SPEEDNET

Poradnik

Moja firma wdrożyła system AI i co dalej?

Oto 9 elementów AI Governance, o których nie możesz zapomnieć.

Spis treści

Executive Summary 3

Wprowadzenie 4

Nowa rzeczywistość po wdrożeniu AI 5

9 kluczowych filarów dojrzałego zarządzania AI 6

- Wizualizacja modelu 9 filarów 6

ETAP I: Budujemy fundamenty i przejmujemy kontrolę 7

- Filar 1: Ustanawiamy ramy organizacyjne i odpowiedzialność 8
- Filar 2: Wdrażamy ład danych 10
- Filar 3: Rozwijamy kulturę organizacyjną i świadomość etyczną 12
- Filar 4: Wdrażamy nadzór technologiczny 14

ETAP II: Wdrażamy strategię i zarządzamy ryzykiem 16

- Filar 5: Wdrażamy proaktywne zarządzanie ryzykiem 17
- Filar 6: Wdrażamy niezależną weryfikację i audyt 19
- Filar 7: Zapewniamy zgodność z ramami prawnymi 21

ETAP III: Optymalizujemy i weryfikujemy 23

- Filar 8: Mierzymy efektywność i optymalizujemy nadzór 24
- Filar 9: Weryfikujemy strategię i zwrot z inwestycji (ROI) 26

Wnioski i rekomendacje strategiczne 28

Następny krok: Droga do zautomatyzowanego zarządzania 29

Bibliografia i dodatkowe źródła 30

O firmie Speednet 31

Executive Summary

Gwałtowna adopcja sztucznej inteligencji odkrywa przed nami pewien paradoks: mimo ogromnych inwestycji, średni zwrot z wdrożeń AI pozostaje na zaskakująco niskim poziomie, który obecnie wynosi zaledwie 5,9%.

Jak pokazują liczne przykłady z rynku, głównym winowajcą takiego stanu rzeczy jest nieefektywne zarządzanie. Brak solidnych instrumentów do AI Governance naraża firmy na straty finansowe, przestