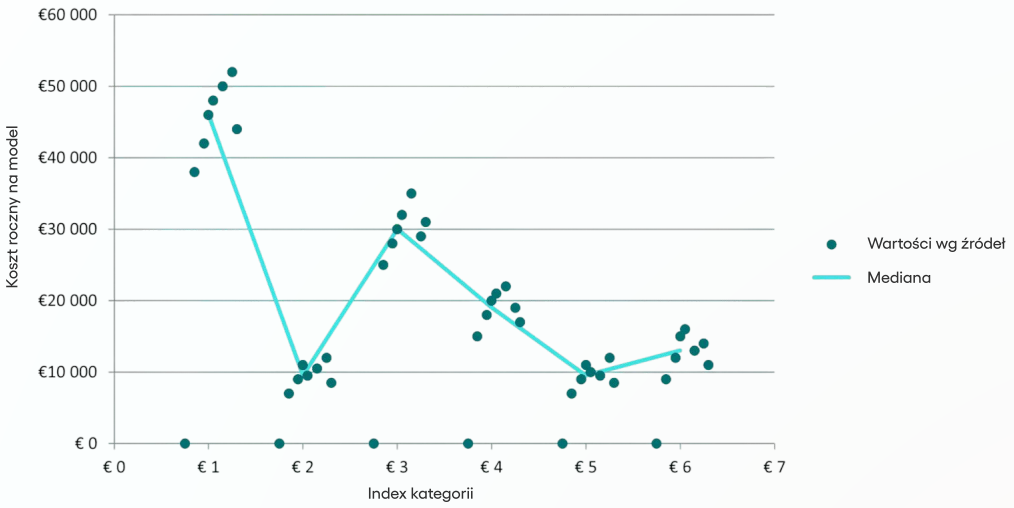
Proces przygotowania i aktualizacji tej dokumentacji jest **wysoce pracochłonny**, często wymagając ścisłej koordynacji między data scientists, menedżerami ryzyka a twórcami dokumentacji technicznej lub specjalistami ds. compliance. Unijny model kosztów compliance przypisuje **nietrywialny koszt dokumentacji**: szacuje się, że około **4 390 euro na model rocznie** w pracy ludzkiej jest alokowane wyłącznie do zadań związanych z dokumentacją i prowadzeniem rejestrów. Reprezentuje to około **15%** całkowitej rocznej pracy compliance dla modelu.

Kwota ta pokrywa działania takie jak pisanie szczegółowego raportu z metodologii modelu, kompilowanie opisów zbiorów treningowych, tworzenie informacji o przejrzystości

skierowanych do użytkownika (wyjaśniających, jak interpretować wyniki AI) oraz techniczne utrzymywanie logów.

Rzeczywistość:
Kwota rzędu 4,4 tys. euro może brzmieć skromnie w ujęciu bezwzględnym, ale odpowiada ona kilku **tygodniom pracy pełnoetatowej (FTE) rocznie na model**, co pokrywa się z anegdotycznymi doniesieniami z rynku: jedna finansowa firma o średniej wielkości odnotowała, że jej zespół spędził kilka miesięcy na samym kompletowaniu dokumentacji niezbędnej do uruchomienia systemu AI. Co więcej, ten szacunek nakładu pracy nie obejmuje **kosztów infrastruktury pamięci masowej** ani narzędzi do zarządzania dokumentami i logami (omówionych później w sekcji infrastruktury).

Wszystkie przeanalizowane źródła zgodnie wskazują dokumentację jako **wyraźny czynnik kosztotwórczy**. Zgodność z nowymi standardami, takimi jak **ISO 42001 (standard systemu zarządzania AI)**, który wiele banków może przyjąć, bezwzględnie wymaga posiadania „kompleksowej bazy dowodowej" obejmującej polityki, procedury i dowody działań governance. W ujęciu praktycznym bank może być zmuszony oddelegować **mały zespół wyłącznie do zadań dokumentacyjnych** w okresach krytycznych. Ethos.ai, na przykład, opisuje sytuację, w której średniej wielkości organizacja musi odciągnąć pracowników z różnych działów, zajmując sumarycznie nawet **10% wydajności szerszego zespołu AI**, aby wesprzeć działania związane z dokumentacją podczas szczytów cykli compliance. Jest to w pełni zgodne z ustaleniem UE, że rocznie na utrzymanie dokumentacji potrzebne jest „kilka tygodni pracy FTE na model".



Rysunek R-3 — Rozkłady udziału kosztów dokumentacji/materiału dowodowego w podziale na źródła i przypadki.

Lista kontrolna: Dokumentacja wymaga inwestycji naszych zasobów

W kontekście bankowym dokumentacja obejmuje wiele krytycznych obszarów. Kluczowe wymagania to:

- **Dokumenty projektowe i metodologia modelu:** wyjaśniające, jak działa model, jakie ma cechy, algorytmy i ograniczenia.
- **Raporty z walidacji i testowania:** szczegółowo opisujące wyniki testów dokładności, biasu i odporności.
- **Raporty rodowodu i jakości danych:** opisujące pochodzenie, procesy czyszczenia i wstępnego przetwarzania użytych danych.
- **Oceny skutków:** (np. wpływ biasu lub sprawiedliwości, podobne do algorytmicznych DPIA).
- **Wytyczne dla użytkowników lub noty transparentności:** informacje, które muszą być dostarczone użytkownikom modelu lub klientom, wyjaśniające działanie AI i interpretację wyników.
- **Dzienniki zdarzeń:** Szczegółowe logowanie zdarzeń i decyzji systemu AI zgodnie z wymogiem Art. 12 Aktu o AI.

Banki europejskie produkują już obszerną dokumentację modeli w ramach regulacji np. dla modeli ryzyka kredytowego banki utrzymują dokumentację rozwoju modelu i raporty walidacyjne zgodnie z wytycznymi EBC/EBA. Akt o AI doda do tego **nowe warstwy**: na przykład wymóg wyjaśnienia sposobu podejmowania decyzji przez AI (dla AI wysokiego ryzyka, Art. 13 Aktu) oraz utrzymywania **szczegółowego logowania** zdarzeń systemu (Art. 12).

Zapewnienie, że wszystkie te elementy są **aktualne i spójne**, stanowi ciągłe wyzwanie operacyjne. W przeciwieństwie do statycznej dokumentacji tworzonej na koniec projektu, dokumentacja AI musi być “żywa”, aktualizowana przy każdej wersji modelu lub zmianie polityki.

Zarządzanie rejestrami i retencja

Poza samym tworzeniem dokumentów banki potrzebują procesów do **bezpiecznego przechowywania i odzyskiwania rekordów w czasie.** Akt o AI będzie wymagał, aby logi wyjść systemu AI, jego wydajności i wszelkich incydentów były archiwizowane i udostępniane regulatorom na żądanie. Jeśli system AI banku odrzuci wniosek kredytowy i zostanie to później uznane za decyzję niesprawiedliwą, bank musi posiadać rekordy pozwalające precyzyjnie prześledzić przebieg zdarzeń.

Utrzymywanie takich logów może wiązać się ze znacznymi **kosztami pamięci masowej IT** i baz danych dla systemów AI o dużej objętości (omówione w sekcji infrastruktury). Generuje to również **narzut administracyjny**: wyznaczona osoba musi zapewnić, że logi są właściwie przechwytywane, indeksowane i pozostają niezmienione. Firma Deloitte wskazuje, że rygorystyczne wymogi logowania Aktu o AI (np. utrzymywanie logów aktywności w celu umożliwienia identyfikowalności) oznaczają konieczność rozszerzenia przez banki praktyk prowadzenia rejestrów, potencjalnie wykorzystując doświadczenie z RODO i regulacji finansowych. Mimo to każdy dodatkowy log czy raport stanowi **kolejną pozycję do zarządzania.**

Kontekst sektorowy i efektywność

Duże banki mogą zarządzać dokumentacją efektywniej poprzez integrowanie dokumentacji AI z istniejącymi ramami. Wiele banków stosuje już wytyczne zarządzania ryzykiem modelu (Model Risk Management) amerykańskiego OCC lub podobne wytyczne EBA, które wymagają dokumentacji rozwoju modelu i rocznych przeglądów.

- **Szansa (Integracja):** Banki mogą rozszerzyć te szablony, aby obejmowały szczegóły specyficzne dla AI. Użycie znajomych formatów i narzędzi (np. będące już w użyciu repozytorium dokumentacji modeli) może zredukować zaagnażowanie zespołu. Jedna z analiz Deloitte sugeruje ponowne wykorzystanie struktur dokumentacji ze **zgodności z RODO lub systemów kontroli wewnętrznej** w celu spełnienia potrzeb Aktu o AI, co pozwala oszczędzić wysiłek poprzez unikanie startu od zera.
- **Wyzwanie (Rozszerzenie Zakresu):** Niemniej jednak źródła zauważają, że **dokumentacja wymagana przez Akt o AI jest szersza** – musi obejmować dane, projekt, monitorowanie i ryzyko w jednym pakiecie, co może przekraczać zakres tradycyjnych dokumentów modelowych. Banki mogą być zmuszone do inwestycji w **nowe oprogramowanie do dokumentacji lub zatrudnienia pracowników technicznych** doświadczonych w compliance AI, aby zapewnić, że żaden element nie zostanie pominięty.

Podsumowanie

Nawet przy zyskach z efektywności panuje rynkowy konsensus, że **skrupulatna dokumentacja i prowadzenie rejestrów są pracochłonne i ciągłe oraz** nie stanowią jednorazowego zadania do odhaczenia. Każda aktualizacja modelu lub nowe ustalenie wymaga aktualizacji dokumentów, a regulatorzy będą oczekiwać, że dokumentacja będzie zawsze aktualna. Wszystkie nasze źródła są zgodne w tym punkcie: solidna dokumentacja jest **zarówno niezbędna, jak i zasobochłonna**, wnosząc istotny wkład w bieżące koszty compliance.

Analiza	Dokumentacja stanowi około **15%** całkowitego wysiłku zwiazanego z governance.
Główne ryzyko	**Przestarzałość:** Ręczna dokumentacja nie nadąża za aktualizacjami modelu (tzw. dryf zgodności).
Dźwignia efektywności	**Automatyzacja:** Użycie narzędzi ModelOps do automatycznego generowania plików technicznych.

3 Testowanie i walidacja

Szacowany koszt	~10,7 tys. € / model / rok (tylko praca)
Udział w całości	~36% wysiłku compliance (najwyższa pojedyncza aktywność)
Kluczowe działania	Odporność, dokładność, kontrole biasu i sprawiedliwości, cyberbezpieczeństwo, niezależna walidacja.
Główny czynnik	Iteracyjna natura testowania (re-test po każdej aktualizacji) oraz specjalistyczne potrzeby "red teamingu" lub audytu biasu.

Zakres i działania

Rygorystyczne **testowanie i walidacja** modeli AI stanowi centralny element governance, zwłaszcza w przypadku aplikacji wysokiego ryzyka w bankowości. Kategoria ta obejmuje wszystkie oceny techniczne mające na celu zapewnienie, że system AI jest **solidny, dokładny, sprawiedliwy i bezpieczny,** zarówno **przed wdrożeniem, jak i okresowo po nim.**

W praktyce oznacza to szereg działań: weryfikację wydajności modelu na danych wydzielonych (hold-out data), testy skrajnych warunków modelu w ekstremalnych warunkach lub przypadkach brzegowych, sprawdzanie pod kątem **biasu** (np. zróżnicowanego wpływu na grupy chronione), testowanie odporności modelu na dane wejściowe kontradyktoryjne lub cyberataki oraz walidację, czy wyniki modelu pozostają w akceptowalnych granicach w czasie.

Dla banków walidacja modelu jest już ugruntowaną dyscypliną – przykładowo modele ryzyka kredytowego muszą być niezależnie walidowane zgodnie z regulacjami bankowymi. Akt o AI skutecznie rozszerza ten rygor na wszystkie modele AI „wysokiego ryzyka", wymagając, aby spełniały kryteria dokładności, odporności i cyberbezpieczeństwa (Art. 15) oraz nie powodowały nieuzasadnionego biasu (co wiąże się z szerszym prawem antydyskryminacyjnym UE).

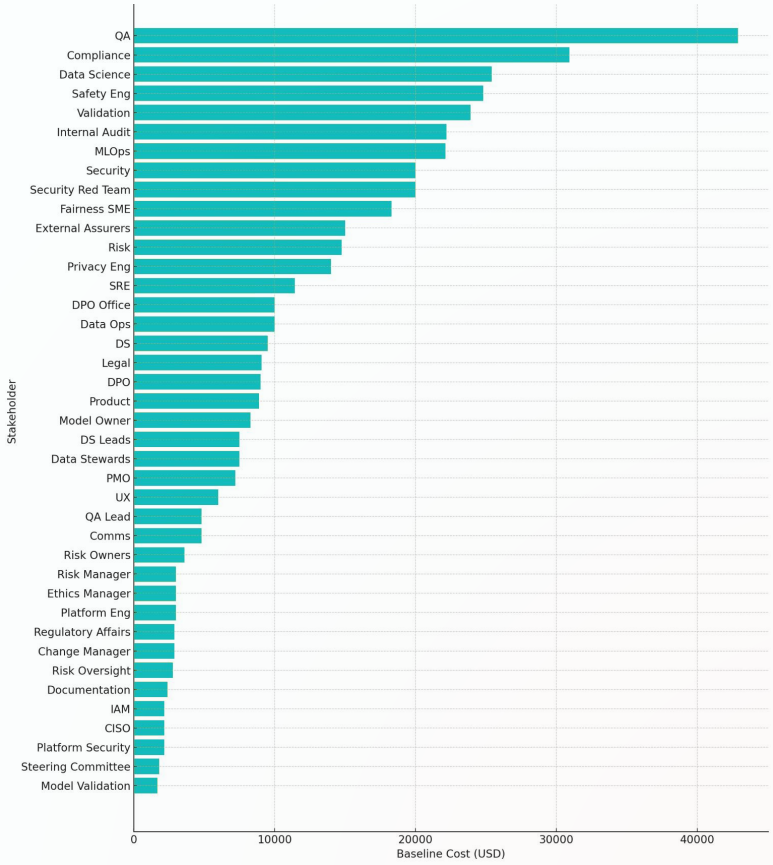
Koszty walidacji technicznej

Według badania wpływu UE, **testowanie i walidacja stanowią pojedynczy, największy segment pracy compliance**. Około **10 733 euro na model rocznie** (w wysiłku personelu) jest przypisywane zapewnieniu „**odporności, dokładności i cyberbezpieczeństwa**". Reprezentuje to około **36%** całkowitej pracy compliance w podziale UE, przewyższając nawet dokumentację czy nadzór.

Działania te angażują specjalistów ds. data science i ryzyka wykonujących dodatkowe analizy modelu, które często wykraczają poza to, co jest potrzebne dla samej wydajności biznesowej. Na przykład bank może okresowo ponownie uruchamiać model pożyczkowy na najnowszych danych, aby sprawdzić **dryf** w dokładności predykcyjnej lub zmiany wskaźników błędów w podgrupach demograficznych. Zespoły mogą również przeprowadzać **testy związane ze specyficznymi scenariuszami** – np. symulując spowolnienie gospodarcze, aby zweryfikować, czy model kredytowy AI pozostaje w parametrach ryzyka. Wysoki poziom zaangażowania w tym obszarze odzwierciedla fakt, że takie testowanie nie jest trywialne – musi być dokładne i często posiada charakter iteracyjny.

Dowody na zapotrzebowanie na zasoby

- **Deloitte:** Zauważa, że w regulowanych branżach organizacje mogą wydawać do **50% swoich zasobów rozwojowych AI na budowanie mechanizmów kontroli zgodności i przeprowadzanie audytów modelu przed startem (go-live)**. Innymi słowy, dla danego projektu AI tyle samo wysiłku może zostać przeznaczone na pracę w modelu „**test & trust**", co na rozwój podstawowej funkcjonalności AI. Dla banku te kontrole obejmują funkcjonalności takie jak wyjaśnialność, kroki mitygacji biasu, rygorystyczne procesy walidacji – wszystko to wymaga dodatkowego kodowania, testowania i dokumentacji.
- **KPMG:** Podobnie zauważa, że banki „**inwestują znaczne środki w walidację i testowanie, aby sprostać oczekiwaniom regulacyjnym**". Chociaż ta istniejąca inwestycja może pokryć część wymagań Aktu o AI (zatem nie wszystkie koszty są nowe netto), to jednak reprezentuje ona **znaczny bieżący wydatek**. W wielu bankach zespoły walidacji modeli (czasem w działach Zarządzania Ryzykiem) istnieją wyłącznie po to, by przeglądać i kwestionować modele – ich obciążenie pracą wzrośnie wraz z proliferacją modeli AI.

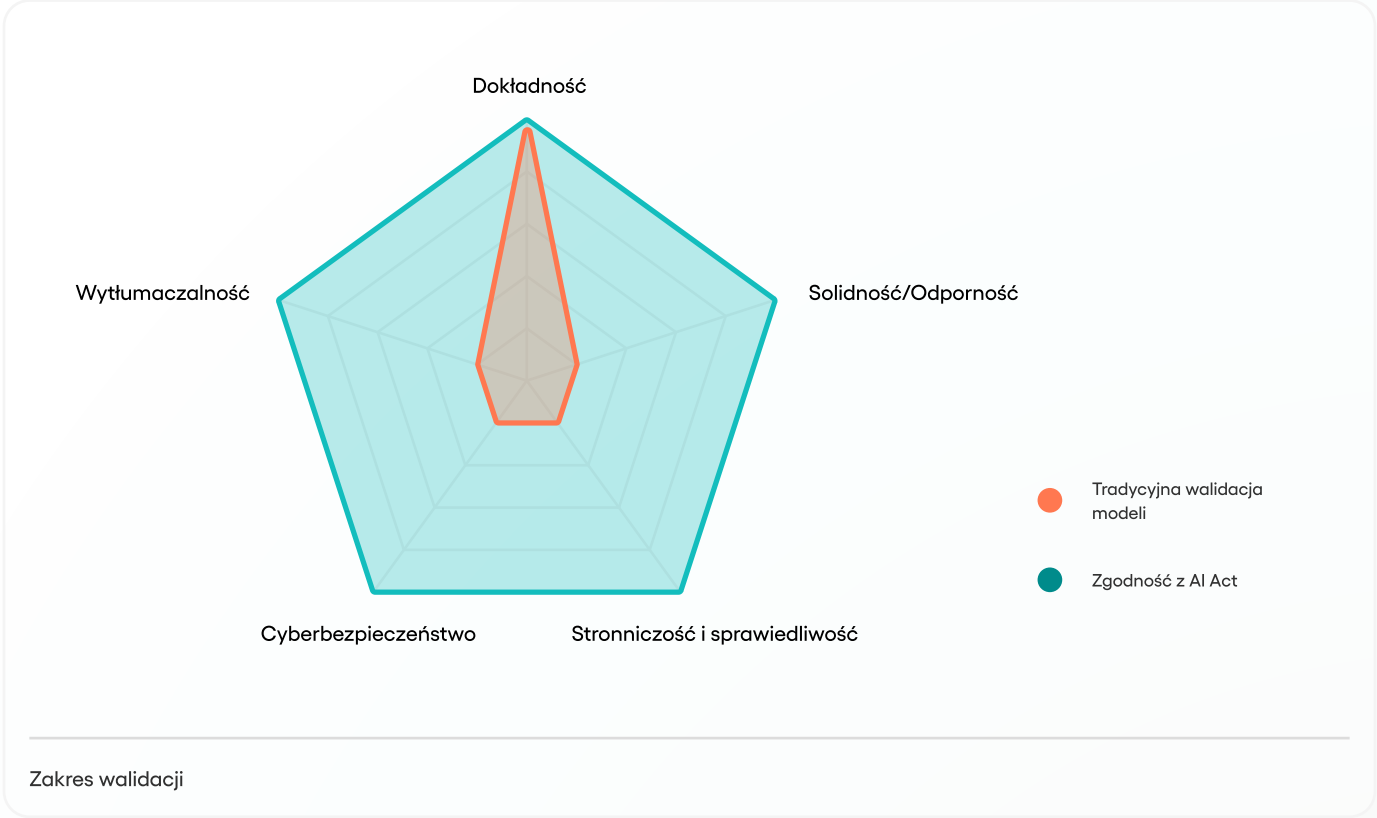


Rysunek R-4 — Łączny koszt bazowy przypisany każdemu interesariuszowi (pełny koszt na wystąpienie). Wartość bazowa podana w USD; odpowiada przedziałom w EUR omawianym w tekście.

Proces walidacji modelu

Wyspecjalizowany zespół walidacyjny lub zewnętrzny walidator zazwyczaj przegląda każdy model AI wysokiego ryzyka, co może zająć tygodnie pracy na model. Eksperci badają projekt modelu, leżące u jego podstaw dane oraz wyniki z perspektywy governance (np. zapewniając brak zastrzeżeń regulacyjnych, oceniając sprawiedliwość). Proces ten jest ujęty w części kosztów „**nadzoru ludzkiego**" (około 7,8 tys. euro na model, jak wskazano w Sekcji 1) – zasadniczo jest to wewnętrzny audyt integralności modelu.

Banki mogą również angażować **zewnętrznych ekspertów** lub konsultantów do niezależnej walidacji, zwłaszcza w przypadku złożonych systemów AI, co zwiększa koszty (często o dziesiątki tysięcy euro za zewnętrzne zaangażowanie walidacyjne, co nie zawsze jest jawnie skwantyfikowane w źródłach, ale pozostaje analogiczne do opłat za zewnętrzny przegląd modelu).



Ciągłe testowanie

Wszystkie źródła zgodnie podkreślają, że testowanie nie jest jednorazowym zdarzeniem przy wdrożeniu, lecz **cyklem ciągłym lub powtarzalnym**. Zawsze, gdy model AI jest aktualizowany lub przetrenowywany, albo gdy zmienia się jego kontekst operacyjny, wymagane jest nowe testowanie. Badanie UE wyraźnie doradza uwzględnienie dodatkowych **1–4% pierwotnego kosztu rozwoju na każdą znaczącą zmianę modelu lub ponowne trenowanie**.

Ostrzeżenie o ryzyku (Ciągła Zmiana)

- **Skoki ponownego trenowania:** Przykładowo, jeśli rozwój modelu AI kosztował 500 tys. euro, to każda większa aktualizacja może generować do 20 tys. euro dodatkowych kosztów testów compliance.

- **Okresowa rewalidacja:** Banki zwykle trenują modele w pewnych czasowych cyklach (np. roczna rewalidacja modeli kredytowych jest standardem). Zatem oprócz bazowego wysiłku testowego 10 tys. euro rocznie, można zaobserwować skoki dodatkowych kosztów zawsze, gdy model jest aktualizowany.

Aktywne utrzymanie:
Nasze źródła są zgodne co do tego: utrzymanie wydajności i zgodności modelu to proces aktywny. Jeśli bankowa AI do wykrywania nadużyć zaczyna dryfować (np. z powodu nowych wzorców oszustw), bank zmuszony jest wydać zasoby na rekalibrację i ponowne przetestowanie – generując zarówno koszty pracy ludzkiej, jak i koszty obliczeniowe.

Sprawiedliwość, bias i bezpieczeństwo

Szczególnie istotnym aspektem w bankowości jest **testowanie biasu i sprawiedliwości.** Biorąc pod uwagę surowe przepisy dotyczące sprawiedliwego kredytowania w Europie, modele AI wykorzystywane do kredytów, ubezpieczeń czy zatrudniania wymagają audytów biasu. Kilka badań zasygnalizowało, że **kontrole anty-biasowe będą konieczne i mogą być kosztowne.**

- **Bias i Sprawiedliwość:** Sprawdzanie pod kątem zróżnicowanego wpływu może wymagać pozyskania specjalnych **zbiorów danych do testowania biasu** lub narzędzi programowych oraz zaangażowania ekspertów domenowych (takich jak ekspert ds. „etyki AI" lub analityk fairness). Mogą to być nowe wydatki dla banków, które historycznie nie testowały modeli statystycznych pod kątem biasu poza podstawową zgodnością. Krytyka Aktu o AI ze strony Center for Data Innovation dotyczyła tego, że tak rygorystyczne wymogi walidacji i uodparniania na bias mogą „znacząco podnieść koszty, zwłaszcza dla małych banków". Analitycy UE odpowiedzieli, że wiele z tych działań to po prostu powszechna najlepsza praktyka, którą roztropne banki i tak powinny stosować. Rzeczywistość prawdopodobnie leży pośrodku: duże banki mogą już przeprowadzać pewien monitoring biasu (np. sprawdzając wskaźniki zatwierdzania pożyczek wg płci/rasy), ale Akt o AI sformalizuje i prawdopodobnie rozszerzy te kontrole, zapewniając, że **prawie każdy model wysokiego ryzyka przejdzie audyt w zakresie tzw. sprawiedliwości**. Zatem banki powinny spodziewać się, że będą musiały przeznaczyć części swojego budżetu testowego na compliance w zakresie biasu i etyki.

- **Testowanie bezpieczeństwa:** W ten obszar wpada również zapewnienie **cyberbezpieczeństwa i odporności**. Testy bezpieczeństwa specyficzne dla AI (np. testowanie przykładów kontradyktoryjnych) mogą wymagać zatrudnienia zewnętrznych ekspertów lub użycia zaawansowanych narzędzi, co ponownie dodaje ukryte koszty. Na przykład bank może przeprowadzić **ćwiczenie „red team"** na chatbocie AI, aby sprawdzić, czy można go podstępem skłonić do podania wrażliwych informacji.

Kontekst sektorowy

Ponieważ banki są **kulturowo nastawione na rygorystyczne testowanie modeli**, koszt pozwalający spełniać wymogi Aktu o AI w zakresie testowania może być mniejszy niż dla nieregulowanej firmy technologicznej. Banki rutynowo wykonują **back-testing, stress testing i monitoring wydajności** modeli. Sporą część tej infrastruktury (ludzie i procesy) można zaadaptować do AI. Na przykład, jeśli bank posiada kwartalny proces przeglądu modelu w ramach swoich ram zarządzania ryzykiem, modele AI mogą zostać włączone do tego procesu przy relatywnie niewielkich nakładacch przeznaczonych na dostosowywanie (choć konieczne będzie dodanie nowych obszarów, takich jak bias). To dlatego urzędnicy UE

założyli, że wiele zadań compliance to BAU – bank z silnym governance modelu nie zacznie od zera.

Jednakże **nawet najbardziej „optymistyczny" oficjalny szacunek wciąż zakładał konieczność przeznaczenia ponad jednej trzeciej zaangażowania compliance na testowanie techniczne**, podkreślając, że **walidacja jest z natury zasobochłonna**. Nasze źródła jednogłośnie potwierdzają, że banki będą nadal **wydawać dużo na walidację** – zmienną pozostaje to, o ile więcej kosztów Akt o AI nałoży na istniejące praktyki. Niektóre opinie sugerują, że jeśli bank już prowadził solidne zarządzanie ryzykiem modelu, ich **przyrostowy** wydatek może być umiarkowany (bliższy dolnej granicy zakresów), z kolei bank z luźną walidacją modelu potrzebowałby dużego skoku kosztowego (górna granica).

Podsumowanie

Testowanie i walidacja pozostają podstawowym elementem kosztów governance AI, zapewniając, że modele są godne zaufania i zgodne z przepisami, ale wymagają znacznych nakadów pracy ze strony ekspertów i narzędzi.

Analiza	Testowanie stanowi około **36%** wysiłku compliance.
Główne ryzyko	**Dryf:** Zmiany w danych lub na rynku wymagają kosztownego re-testowania.
Dźwignia efektywności	**Pakiety testowe:** Zautomatyzowane potoki testów regresji i biasu.

4 Monitorowanie i bieżące utrzymanie

Szacowany koszt	Zmienny: ~8 tys. € (baza) do 200 tys. €+ (scenariusz złożony) na model/rok.
Charakter wydatku	Powtarzalny koszt operacyjny (OPEX).
Kluczowe działania	Wykrywanie dryfu, zarządzanie incydentami, przeglądy z udziałem ludzi, ponowne trenowanie.
Główny czynnik	Krytyczność modelu, wolumen transakcji oraz stabilność środowiska (dryf koncepcji).

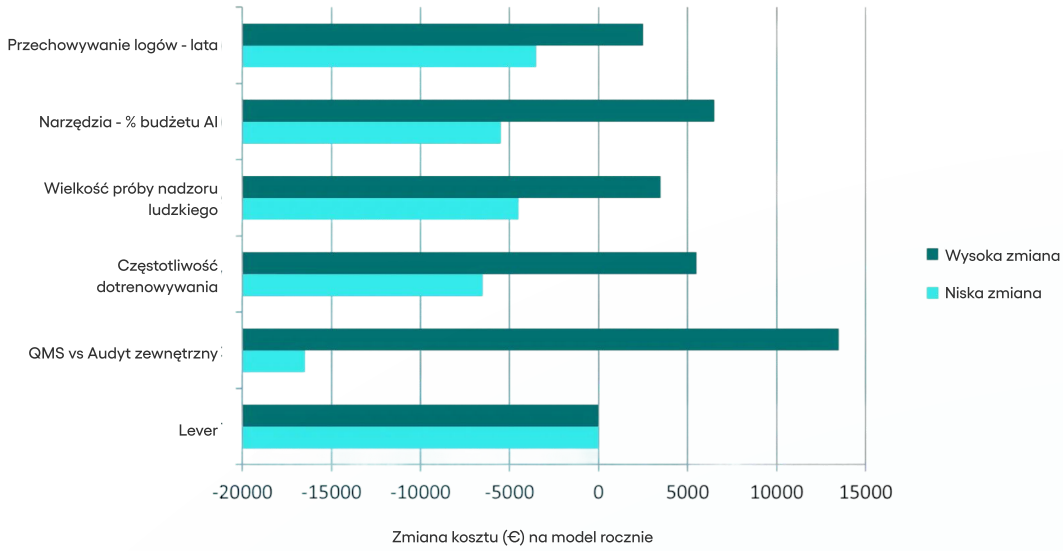
Zakres i potrzeba monitorowania

W momencie wdrożenia modelu AI do procesu bankowego konieczność zaangażowania związanego z governance bynajmniej się nie kończy. Ciągłe monitorowanie i utrzymanie są absolutnie kluczowe, aby zapewnić, że model pozostaje zgodny z przepisami i działa zgodnie z założeniami przez dłuższy czas.

Akt o AI wyraźnie nakłada obowiązek posiadania „systemu monitorowania po wprowadzeniu do obrotu" dla AI wysokiego ryzyka. W praktyce oznacza to, że banki muszą:

- Śledzić wyniki (outputs) i rezultaty działania AI.
- Obserwować system pod kątem oznak spadku wydajności lub niewłaściwego użycia.
- **Umożliwić nadzór ludzki** (np. przegląd próbki zautomatyzowanych decyzji przez ludzi).
- **Obsługiwać wszelkie incydenty lub błędy** (w tym zgłaszać poważne awarie organom regulacyjnym w ściśle określonym czasie).
- **Aktualizować model** lub jego mechanizmy kontrolne w miarę potrzeb.

Działania te generują **powtarzalne koszty rok po roku** – efektywnie tworząc stały koszt operacyjny compliance AI.



Rysunek R-5 — Czynniki wrażliwości wpływające na koszt w przeliczeniu na model; największe odchylenia wynikają ze skali, głębokości monitoringu oraz częstotliwości wydań (release cadence)

Koszty monitorowania: Baza vs. Rzeczywistość

Model oceny skutków UE zawiera pewne elementy monitorowania w ramach wspomnianego wcześniej kosztu pracy „nadzoru ludzkiego" (~7,8 tys. €), co obejmuje zadania takie jak ręczny przegląd decyzji AI i adresowanie problemów. Jednakże doświadczenie branżowe sugeruje, że **rzeczywiste koszty monitorowania mogą być znacznie wyższe** niż ta baza, szczególnie w przypadku systemów AI o znaczeniu krytycznym.

OSTRZEŻENIE O RYZYKU:
Niespodzianka za 200 tys. dolarów

Dobrym przykładem jest analiza oparta na danych Gartnera (scenariusz banku średniej wielkości CostPerform). Wykazała ona, że zapewnienie zgodności z ewoluującymi regulacjami AI dodało około 200 000 dolarów rocznych kosztów poza samym wdrożeniem dla tego banku. Te dodatkowe koszty wynikały w dużej mierze z bieżącej złożoności monitorowania i kontrolowania systemu AI w środowisku produkcyjnym. Ten przykład, choć hipotetyczny, ilustruje, jak utrzymanie zgodności AI „na żywym organizmie" może być o rząd wielkości droższe, niż można by zakładać na podstawie statycznej listy kontrolnej compliance. Znacznie przekracza to unijną bazę ~8 tys. €, uwypuklając przepaść między minimalną zgodnością a solidnymi operacjami w świecie rzeczywistym.

Działania generujące koszty monitorowania

W tej kategorii wyróżniamy kilka składników kosztowych:

1. **Zautomatyzowane systemy monitorowania:**
   Banki często konfigurują zautomatyzowane dashboardy do nawigacyji i alerty do śledzenia wydajności modelu (dokładność, metryki biasu, dryf w dystrybucji danych wejściowych). Budowa i dostrajanie tych systemów wymaga początkowych inwestycji (ujętych w kosztach infrastruktury) oraz bieżących zasobów do przeglądu alertów i ich analizy. Jeśli system zasygnalizuje, że liczba fałszywych alertów w modelu antyfraudowym podwoiła się w danym miesiącu, analityk musi to zbadać.

2. **Wykrywanie dryfu koncepcji (Concept drift):**
   Z czasem zmiany w warunkach ekonomicznych lub zachowaniach klientów mogą spowodować, że model stanie się mniej dokładny. Banki muszą inwestować w narzędzia i analityków, aby wykrywać dryf na wczesnym etapie. Gdy wykryty zostanie dryf lub degradacja, zespół może być zmuszony do rekalibracji lub ponownego przetrenowania modelu, co, jak zauważono wcześniej, wyzwala dodatkowe koszty testowania, a być może nawet drobną re-certyfikację.

3. **Cykle ponownego trenowania:**
   Źródła takie jak 2021.AI podkreślają konieczność budżetowania kilku procent pierwotnego kosztu rozwoju na każdy cykl retrainingu, traktując to jako część bieżącego utrzymania. W praktyce wiele banków planuje roczne przeglądy/rewalidacje modeli, a każdy taki cykl pochłania czas personelu (walidatorów, właścicieli modeli) oraz ewentualnie opłaty dla zewnętrznych recenzentów. Te cykliczne koszty przeglądów, choć rutynowe, zwiększają roczny wydatek na model.

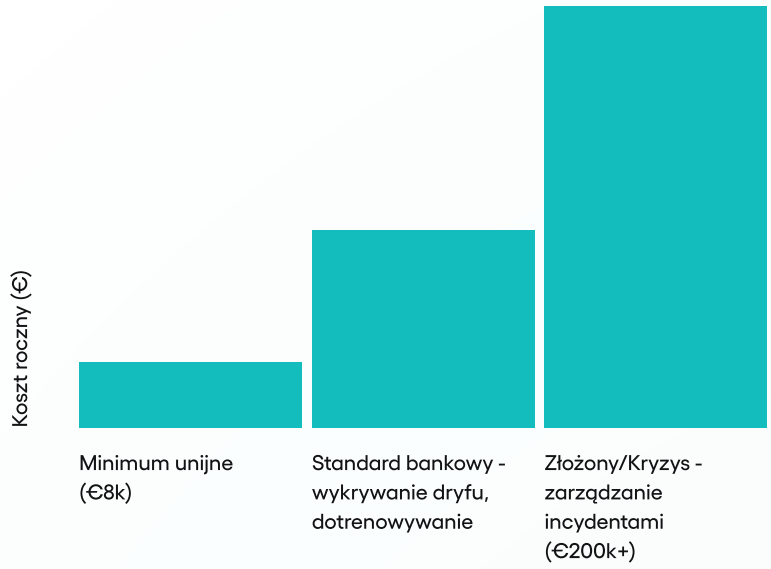
4. **Zarządzanie incydentami:**
   Jeśli system AI spowoduje incydent – np. algorytm transakcyjny popełni błąd lub decyzja kredytowa oparta na AI doprowadzi do skarg klientów na dyskryminację – bank musi to zbadać i udokumentować. Obsługa incydentów często wymaga zwołania komitetu przeglądowego, przeprowadzenia analizy przyczyn źródłowych i podjęcia decyzji o poprawkach, a także raportowania do regulatorów, jeśli jest to wymagane.

5. **Ukryte koszty infrastruktury:**
   Scenariusz CostPerform dobitnie pokazał, że nieprzewidziane potrzeby, takie jak dodatkowa pamięć masowa lub moc obliczeniowa do monitorowania, mogą dodać kolejne 150 tys. dolarów do kosztów rocznych. Kwota ta została przypisana wyższym niż oczekiwano wymaganiom obliczeniowym i przechowywaniu logów monitoringu – efektywnie jest to forma kosztu zapobiegania incydentom. Podkreśla to, że poza bezpośrednią pracą ludzką infrastruktura wspierająca (serwery, koszty chmury dla procesów monitorowania) dokłada się do rachunku za utrzymanie. (Omówimy infrastrukturę w następnej sekcji, ale granica jest płynna, ponieważ potrzeby monitorowania napędzają potrzeby infrastrukturalne).

6. **Aktualizacje i łatki modelu:**
   Częścią kosztu utrzymania jest aplikowanie aktualizacji lub łatek do systemu AI. Na przykład, jeśli wykryty zostanie bias, deweloperzy mogą musieć dostosować model lub dodać mitygację, a następnie wdrożyć go ponownie – generując dodatkową pracę deweloperską i testową. Nie są to zdarzenia jednorazowe; pojawiają się, gdy pojawiają się problemy lub w życie wchodzą nowe regulacje.

7. **Operacje z udziałem człowieka (Human-in-the-loop):**
   W bankowości wiele decyzji AI wciąż podlega nadrzędnej kontroli lub przeglądowi człowieka (np. analityk kredytowy może odrzucić rekomendację AI). Banki często przydzielają personel do regularnego przeglądu wyników AI (np. weryfikując 5% wszystkich odrzuceń kredytowych pod kątem sprawiedliwości). Ten nadzór ludzki to ciągła praca. Jeśli każdy model wymaga 1-2 analityków na część etatu do monitorowania wyników, generuje to stały koszt pracy w przeliczeniu na model.

Ethos.ai zauważa, że organizacje mogą musieć poświęcić ~5% czasu swojej siły roboczej AI na ciągłe szkolenia z governance i rozwój kompetencji (jak wspomniano w Personelu), co jest częścią utrzymania skuteczności procesu monitorowania w miarę ewolucji przepisów. Personel musi być na bieżąco z nowymi listami kontrolnymi compliance lub technikami monitorowania.



The Cost Escalator of Monitoring

Zakres szacunków i kontekst sektorowy

Koszt monitorowania wyraźnie zależy od skali. Nasze źródła wskazują na **zakres od zaledwie ~8 tys. euro na model** (domyślna baza UE dla minimalnych zadań nadzoru) aż do **setek tysięcy euro** rocznie w praktyce dla bardziej złożonych konfiguracji.

Zakres ten zależy od trzech czynników:

- **Krytyczność:** Modele krytyczne dla biznesu uzasadniają intensywniejsze monitorowanie.
- **Wolumen:** Duże wolumeny transakcji wymagają większego logowania i analizy.
- **Dojrzałość:** Stopień zaawansowania istniejącej infrastruktury monitorującej w banku.

Duży bank może zaabsorbować część kosztów monitorowania w ramach istniejących operacji IT (np. podłączając monitorowanie AI do istniejącego pulpitu ryzyka), utrzymując koszty na model bliżej dolnej granicy. Z kolei **mniejszy lub mniej dojrzały cyfrowo bank** może

być zmuszony do budowania procesów i narzędzi monitorowania od zera dla każdego modelu, co sprawia, że pierwsze lata są bardzo kosztowne.

Na szczęście banki posiadają wręcz wrodzoną kulturę monitorowania ze względu na compliance w innych obszarach. Z**espoły operacyjne i pulpity ryzyka** w sposób ciągły śledzą metryki np. jakość portfela kredytowego czy straty z tytułu oszustw. Można je rozszerzyć o metryki modeli AI (indeks dryfu, wskaźnik biasu) przy relatywnie niewielkim nakładzie. Co więcej, banki często praktykują model human-in-the-loop (**człowieka w pętli decyzyjnej) szczególnie przy istotnych decyzjach** (np. brak w pełni zautomatyzowanych odrzuceń kredytowych), co z natury ogranicza działania AI i zapewnia warstwę bieżącego nadzoru ludzkiego przy koszcie krańcowym. Praktyki te mogą w pewnym stopniu redukować koszty nowego monitorowania.

Jednakże w miarę jak banki wdrażają więcej AI i polegają na niej przy decyzjach w czasie rzeczywistym, prawdopodobnie będą potrzebować specyficznych **rozwiązań do monitorowania AI** (np. zautomatyzowane wykrywanie biasu na produkcji, specjalistyczne dzienniki audytowe dla AI).

Podsumowanie

Eksperci są zgodni: utrzymanie zgodności modeli AI to proces długofalowy, wymagający nieustannej uwagi i dedykowanego budżetu. W sektorze bankowym monitorowanie jest kosztem nieuniknionym – modeli podlegających ścisłym regulacjom nie można po prostu wdrożyć i pozostawić bez nadzoru.

Pytanie nie brzmi „czy", ale „jak" to finansować: czy można obniżyć koszty, wykorzystując istniejące systemy, czy konieczne są zupełnie nowe inwestycje? Koszty utrzymania, często niedoszacowane, bywają znaczące. Obejmują one nie tylko oczywiste nakłady na personel nadzorujący modele, ale także ukryte wydatki, takie jak zwiększona przestrzeń dyskowa, moc obliczeniowa niezbędna do ciągłych kontroli oraz zasoby potrzebne do reagowania na incydenty.

Podsumowując, wdrożenie to dopiero początek. Utrzymanie zgodności AI na dużą skalę wymaga ciągłego wysiłku. Dlatego banki planujące budżety powinny, obok kosztów budowy (build costs), uwzględnić odpowiedni bufor na koszty operacyjne (run costs).

Analiza	Koszty monitorowania wahają się drastycznie od **8 tys. € do 200 tys. €** w zależności od złożoności.
Główne ryzyko	**Przeciążenie alertami (Alert Fatigue):** Zbyt wiele ręcznych powiadomień przytłacza personel, prowadząc do ignorowania ryzyk.
Dźwignia efektywności	**Integracja:** Podłączenie monitorowania AI pod istniejące Pulpity Ryzyka (Risk Dashboards) pozwala zaoszczędzić ~30%.

5 Zarządzanie danymi i infrastruktura technologiczna

Szacowany koszt	~2–5% całkowitego budżetu AI (dziesiątki tysięcy na model).
Charakter wydatku	Mieszanka kosztów wstępnych (Narzędzia) i powtarzalnych (Pamięć/Obliczenia).
Kluczowe działania	Rodowód danych, narzędzia do wykrywania biasu, bezpieczne logowanie, inwentaryzacja modeli.
Główny czynnik	Wolumen retencji danych wymagany dla audytowalności i "wyjaśnialności".

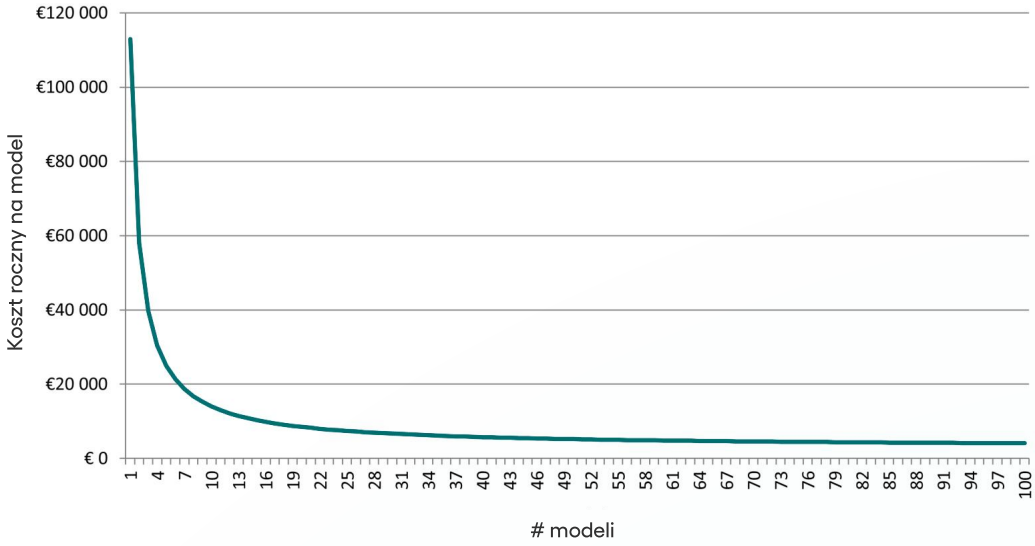
Zakres i potrzeba monitorowania

Fundamentem wszystkich powyższych kategorii są **dane i infrastruktura IT** niezbędna do governance AI. Zgodność to nie tylko ludzie i procesy; wymaga ona również odpowiednich narzędzi, systemów i praktyk zarządzania danymi.

W tej kategorii uwzględniamy:

- **Przygotowanie i ład danych:** Zapewnienie, że dane treningowe i testowe spełniają standardy jakości i reprezentatywności.
- **Oprogramowanie/narzędzia governance:** Do śledzenia modeli, zarządzania dokumentacją, wykrywania biasu itp.
- **Obliczenia i pamięć masowa:** Zasoby potrzebne do wspierania działań compliance (np. uruchamianie dodatkowych zadań walidacyjnych, przechowywanie logów).
- **Infrastruktura bezpieczeństwa/prywatności:** Do ochrony danych i modeli.

Choć koszty te mogą być mniej widoczne niż zatrudnianie personelu, są one wskazywane w wielu raportach jako **kluczowe elementy struktury kosztów** governance AI. Zasadniczo bez odpowiedniej infrastruktury bank musiałby rzucić na problem jeszcze więcej ludzi, co jest rozwiązaniem nieskalowalnym.



Rysunek R-6 — Koszt platformy/narzędzi w przeliczeniu na model spada wraz ze wzrostem wielkości portfela.

Przygotowanie i jakość danych

Akt o AI będzie wymagał od banków zwrócenia bacznej uwagi na **jakość danych treningowych**. Artykuł 10 Aktu nakazuje, aby dane treningowe dla AI wysokiego ryzyka były istotne, reprezentatywne, wolne od błędów „w miarę możliwości" oraz **wolne od uprzedzeń (bias)**, które mogłyby skutkować dyskryminacją. Zapewnienie tego może oznaczać dodatkową pracę: pozyskanie nowych zbiorów danych w celu zrównoważenia biasów, przeprowadzenie obszernego czyszczenia danych i udokumentowanie pochodzenia danych (provenance).

Badanie UE alokuje mniejszą część (**~2 763 euro na model/rok**) na zgodność „Danych Treningowych", co pokrywa zadania takie jak dokumentacja zbiorów danych i ustanowienie środków ładu danych dla AI. Jednakże kwota 2,8 tys. euro rocznie (ok. 9% pracy compliance) sugeruje zaledwie kilka dni pracy inżynierów danych na model rocznie – prawdopodobnie niedoszacowanie, jeśli potrzebne jest poważne pozyskiwanie danych lub etykietowanie.

W rzeczywistych przypadkach, jeśli bank zda sobie sprawę, że zbiór danych jego modelu AI nie posiada reprezentacji pewnych mniejszości, może zainwestować w uzupełniający zbiór danych lub nową inicjatywę zbierania danych, co może kosztować dziesiątki tysięcy w opłatach dla dostawców lub kosztach etykietowania. Jedno ze źródeł (CostPerform) wskazało, że **nieefektywne wykorzystanie pamięci masowej w chmurze dla danych AI doprowadziło do znacznych przekroczeń kosztów (~25% przekroczeń)**, pokazując, że nieefektywności w przechowywaniu i zarządzaniu danymi mogą bezpośrednio uderzyć w wynik finansowy.

Narzędzia i platformy governance

Wiele banków zwraca się ku specjalistycznemu **oprogramowaniu do governance AI**, aby usprawnić compliance. Obejmuje to:

- **Systemy inwentaryzacji modeli:** Do katalogowania wszystkich modeli AI i ich statusu zgodności.
- **Zautomatyzowane narzędzia dokumentacyjne:** Generujące części pliku technicznego.
- O**programowanie do wykrywania biasu:** Do testowania sprawiedliwości.
- **Platformy monitorujące:** Do śledzenia metryk modeli.

Wdrożenie tych narzędzi wiąże się z kosztami licencji lub subskrypcji, kosztami integracji, a być może także niestandardowym rozwojem. Analizy branżowe szacują, że duże przedsiębiorstwa przeznaczają około **2–5% swoich budżetów AI na technologię governance (narzędzia i platformy)**. Dla banku wydającego np. 10 milionów euro na AI oznacza to wydatek rzędu 200–500 tys. euro na narzędzia.

W przeliczeniu na model, jeśli bank posiada 50 modeli, może to średnio wynosić **4–10 tys. euro na model** w kosztach narzędzi. Jeśli modeli jest mniej, udział na model jest proporcjonalnie wyższy. W naszym całkowitym zakresie kosztów 116 tys. – 137 tys. euro ta inwestycja w narzędzia jest jednym z czynników przesuwających koszty w górę.

Banki często stają przed wyborem „zbudować czy kupić" (build vs. buy): duże instytucje mogą rozwijać własne platformy governance (ponosząc koszt deweloperów, ale zyskując elastyczność), podczas gdy inne kupują rozwiązania korporacyjne od dostawców (płacąc za licencje). Tak czy inaczej, jest to nietrywialna pozycja w budżecie. **Bez tych narzędzi compliance polegałoby wyłącznie na pracy ręcznej, co prawdopodobnie kosztowałoby jeszcze więcej w roboczogodzinach**, więc narzędzia są częścią strategii efektywności.

Narzut obliczeniowy i pamięci masowej

Wymogi compliance mogą podnieść **koszty wykorzystania IT** poza to, czego potrzebuje samo rozwiązanie AI. Na przykład, aby zachować zgodność z wymogami przejrzystości i prowadzenia rejestrów, bank może przechowywać **każdy wynik decyzji systemu AI przez X lat** – jeśli model wykonuje miliony predykcji, jest to ogromna ilość danych do zarchiwizowania. Podobnie uruchamianie dodatkowych **zadań walidacyjnych i testów biasu** oznacza dodatkowe godziny obliczeniowe w chmurze lub wykorzystanie serwerów lokalnych.

W scenariuszu banku CostPerform, w miarę jak system AI skalował swoje użycie, bank odnotował wzrost kosztów przetwarzania i przechowywania danych o **20%, co dodało około 600 tys. dolarów rocznie** (choć scenariusz ten obejmował więcej niż tylko narzut compliance). Specyficznie w powiązaniu z compliance odnotowano nieoczekiwane **150 tys. dolarów dodane do budżetu na pamięć masową i obliczenia** ze względu na potrzeby przejrzystości i monitorowania. Wskazuje to, że logowanie każdego szczegółu i utrzymywanie środowisk testowych typu sandbox nie jest darmowe – wymaga miejsca na dysku i cykli CPU. Banki korzystające z usług chmurowych mogą zobaczyć wzrost miesięcznych rachunków, ponieważ przechowują więcej danych i uruchamiają więcej procesów analitycznych, aby zadowolić audytorów.

Możemy przyjąć, że z naszych ponad 100 tys. euro na model pewna część to infrastruktura: być może rzędu **10 tys.+ euro na model rocznie** w dodatkowych kosztach chmury/serwera w aktywnych przypadkach użycia (zależnie od wolumenu danych). Banki muszą to uwzględnić przy uzasadnianiu projektów AI: **całkowity koszt posiadania (TCO)** obejmuje te koszty obliczeniowe compliance.

Infrastruktura bezpieczeństwa i prywatności

Zapewnienie **bezpieczeństwa danych i prywatności** dla systemów AI jest zarówno wymogiem regulacyjnym, jak i dobrą praktyką – i niesie ze sobą koszty. Obejmuje to **szyfrowanie** danych. solidne **kontrole dostępu** (aby tylko upoważniony personel miał dostęp do modelu lub jego danych) oraz monitorowanie pod kątem wycieków danych lub nieautoryzowanego użycia.

Choć pozycje te mogą nie być wyszczególnione jako specyficzne „koszty compliance Aktu o AI", są częścią szerszego wydatku na governance. Na przykład, jeśli AI wykorzystuje dane osobowe, zgodność z RODO (które nadal obowiązuje) oznacza inwestycję w rozwiązania do anonimizacji lub pseudonimizacji oraz ciągłe monitorowanie pod kątem naruszeń danych. Bank może rozszerzyć swoje istniejące narzędzia bezpieczeństwa, aby objąć potoki AI – np. zapewniając, że dane treningowe modelu są przechowywane w bezpiecznym data lake z odpowiednim logowaniem dostępu.

Większość banków dysponuje już znacznymi budżetami na bezpieczeństwo IT, które w pewnym stopniu pokryją także koszty nadzoru nad sztuczną inteligencją (AI governance). Z dostępnych analiz wynika, że część istniejących wydatków można przypisać do wsparcia tego obszaru, na przykład alokując koszty cyberbezpieczeństwa proporcjonalnie do realizowanych projektów AI.

Kluczowe jest jednak zrozumienie, że nawet jeśli infrastruktura nie została zakupiona specjalnie z myślą o sztucznej inteligencji, wykorzystanie jej w tym celu generuje dodatkowe obciążenia. Działania takie jak rotacja kluczy szyfrujących chroniących modele czy dodatkowy monitoring przepływu danych wymagają zwiększonego zaangażowania zespołów IT, co bezpośrednio przekłada się na koszty czasu i pieniędzy.

Kontekst sektorowy i ekonomia skali

Banki – zwłaszcza te największe – dysponują istotną przewagą infrastrukturalną: posiadają już korporacyjne jeziora danych (data lakes), systemy rejestrowania zdarzeń oraz platformy GRC (Governance, Risk, Compliance). Te istniejące zasoby można często zaadaptować na potrzeby sztucznej inteligencji. Przykładowo, system zarządzania ryzykiem operacyjnym można rozszerzyć o rejestrację incydentów związanych z AI, eliminując konieczność budowy nowego narzędzia. Analogicznie, infrastruktura Big Data archiwizująca historię transakcji może służyć również do przechowywania rejestrów decyzji podejmowanych przez algorytmy.

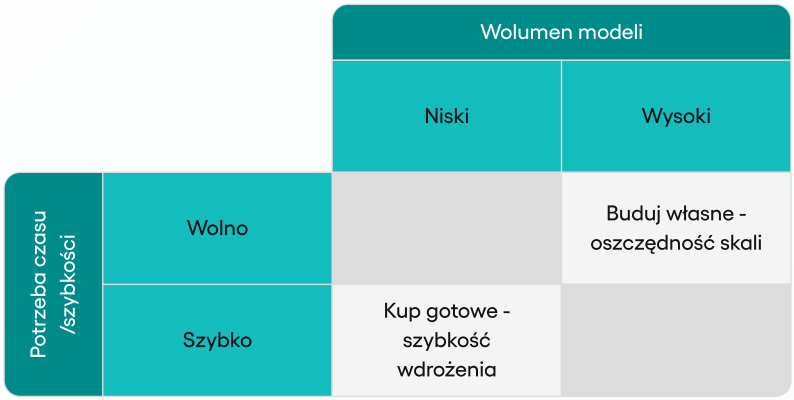
Integracja procesów zgodności (compliance) AI z zastanymi systemami (legacy) pozwala na znaczną redukcję kosztów. Wiele banków posiada już centralne systemy zarządzania ryzykiem modelu (często oparte na zewnętrznym oprogramowaniu do inwentaryzacji), które można dostosować do monitorowania AI. Zapewnia to efekt korzyści skali: im więcej modeli i procesów obsłuży jeden system, tym niższy będzie jednostkowy koszt utrzymania modelu.

Analizy jasno wskazują, że wczesna inwestycja w scentralizowane platformy nadzoru nad AI (AI governance) jest najbardziej efektywna kosztowo. Banki, które podejmą ten krok, mogą utrzymać wydatki na model w dolnych granicach szacunków. Z kolei podmioty działające reaktywnie i wdrażające rozwiązania doraźne (ad-hoc) w odpowiedzi na kolejne wymogi, narażają się na stale rosnące koszty krańcowe. Rachunek jest prosty: wdrożenie platformy za 300 tys. euro przy obsłudze 30 modeli daje koszt 10 tys. euro na model, podczas gdy suma wydatków na rozwiązania cząstkowe może finalnie okazać się znacznie wyższa.

Podsumowanie

Podsumowując, choć koszty infrastruktury i zarządzania danymi rzadziej trafiają na nagłówki niż wydatki na personel czy audyty, stanowią one kluczowy element rachunku ekonomicznego. To właśnie odpowiednie zaplecze technologiczne gwarantuje sprawne funkcjonowanie procesów compliance. Źródła są zgodne – czy to wprost, czy pośrednio – że brak właściwych narzędzi czyni zapewnienie zgodności procesem znacznie bardziej pracochłonnym i kosztownym. Inwestycje w infrastrukturę są więc niezbędne do utrzymania ogólnych wydatków w ryzach, nawet jeśli same stanowią jedynie 10–20% całkowitego budżetu na zgodność.

Z perspektywy planowania menedżerowie powinni traktować te nakłady jako inwestycje wstępne lub koszty stałe (np. zakup oprogramowania, konfiguracja logowania). Charakteryzują się one wysokim kosztem początkowym, ale pozwalają na znaczące obniżenie kosztów krańcowych przy każdym kolejnym modelu. Ci, którzy wcześnie zainwestują w solidną infrastrukturę nadzoru (governance), z czasem odczują stabilizację lub spadek jednostkowych kosztów obsługi modeli. Z kolei banki zwlekające z tymi decyzjami będą musiały mierzyć się z narastającą nieefektywnością operacyjną



Macierz decyzji: Budować czy Kupować

Analiza	Koszty technologiczne stanowią **2-5%** budżetu AI, ale zapobiegają eksplozji kosztów pracy.
Główne ryzyko	**Dług technologiczny:** Narzędzia ad-hoc dla każdego modelu tworzą koszmar integracyjny.
Dźwignia efektywności	**Strategia platformowa:** Wczesna centralizacja narzędzi governance w celu amortyzacji kosztów.

6 Audyt i certyfikacja zgodności

Szacowany koszt	Zmienny: ~20 tys. € (Zewnętrzny/model) vs ~71 tys. €/rok (Utrzymanie wewn. QMS).
Udział w całości	Zależy od strategii (10-20% kosztu na model).
Kluczowe działania	Oceny zgodności, wdrożenie QMS, audyty nadzoru, aktualizacje rejestrów.
Główny czynnik	Strategiczny wybór między modelem "płatność za model" (Zewnętrzny) a "inwestycja wstępna" (Wewnętrzny QMS).

Zakres i oczekiwania regulacyjne

Modele AI wysokiego ryzyka w UE będą podlegać **formalnej ocenie zgodności** przed wprowadzeniem do użytku (oraz okresowo później w niektórych przypadkach). Jest to odpowiednik procesu certyfikacji, zapewniający, że model spełnia wszystkie wymogi Aktu o AI.

Istnieją dwie główne ścieżki do osiągnięcia zgodności:

- **Zewnętrzny audyt strony trzeciej:** Niezależna jednostka notyfikowana ocenia system AI i wydaje certyfikat.
- **Wewnętrzna ocena zgodności poprzez System Zarządzania Jakością (QMS):** Dostawca (np. bank) wdraża kompleksowy QMS i dokonuje samooceny zgodności modelu, pod nadzorem władz.

Obie ścieżki wiążą się z kosztami: albo płaceniem zewnętrznym audytorom, albo inwestowaniem wewnętrznie w ramy QMS. Dodatkowo banki będą stawiać czoła **bieżącym działaniom audytowym**: ich działy audytu wewnętrznego będą włączać AI do rutynowych audytów, a regulatorzy (lub audytorzy zewnętrzni) mogą przeprowadzać **audyty nadzoru lub inspekcje** okresowo. Kategoria ta obejmuje te jednorazowe i powtarzalne koszty oceny, a także narzut utrzymania systemów ułatwiających audyty.

Początkowe koszty certyfikacji (Zewnętrzna vs. QMS)

Badanie wpływu UE dostarcza tutaj konkretnych szacunków.

- **Zewnętrzny audyt „typu UE”:** Koszt oszacowano na **16 800 do 23 000 euro na model** (jednorazowo). Byłaby to opłata uiszczana zewnętrznemu audytorowi za certyfikację modelu jako zgodnego przed wdrożeniem.

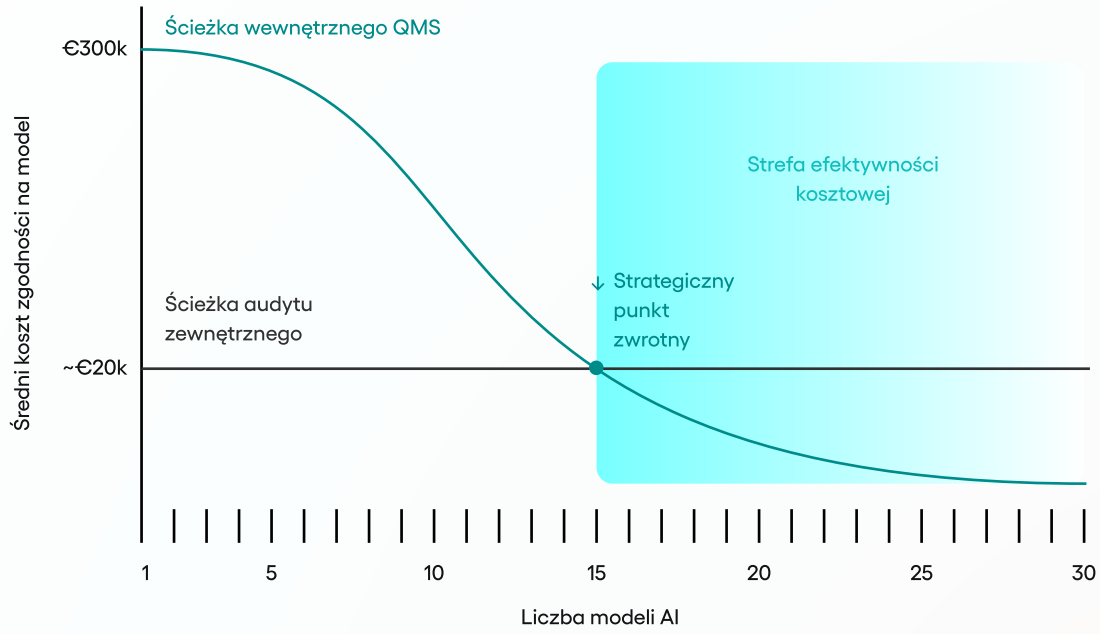
- **Wewnętrzny QMS:** Ustanowienie wewnętrznego QMS dla compliance AI jest znacznie droższe na początku: około **193 000 – 330 000 euro** na skonfigurowanie systemu, plus **71 400 euro rocznie** na jego utrzymanie. Liczby te zostały później potwierdzone przez badaczy CEPS, którzy byli autorami badania, podkreślając, że nowy QMS (obejmujący procesy, systemy dokumentacji, szkolenia itp.) to ogromny wydatek – prawdopodobnie zaporowy dla małych dostawców.

Rzeczywiście logika jest taka, że **mniejsze firmy wybiorą zewnętrzne audyty na model, zamiast ponosić wysoki koszt stały QMS.**

Zakres i oczekiwania regulacyjne

Dla banków obraz ten wygląda inaczej: banki zazwyczaj posiadają już przynajmniej częściowe ramy QMS (np. wiele z nich postępuje zgodnie z ISO 9001 lub posiada systemy zarządzania ryzykiem korporacyjnym). Zatem bank może nie potrzebować budowy za 300 tys. euro od podstaw; zamiast tego może **rozbudować istniejące systemy governance**, aby spełnić kryteria Aktu o AI. Nasze źródła rozwijają tę dynamikę. Analiza personelu Komisji Europejskiej (odnotowana przez CEPS) zakładała, że wiele firm „już spełnia część wymagań jako BAU", stąd bagatelizowanie kosztów netto-nowych QMS.

W praktyce **duży bank z dziesiątkami modeli AI** mógłby rozłożyć koszt wstępny QMS na te modele, czyniąc udział na model relatywnie małym.



Krzywa amortyzacji

Na przykład jednorazowe wdrożenie za 300 tys. euro rozłożone na 30 modeli to 10 tys. euro na model na start, plus być może udział każdego modelu w rocznym utrzymaniu 71 tys. euro (ok. 2,4 tys. euro). Jest to wykonalne i prawdopodobnie znajduje się w dolnym zakresie kosztów na model. Dla kontrastu **mały bank fintech z tylko 1-2 modelami AI** może uznać wewnętrzny QMS za nieuzasadniony i zamiast tego zapłacić ~20 tys. euro na model za certyfikację zewnętrzną.

Ta **dychotomia** wyjaśnia wiele zmienności w szacunkach kosztów w różnych źródłach: niektóre średnie liczby zakładają, że duzi gracze amortyzują koszty (co daje być może poziom ~100 tys. euro ogółem), podczas gdy inni rozważają mniejszych graczy ponoszących pełny pakiet kosztów na jednym modelu (co prowadzi do bardzo wysokich liczb na model).

Rozkładanie i amortyzacja kosztów

Jak zauważono, koszty QMS są w dużej mierze **stałe** – gdy masz solidne ramy governance, dodanie kolejnego modelu nie podwaja kosztu, a jedynie dodaje pracę przyrostową. Nasz zwalidowany zakres kosztów (116 tys. – 137 tys. euro/model/rok) prawdopodobnie **zakłada pewną amortyzację** dla typowych banków. Plasuje się on pomiędzy skrajnymi przypadkami: znacznie powyżej minimalnego scenariusza konserwatywnego 52 tys. euro (gdzie liczono tylko jednorazowy audyt 23 tys. euro + pracę 29 tys. euro), ale poniżej najgorszego przypadku pojedynczego modelu za 400 tys. euro.

Jeden z komentarzy CEPS odniósł się do nieporozumienia: mała firma może stanąć w obliczu do 400 tys. euro za jeden produkt AI wysokiego ryzyka (jeśli wcześniej miała zerowy QMS), ale ich rzeczywiste badanie sugerowało 193 tys. – 330 tys. euro + 71 tys. utrzymania, co w przypadku ponownego wykorzystania dla przyszłych modeli rozkłada się.

Rozkładanie i amortyzacja kosztów

Uzyskanie wstępnej certyfikacji to nie koniec; jej utrzymanie to koszt ciągły. Banki z wewnętrznym QMS będą musiały przechodzić **coroczne audyty nadzoru** przez jednostkę certyfikującą, aby utrzymać aktywność swojej certyfikacji. Muszą również stale **doskonalić QMS**, dedykować personel do zarządzania nim i aktualizować dokumentację w miarę ewolucji przepisów. Kwota 71 tys. euro rocznie za utrzymanie pokrywa prace papierkowe i utrzymanie systemu, ale **nie czas personelu** na faktyczne operowanie w ramach QMS – efektywnie ten czas personelu jest już policzony w kategoriach personelu/dokumentacji.

Mimo to QMS wnosi swój własny narzut administracyjny. Tymczasem banki polegające na audytach zewnętrznych mogą musieć okresowo ponownie certyfikować modele (np. jeśli dokonano dużej zmiany w modelu, nowy audyt może być wymagany). Każdy taki audyt może kosztować podobne ~20 tys. euro. Dodatkowo Akt o AI będzie wymagał **rejestracji systemów AI wysokiego ryzyka w bazie danych UE** i utrzymywania tych wpisów w aktualności. Choć wypełnianie formularzy rejestrowych lub przesyłanie informacji może być drobnym zadaniem, robienie tego dla dziesiątek modeli i utrzymywanie aktualności dodaje do obciążenia pracą compliance (uznajmy to za część narzutu audytowego).

Konsensus w sprawie kosztów certyfikacji (Zróżnicowane, ale znaczące)

Nasze źródła zgodnie przyznają, że **spełnienie wymogu certyfikacji/oceny zgodności jest zauważalnym kosztem**, ale kwantyfikują go różnie w zależności od kontekstu. **Analiza 2021.AI/EY**, którą cytowaliśmy, połączyła zannualizowany koszt certyfikacji z pracą, uzyskując ~52 tys. euro na model rocznie jako sumę „konserwatywną" – to zasadniczo zakładało tańszą ścieżkę (zewnętrzny audyt ~23 tys. euro, nie co roku, ale przy każdej głównej wersji) plus bazową pracę ~29 tys. euro. Dla kontrastu nasza metaanaliza identyfikuje wyższy zakres (116 tys. – 137 tys. euro), ponieważ uwzględniamy **wszystkie kategorie** (personel, infrastrukturę, itp.) – efektywnie dając pełny obraz, a nie tylko pracę i audyt.

Niektórzy eksperci, zwłaszcza z branży, argumentują, że szacunek Komisji (~50 tys. euro) był **zbyt niski**, gdy uwzględni się wszystko. Wspomniany dokument CDI ekstrapolował do **10 miliardów euro rocznie w całej branży** i ~400 tys. euro dla systemu AI MŚP z pełnym QMS. Chociaż było to prawdopodobnie przeszacowanie (i CEPS to odparł), podkreśla to, że **jeśli firma musi na nowo inwestować w systemy governance i wiele audytów, obciążenie na model może drastycznie wzrosnąć**. W rzeczywistości większość banków znajdzie się gdzieś pośrodku: nie tak tanio, jak zakładała Komisja, ale też nie startując od zera.

Integracja z istniejącymi programami audytu

Banki mają tę przewagę, że podlegają już **częstym audytom** – działy audytu wewnętrznego sprawdzają zgodność z różnymi regulacjami, a zewnętrzni regulatorzy przeprowadzają inspekcje. Wiele większych banków planuje **zintegrować compliance AI z istniejącymi cyklami audytowymi.** Na przykład, jeśli bank wykonuje już roczny audyt kontroli wewnętrznych (być może dla wymogów SOX lub podobnych), może go rozszerzyć o kontrole modeli AI przy minimalnym koszcie związanym z przyrostem. Audytorzy wewnętrzni będący na liście płac mogą zostać przeszkoleni, aby uwzględniać punkty kontrolne AI w swoich przeglądach.

Podobnie banki mogą wspólnie opracowywać **współdzielone ramy oceny** (poprzez stowarzyszenia branżowe) w celu standaryzacji audytów AI, co mogłoby zredukować duplikację wysiłku, jeśli regulatorzy zaakceptują te ramy. Praktyki te mogłyby utrzymać bieżące koszty audytu po niższej stronie dla dobrze przygotowanych banków. Niemniej jednak, biorąc pod uwagę, że wiele przypadków użycia AI w bankowości to wysokie ryzyko (kredyty, nadużycia, AML), **regulatorzy prawdopodobnie będą żądać dokładnych audytów**. Banki mogą nadal angażować **ekspertów zewnętrznych** jako dodatkowe zabezpieczenie, zwłaszcza we wczesnych latach, gdy budowana jest ekspertyza wewnętrzna. Firmy konsultingowe takie jak Deloitte oferują już usługi audytu „gotowości do Aktu o AI". Takie zewnętrzne ekspertyzy nie są jednak tanie – mogą być wliczane w budżety projektów lub pojawiać się jako opłaty konsultingowe.

Według analizy Deloitte, banki mogą znacząco zredukować koszty wdrożenia AI Act, adaptując istniejące już ramy zgodności, takie jak RODO. Budowanie nowych procesów od podstaw, zamiast wykorzystania obecnych zasobów, grozi drastycznym wzrostem kosztów i nakładu pracy. Kluczowa zasada brzmi: nie wymyślaj koła na nowo, lecz wykorzystuj to, co już masz

Duzi vs. mali gracze

Podsumowując zakres, spodziewamy się, że **duże banki w UE z dojrzałymi programami compliance** utrzymają koszty certyfikacji w pobliżu dolnych granic – być może **dziesiątki tysięcy euro na model rocznie** (po amortyzacji), co może stanowić zaledwie 10-20% ich całkowitego kosztu compliance na model. W przeciwieństwie do tego **mniej przygotowane organizacje lub te posiadające tylko kilka modeli** doświadczą wyższych kosztów certyfikacji na model (~137 tys. euro lub więcej). Jest to zgodne z naszą wcześniejszą dyskusją na temat ekonomii skali i początkowych obciążeń konfiguracyjnych.

Podsumowanie

Podsumowując, audyt i certyfikacja stanowią istotną, odrębną kategorię kosztową w zarządzaniu AI (AI Governance). Formalizacja zgodności modelu wiąże się z realnymi nakładami finansowymi – zarówno na zewnętrznych audytorów, jak i utrzymanie wewnętrznych struktur compliance. Choć rynkowe analizy są zgodne co do konieczności tych działań, szacunki ich kosztów pozostają zróżnicowane.

Rekomendacja: Banki powinny przyjąć strategię inwestycji w skalowalne systemy compliance. Choć wiąże się to z wyższym kosztem początkowym, zapobiega liniowemu wzrostowi wydatków przy wdrażaniu kolejnych modeli. Głęboka integracja AI z istniejącymi procesami kontroli sprawi, że certyfikacja nowych rozwiązań będzie znacznie tańsza i szybsza

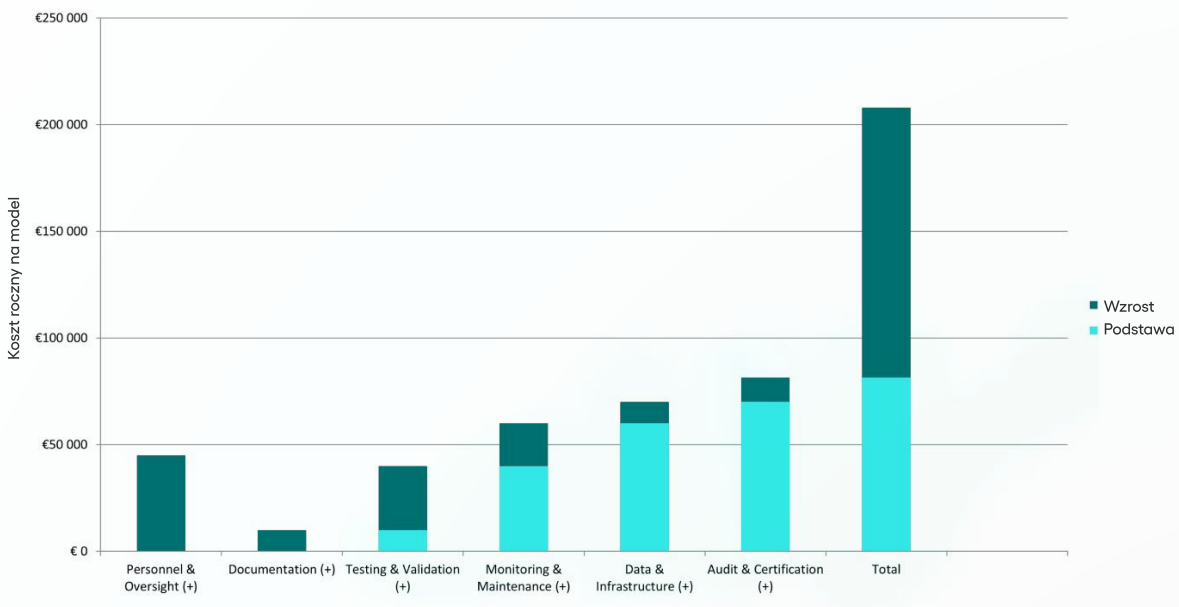
Analiza	Audyt to "Oficjalna Pieczątka". Koszt zależy od wybranej ścieżki (Zewnętrzna vs Wewnętrzna).
Główne ryzyko	**Wąskie gardło:** Niedobór zewnętrznych audytorów może opóźnić uruchomienie modeli.
Dźwignia efektywności	**QMS:** Budowa systemu wewnętrznego jest tańsza dla portfeli >10 modeli.

Dyskusja

Łącząc ustalenia z tych sześciu domen kosztowych, wyłania się **holistyczny obraz** tego, co jest potrzebne – finansowo i operacyjnie – do zarządzania AI w europejskim sektorze bankowym. Istnieje silny konsensus co do tego, **które elementy kosztowe mają kluczowe znaczenie**: praktycznie każde renomowane źródło podkreśla potrzebę (i koszt) następujących obszarów:

- Wykwalifikowany personel
- Kompleksowa dokumentacja
- Rygorystyczne reżimy testowania
- Ramy ciągłego monitorowania
- Wspierająca infrastruktura danych/IT
- Formalne procesy audytu/certyfikacji

Można je postrzegać jako **filary governance AI w bankowości**, a nasza analiza potwierdza, że niosą one ze sobą łącznie **znaczącą cenę**.



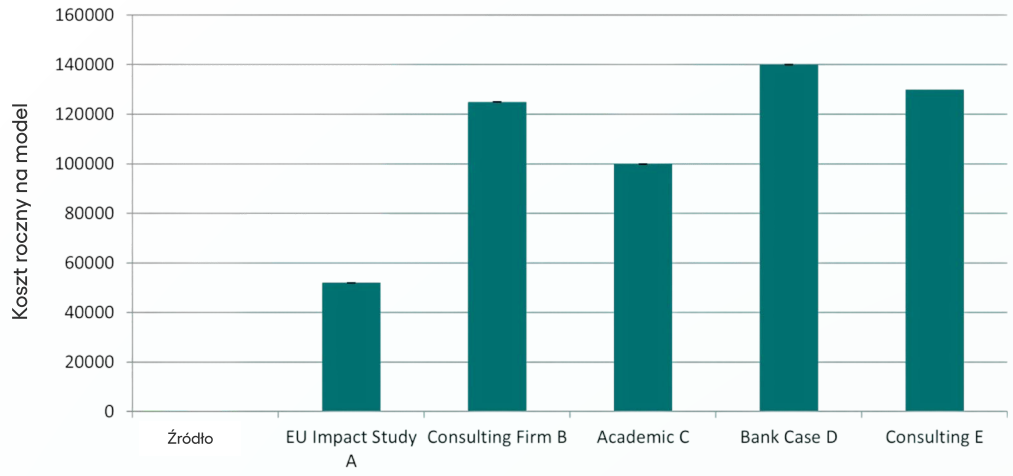
Rysunek D1 — Wykres kaskadowy: od szacunków składowych do poziomu 116–137 tys. EUR rocznie w przeliczeniu na mode

Zbieżność co do całkowitego zakresu kosztów

Jednym z kluczowych wyników tej metaanalizy jest walidacja **rocznego kosztu compliance na model rzędu sześciu cyfr (EUR)**. Wiele niezależnych źródeł wspiera ten rząd wielkości.

Sumując wkład każdej kategorii zgodnie z raportami (i korygując o nakładania się), dochodzimy do zakresu w przybliżeniu od **116 000 do 137 000 euro na model rocznie** na bieżący governance i utrzymanie. Warto zauważyć, że zakres ten nie jest **ani skrajnie wysokim szacunkiem, ani regulacyjnym zaniżeniem** – plasuje się **pomiędzy** konserwatywnymi oficjalnymi liczbami a bardziej ekspansywnymi scenariuszami branżowymi, sugerując, że jest to realistyczny złoty środek.

Na przykład własna analiza UE może sugerować kwotę rzędu ~50 tys. euro na model, jeśli wiele kontroli już istnieje, podczas gdy niektóre scenariusze konsultingowe sugerują kwoty >100 tys. euro (na których się skupiamy), a skrajne przypadki, takie jak projekcja CDI, szybowały do poziomu ~400 tys. euro dla przypadku jednorazowego. Zakres powyżej 100 tys. euro, który prezentujemy, jest zatem **wyważonym szacunkiem**, odzwierciedlającym fakt, że banki prawdopodobnie wdrożą **więcej niż absolutne minimum**, ale też **zyskają efektywność** w porównaniu do najgorszych przypadków nowych podmiotów.



Rysunek D2 — Roczne szacunki kosztów w przeliczeniu na model według źródeł wraz z przedziałami 95%

Weryfikacja krzyżowa pomiędzy źródłami

Znaleźliśmy również weryfikację krzyżową dla konkretnych liczb benchmarkowych w ramach tej sumy. Na przykład:

- **29 tys. euro kosztów pracy compliance** z badania UE znajduje odzwierciedlenie w praktyce banków alokujących 10–20% budżetów AI na compliance (co dla wielomilionowego projektu łatwo przekłada się na dziesiątki tysięcy w kosztach personelu).
- Część dotycząca **nadzoru ludzkiego w kwocie 7,7 tys. euro** pokrywa się z praktyką banków polegającą na dedykowaniu personelu do sprawdzania wyników AI oraz wymogiem Art. 14 Aktu o AI (nadzór ludzki), co wzmacnia tezę, że tysiące na model są wydawane na tę aktywność.

- **Koszt dokumentacji wynoszący 4,4 tys. euro** rezonuje z jakościowymi relacjami zespołów spędzających tygodnie na papierkowej robocie – wiele źródeł, takich jak Ethos.ai, podkreśla, że dokumentacja to około 10–15% wysiłku, więc pasuje to dobrze.
- **Koszt testowania na poziomie 10,7 tys. euro** (36% udziału) pasuje do uwagi Deloitte, że do połowy wysiłku projektowego może iść na compliance/testowanie. Nawet jeśli bank jest efektywny, fakt, że jedna trzecia lub więcej wysiłku compliance idzie na testowanie, nie jest zaskakujący, biorąc pod uwagę normy walidacji modeli.
- **Koszt zgodności danych wynoszący 2,8 tys. euro** jest stosunkowo mały, ale widzieliśmy, że może wzrosnąć, jeśli potrzebne są dodatkowe zbiory danych lub pamięć masowa (niespodzianka 150 tys. dolarów w CostPerform). Zatem o ile podstawowe zadania ładu danych mogą wynosić pojedyncze tysiące, **infrastruktura** wspierająca dane i logowanie może dodać dziesiątki tysięcy (cytowane 2–5% budżetu na narzędzia odpowiada pokaźnym kwotom).
- Analizy konsultingowe konsekwentnie wskazują na wyraźną różnicę kosztową: 20 tys. euro za audyt wobec ponad 200 tys. euro za System Zarządzania Jakością (QMS). Ta powtarzalność danych uwiarygadnia nasze szacunki. Zakładając, że banki będą amortyzować koszty QMS, nasza wycena jednostkowa za model nie jest zawyżona. Duże instytucje nie ponoszą bowiem kosztu 200 tys. euro przy każdym wdrożeniu – jest to inwestycja w infrastrukturę, która obsługuje wiele modeli jednocześnie

Ogólnie rzecz biorąc, zgodność pomiędzy źródłami jest uderzająco silna. Prawie żadne wiarygodne źródło nie argumentowało, że dokumentację lub monitorowanie można pominąć lub zrobić tanio – wszystkie uznają je za konieczne i często kosztowne. Tam, gdzie źródła się różniły, wynikało to głównie z **wielkości i założeń początkowych**.

Przyczyny zmienności szacunków

Różnice w poziomach kosztów w różnych badaniach można w dużej mierze wyjaśnić różnicami **w założeniach dotyczących zakresu, skali i podejściu metodologicznym:**

Czynnik zmienności	Scenariusz niskiego szacunku (~50 tys. €)	Scenariusz wysokiego szacunku (100 tys. – 400 tys. €)
1. Zakres compliance	Patrzy tylko na przyrostowe obciążenie administracyjne.	Kompleksowy widok obejmujący narzut monitorowania i infrastrukturę.
2. Istniejące kontrole (BAU)	Zakłada, że procesy (ISO, Ryzyko) istnieją i można je ponownie wykorzystać.	Zakłada wdrożenie „Greenfield” (start od zera).
3. Czas (Wdrożenie vs Bieg)	Amortyzuje koszty wdrożenia idealnie w czasie.	Łączy skoki „wdrożeniowe” pierwszego roku (np. budowa QMS) z rocznym run-rate.
4. Marginesy bezpieczeństwa	Minimum viable compliance (minimalna zgodność).	Konserwatyzm branżowy: buforowanie na „nieprzewidzianą złożoność”.
5. Wybiórczość (Cherry-picking)	Skupia się na najtańszej ścieżce audytu.	Skupia się na złożonych, wysokiego ryzyka scenariuszach (np. przypadek 400 tys. € wg CDI).

1. Zakres compliance

Niektóre badania patrzyły na podzbiór kosztów (np. tylko przyrostowe obciążenie administracyjne), podczas gdy inne przyjmowały kompleksowy widok. Analiza 2021.AI/EY dająca ~52 tys. euro była explicite „konserwatywnym" częściowym widokiem (tylko koszty rozwoju, bez uwzględnienia retrainingu czy infrastruktury). W przeciwieństwie do tego, nasza analiza uwzględnia te dodatkowe czynniki (narzut monitorowania itp.), stąd wynik ~100 tys. euro+. Konsultanci branżowi często przyjmują bardziej kompleksowy (i czasem pesymistyczny) zakres, wliczając rezerwę na „nieprzewidzianą złożoność", co podnosi ich szacunki.

2. Istniejące kontrole (BAU) vs. Greenfield

Oficjalne szacunki UE zakładały, że wiele praktyk compliance jest już na miejscu (stąd niższy koszt przyrostowy). Na przykład, jeśli bank już posiada procesy zgodne z ISO, spełnienie niektórych wymogów Aktu o AI może oznaczać jedynie ich drobne dostosowanie. Z drugiej strony, analizy wskazujące na wysokie koszty często implicite rozważają firmy, które muszą wdrażać wiele rzeczy od zera. Ten czynnik BAU jest kluczowy: nasza sekcja wniosków zauważyła, że różnice w dużej mierze odzwierciedlają skalę i punkt wyjścia.

- **Duże banki** = wysoka zdolność bazowa, co oznacza umiarkowane nowe koszty na model;
- **Mali/nowi gracze** = niska baza, co oznacza wysokie koszty początkowe.

3. Koszty jednorazowe vs. powtarzalne i pierwszy rok vs. faza stabilizacji

Niektóre źródła (jak krytyka CDI) łączyły koszty wdrożenia pierwszego roku z rocznymi kosztami bieżącymi, prowadząc do sensacyjnych liczb (nagłówek o „30 miliardach euro do 2025 roku"). CEPS wyjaśnił, że było to przeszacowanie częściowo przez nierozłożenie kosztów w czasie lub nieuwzględnienie faktu, że tylko 10% AI to wysokie ryzyko. W fazie stabilizacji, gdy systemy są już na miejscu, koszty na model prawdopodobnie nieco spadają.

Nasza analiza stara się odzwierciedlić roczny koszt w fazie stabilizacji. Warto jednak zauważyć, że w **początkowych latach zgodności z Aktem o AI (np. 2025–2026)** banki mogą ponieść dodatkowe koszty „wdrożeniowe" ponad te roczne liczby, ustanawiając ramy i szkoląc personel. Na przykład bank może wydać dużą sumę ryczałtową na nowy system inwentaryzacji modeli lub zewnętrznych konsultantów, aby uruchomić compliance – nie będą to wydatki powtarzające się co roku. Zatem nasze ~100 tys. euro+ rocznie to średni wskaźnik bieżący; pierwszy rok dla danego banku lub modelu może być wyższy (być może podwójnie, jeśli potrzebna jest pełna budowa QMS), co następnie spada w kolejnych latach. Ten wgląd może być ważny dla budżetowania: inwestycja początkowa vs. koszty bieżące.

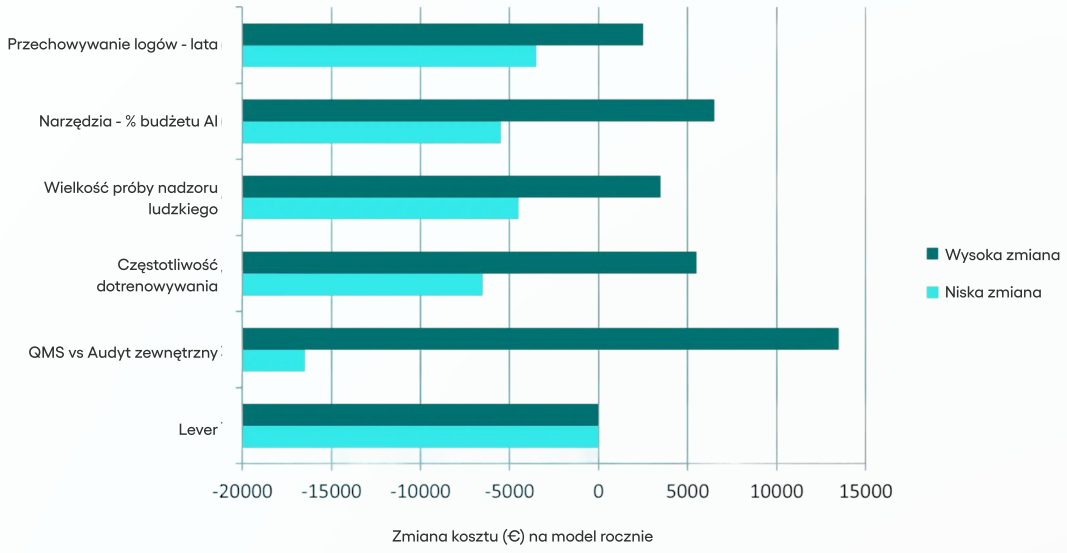
4. Konserwatyzm i „Marginesy bezpieczeństwa"

Kultura zarządzania ryzykiem w branży często dodaje bufory do szacunków kosztów jako zabezpieczenie przed nieznanymi wyzwaniami. Na przykład niektóre banki mogą celowo prze-budżetować compliance, aby uniknąć niedoborów, podczas gdy Komisja (starając się nie wyolbrzymiać obciążeń) dostarczyła raczej minimalne szacunki. Nasz zakres 116–137 tys. euro może implicite zawierać pewien margines bezpieczeństwa, ponieważ wynika z sumowania solidnych praktyk w różnych kategoriach. Zakłada on na przykład, że banki wdrożą dość kompleksowe monitorowanie, a nie tylko absolutne minimum. Jeśli bank wybrałby absolutne minimum (tylko to, czego regulatorzy explicite wymagają i nic więcej), mógłby operować na dolnym końcu zakresu lub poniżej. Ale niesie to ryzyko, jeśli coś pójdzie nie tak, co nie było monitorowane.

5. Wybiórczość vs. Triangulacja

Pytanie przestrzegało przed wybiórczym traktowaniem punktów danych bez walidacji. Napotkaliśmy przykład: jedno źródło podało „29 300 euro za pracę compliance" – zwalidowaliśmy to z innymi źródłami: procent budżetu wg Accenture i Deloitte implikują podobną skalę (jeśli 10–20% wielomilionowego projektu, to łatwo wychodzi kilkadziesiąt tysięcy w pracy). Podobnie „71 400 euro za utrzymanie QMS" zostało sprawdzone krzyżowo z CEPS, który to potwierdził. Ta triangulacja daje pewność co do tych liczb. Z drugiej strony, roszczenie **CDI o 400 tys. euro** zostało skonfrontowane z oryginalnymi liczbami CEPS, które były niższe, więc potraktowaliśmy 400 tys. euro jako wartość odstającą mającą zastosowanie tylko do bardzo wąskiego scenariusza (mała firma, pierwszy model) – nie jako liczbę uogólnialną dla banków (zwłaszcza dużych banków).

Nasze podejście oparte na metaanalizie z natury unika wybiórczości poprzez łączenie wielu odniesień dla każdego twierdzenia. Jeśli jedna firma konsultingowa raportuje bardzo wysoki koszt w jednej kategorii, zestawiamy go z być może oficjalnym szacunkiem lub szacunkiem innej firmy, aby pokazać kontekst. Na przykład, jeśli CostPerform podał 200 tys. dolarów za monitorowanie, zauważamy również, że oficjalna baza wynosiła 8 tys. euro, a następnie wyjaśniamy, dlaczego istnieje taka luka. Zapewnia to bardziej zniuansowane zrozumienie: te 200 tys. dolarów to nie rzeczywistość każdego modelu, ale przestroga, jak sprawy mogą eskalować, jeśli zostaną niedoszacowane.



Rysunek R-5 — Czynniki wrażliwości wpływające na koszt w przeliczeniu na model; największe wahania wynikają ze skali, głębokości monitoringu oraz częstotliwości wydań (release cadence).

Kontekst specyficzny dla sektora

Skupiając się na bankach w UE, pojawiło się kilka tematów, które mogą nie mieć zastosowania do innych sektorów:

- **Istniejący rygor:**
  Wcześniejsza rygorystyczna kultura compliance w bankach (dzięki regulacjom finansowym) zarówno pomaga, jak i szkodzi. Pomaga, bo banki mogą adaptować istniejące systemy (więc koszt przyrostowy jest nieco zredukowany). Szkodzi, bo oczekiwania bazowe są już wysokie – regulatorzy nie dadzą bankom taryfy ulgowej; będą oczekiwać zarządzania ryzykiem AI na poziomie state-of-the-art, tak jak robią to dla ryzyka kredytowego czy operacyjnego. Zatem banki nie mogą przyjąć lekkiego podejścia bez ryzyka reputacyjnego lub regulacyjnego. Oznacza to, że w przeciwieństwie do startupu, bank prawdopodobnie wdroży większość kontroli w stopniu dokładnym, generując tym samym znaczne koszty. W istocie kultura compliance sektora bankowego oznacza, że **governance AI staje się rozszerzeniem istniejącego złożonego governance**, a nie czymś traktowanym pobieżnie.

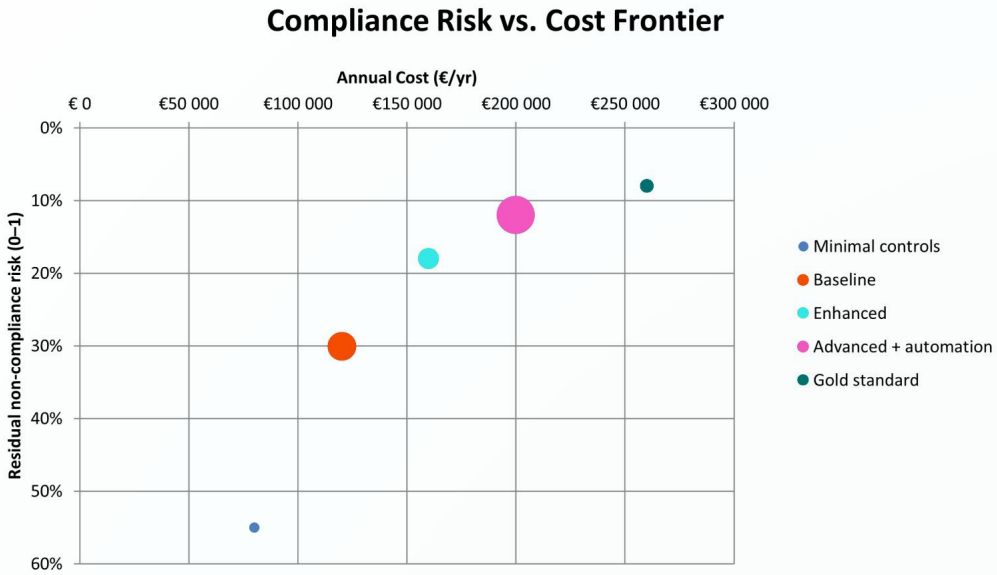
- **Wykorzystanie ram ryzyka modelu:**
  Wiele dużych banków posiada już inwentarz modeli, jednostki walidacji modeli, cykle okresowych przeglądów itp. Jest to przewaga – na przykład bank może nie potrzebować zatrudniania całego nowego zespołu „walidatorów AI", jeśli jego obecni walidatorzy modeli mogą obsłużyć modele AI (po przeszkoleniu). Wspomnieliśmy, jak to nakładanie się może ograniczać przyrostowe koszty związane z personelem. W naszych szacunkach zakładamy, że banki wykorzystają ten mechanizm; gdyby tego nie zrobiły, koszty byłyby wyższe. Na przykład bank prowadzący oddzielną, równoległą strukturę governance dla AI, odrębną od istniejącego zarządzania ryzykiem, duplikowałby wysiłki (niektóre wczesne raporty pokazują, że banki tworzą „Komitety Etyki AI" oddzielne od komitetów ryzyka – co może być konieczne początkowo, ale idealnie powinno stopić się z ogólnym governance, aby oszczędzić koszty).

- **Regulacje w UE:**
  Od 2025 roku Akt o AI w UE zbliża się do wdrożenia (prawdopodobnie egzekwowalny do 2026 roku). Banki są wśród organizacji przygotowujących się wcześnie (niektóre już **przeprowadzają oceny gotowości do Aktu o AI** w 2024 roku). Ta proaktywna postawa oznacza, że niektóre koszty compliance są ponoszone teraz, nawet zanim prawo wejdzie w życie – np. banki inwestujące w audyty pilotażowe lub analizy luk. Nasza analiza ujmuje koszt w fazie stabilizacji (gdy compliance jest osiągnięte); jednak w Dyskusji warto zauważyć, że **lata 2024–2025 mogą przynieść skoki wydatków, gdy banki przygotowują się na nadejscie Aktu o AI**. Aktywność firm doradczych, takich jak Deloitte czy EY, potwierdza, że banki są gotowe inwestować już teraz, aby uniknąć zaskoczenia w przyszłości. To zjawisko różnicuje przewidywane koszty wdrożenia. Dla instytucji, które sukcesywnie budowały swoje kompetencje, koszty te znajdą się w dolnym przedziale szacunków. Z kolei banki, które zwlekały z adaptacją, w momencie wejścia przepisów w życie muszą liczyć się z gwałtownym, skokowym wzrostem wydatków

Implikacje dla kadry zarządzającej banków

Dla kadry zarządzającej (grupa docelowa), implikacje są jasne: **zarządzanie AI nie jest tanie**, ale jest konieczne. Powinni planować **sześciocyfrowe roczne koszty na każdy model AI wysokiego ryzyka** w ramach narzutu compliance. Dla banku wdrażającego dziesiątki modeli AI przekłada się to na wielomilionowe wydatki na governance. Może się to wydawać obciążające, ale jest spójne z tym, co te modele mogą wygenerować w wartości (np. AI do wykrywania nadużyć może zaoszczędzić miliony na stratach z oszustw – uzasadniając solidny wydatek na governance, aby zapewnić, że jest niezawodne i bezstronne).

Dyrektorzy mogą również wynieść wniosek, że **inwestycje w infrastrukturę i procesy mogą się opłacić długoterminowo** poprzez redukcję kosztów krańcowych: np. budując solidny QMS lub kupując dobrą platformę governance raz, a następnie czerpiąc korzyści z niższych kosztów na model. Inny punkt strategiczny: **współpraca i ponowne wykorzystanie**. Ponowne wykorzystanie istniejących struktur compliance (procesy RODO, ramy ryzyka modelu itp.) może materialnie obniżyć koszty. Współpraca poprzez organy branżowe w celu dzielenia się najlepszymi praktykami lub nawet wspólnego finansowania pewnych narzędzi compliance (być może przez konsorcja) mogłaby być korzystna.



Rysunek D3 — Krzywa kompromisu: od wariantu „minimum viable" do kompleksowego governance.

Ryzyko niedoinwestowania

Warto omówić fakt, że o ile koszty te są znaczące, koszt braku zgodności może być wyższy. Akt o AI przewiduje dotkliwe grzywny (do 30 mln euro lub 6% obrotu za poważne naruszenia). Zatem bank, który próbuje oszczędzać pieniądze, skąpiąc na governance, może stanąć w obliczu kar znacznie przekraczających koszty compliance, nie wspominając o szkodach reputacyjnych. W tym sensie wielu dyrektorów postrzega te koszty governance jako ubezpieczenie i ochronę licencji organizacji na działanie. Te nastroje odzwierciedla raport Accenture – 77% dyrektorów traktuje regulacje AI priorytetowo. Wskazuje to na racjonalną kalkulację biznesową: lepiej wydać środki na prewencję, niż mierzyć się z kosztownymi konsekwencjami braku przygotowania.

Niepewności i perspektywy na przyszłość

Wciąż istnieje wiele niewiadomych, które mogą zmienić tę dynamikę kosztów. Na przykład, jeśli pojawią się wytyczne upraszczające compliance dla banków (być może uznające, że istniejący nadzór bankowy może pokryć niektóre aspekty Aktu o AI), może to zredukować koszty. Z drugiej strony, jeśli wystąpią głośne incydenty, regulatorzy mogą zażądać jeszcze bardziej rygorystycznego nadzoru (podnosząc koszty). Postęp technologiczny może również pomóc: lepsza automatyzacja governance AI może zredukować potrzeby pracy ludzkiej (niektórzy dostawcy twierdzą, że automatyzują dokumentację lub wykrywanie biasu, potencjalnie tnąc godziny pracy). W perspektywie kilku lat przewidujemy wzrost efektywności kosztowej, wynikający z dojrzewania procedur i rozwoju narzędzi wspierających. Może to doprowadzić do stabilizacji, a nawet nieznacznego spadku jednostkowego kosztu obsługi modelu. Należy jednak pamiętać o kluczowym ryzyku: potencjalne oszczędności mogą zostać całkowicie skonsumowane przez rosnącą złożoność technologii. Generatywna sztuczna inteligencja (GenAI) wymaga bowiem znacznie bardziej zaawansowanego nadzoru niż tradycyjne algorytmy uczenia maszynowego

Wyłączność dla bankowości

Choć nasza analiza skupia się na bankowości, warto odnotować istotną różnicę względem sektora technologicznego (Big Tech). Banki ponoszą nieproporcjonalnie wyższe koszty compliance ze względu na rygorystyczne otoczenie prawne (m.in. wymogi Bazylei, audyt wewnętrzny, ścisłe RODO). Firmy technologiczne, działając w luźniejszym reżimie regulacyjnym, mogą wdrażać AI taniej – przynajmniej do momentu, gdy prawo je dogoni. Nasze szacunki odzwierciedlają więc specyficzną dla bankowości "wysoką poprzeczkę" regulacyjną.

Należy również uściślić, że wewnątrz banku koszty różnią się w zależności od zastosowania. Proste narzędzia marketingowe (niskie ryzyko) wymagają mniejszego nadzoru niż systemy kredytowe. Nasz model koncentruje się jednak na systemach wysokiego ryzyka (High-Risk AI), ponieważ to one stanowią trzon najbardziej wpływowych wdrożeń w sektorze.

Wnioski dla kadry zarządzającej Koszty compliance nie powinny być traktowane jako jednorazowa przeszkoda, lecz jako stała inwestycja w budowę godnej zaufania sztucznej inteligencji (Trustworthy AI). Narracja rynkowa ewoluuje: solidny governance przestaje być postrzegany jako koszt, a staje się przewagą konkurencyjną. Banki, które skutecznie zarządzają ryzykiem, zyskują zaufanie klientów i mogą szybciej skalować innowacje. Zgodność z regulacjami daje pewność działania, podczas gdy jej brak grozi paraliżem decyzyjnym lub stratami wizerunkowymi.

Wnioski końcowe

Walidacja zakresu kosztów
(116 tys. – 137 tys. € na model/rok)

Podsumowując, przeprowadzona metaanaliza wskazuje, że europejskie banki muszą liczyć się z kosztami rzędu kilkuset tysięcy euro rocznie na nadzór (governance) i utrzymanie cyklu życia każdego systemu AI wysokiego ryzyka. Szacunki te znajdują silne oparcie w danych rynkowych – potwierdza je spójność wniosków płynących zarówno z analiz regulacyjnych, jak i raportów wiodących firm doradczyc

Drobne różnice w szacunkach między źródłami sprowadzają się w dużej mierze do zakresu i skali: oficjalne analizy zakładają, że wiele kontroli jest już na miejscu (co daje niższe szacunki, ~50 tys. euro/model w idealnych scenariuszach), podczas gdy oceny branżowe i konsultingowe biorą pod uwagę bardziej kompleksowe lub najgorsze przypadki wdrożeń (przesuwając koszty powyżej 100 tys. euro/model). Nasz zwalidowany zakres plasuje się pomiędzy tymi skrajnościami, włączając wszystkie główne składniki kosztowe.

Kluczowe czynniki kosztotwórcze

Co istotne, **wszystkie źródła zgadzają się co do kluczowych czynników kosztotwórczych.** Niemal każde badanie podkreśla znaczenie – i koszt – następujących filarów:

- **Wykwalifikowany personel i nadzór:** Ludzcy eksperci (oficerowie compliance, menedżerowie ryzyka, data scientists) i komitety governance są niezbędni, tworząc kręgosłup wysiłków compliance AI.
- **Solidna dokumentacja:** Utrzymywanie szczegółowej dokumentacji technicznej i ścieżek audytu jest pracochłonne, ale powszechnie uznawane za kluczowe dla rozliczalności.

- **Rygorystyczne testowanie i walidacja:** Ciągła walidacja techniczna (pod kątem dokładności, biasu, odporności) jest znaczącym bieżącym wydatkiem, postrzeganym jako niezbędny do spełnienia standardów zarówno regulacyjnych, jak i etycznych.

- **Ciągłe monitorowanie:** Systemy i procesy do monitorowania wydajności AI na produkcji i zarządzania incydentami są nienegocjowalnym kosztem, który rośnie wraz ze złożonością modeli.

- **Dane i infrastruktura:** Inwestycja w jakość danych, bezpieczne potoki i narzędzia governance jest potrzebna, aby umożliwić sprawne compliance; bez tego koszty personelu poszybowałyby w górę.

- **Audyt i certyfikacja:** Formalne oceny zgodności (czy to przez audyty zewnętrzne, czy wewnętrzny QMS) niosą ze sobą znaczne koszty, a banki muszą budżetować zarówno certyfikacje wstępne, jak i bieżące.

Czynnik skali

Różnice w poziomach kosztów wynikają głównie ze zdolności banku do rozkładania kosztów stałych i wykorzystywania istniejących ram. Duży bank może amortyzować jednorazowe inwestycje w compliance (takie jak QMS lub korporacyjny system monitorowania) na wiele modeli AI, spychając koszty na model w stronę dolnej granicy. W przeciwieństwie do tego mniejszy gracz wdrażający governance dla pojedynczego systemu AI może ponieść pełny pakiet kosztów dla tego jednego modelu – uderzając w górną granicę lub nawet ją przekraczając (zwłaszcza w pierwszym roku, jeśli pełna konfiguracja governance jest budowana od zera).

Czynniki specyficzne dla sektora również odgrywają rolę: istniejąca infrastruktura compliance banków i rygorystyczne zasady zarządzania ryzykiem modelu oznaczają, że niektóre potrzebne działania (np. dokumentacja modelu, walidacja) są już częścią business-as-usual i są budżetowane, łagodząc nowe koszty. Jednakże te same czynniki ustawiają **wysoką poprzeczkę**, której governance AI musi dorównać, zapewniając, że nawet przy synergiach koszty przyrostowe pozostają znaczące – po prostu nie ma opcji „lekkiego podejścia" (light-touch) dla AI wysokiego ryzyka w bankowości.

Ostatni wniosek

Dla kadry zarządzającej wniosek jest jasny: zarządzanie AI to **poważna, ciągła inwestycja.** Kwoty rzędu **ponad 100 tys. euro na model rocznie** powinny być włączone do kalkulacji ROI i planowania projektów dla inicjatyw AI. W wielu przypadkach te koszty governance będą reprezentować **10–20% (lub więcej) całkowitego kosztu projektu AI.**

Dla zarządów banków kluczowa jest zmiana perspektywy: wydatki na governance to nie opcjonalny dodatek, lecz fundamentalny koszt prowadzenia biznesu opartego na AI – analogiczny do rezerw kapitałowych przy udzielaniu kredytów czy budżetów na cyberbezpieczeństwo w bankowości cyfrowej.

Patrząc w przyszłość, wejście w życie AI Act przyniesie większą jasność dotyczącą regulacji, co pozwoli bankom na standaryzację i optymalizację procesów. Istotną rolę odegra tu współpraca branżowa (w ramach federacji czy organów normalizacyjnych), która pozwoli uniknąć powielania pracy nad tymi samymi rozwiązaniami. Równie ważna będzie technologia: rozwój narzędzi wspierających governance (np. automatyczne generowanie dokumentacji czy monitoring oparty na AI) pomoże wyhamować dynamikę wzrostu kosztów compliance.

Biorąc pod uwagę kluczowe znaczenie AI w bankowości – jej wpływ na klientów, stabilność finansową i reputację instytucji – zarówno regulatorzy, jak i banki stawiają na rygor, a nie na oszczędności. Nasza metaanaliza potwierdza, że solidny ład korporacyjny (governance) AI w Unii Europejskiej jest przedsięwzięciem kosztownym, ale w pełni uzasadnionym i popartym szerokim konsensusem rynkowym.

Inwestycja w governance to coś więcej niż spełnienie wymogów prawnych – to budowa fundamentu pod godną zaufania sztuczną inteligencję (Trustworthy AI). Szacowany roczny koszt rzędu 116 tys. – 137 tys. euro na model należy traktować jako polisę bezpieczeństwa, gwarantującą sprawiedliwość i rozliczalność systemów. Jak wskazują raporty branżowe, możliwe jest przekucie compliance w przewagę konkurencyjną, ale wymaga to najpierw zaakceptowania i sfinansowania realnych kosztów nadzoru. Banki powinny zatem uwzględniać te kwoty w budżetach nie jako zbędny ciężar, lecz jako zobowiązanie do etycznego i skutecznego wdrażania technologii przyszłości.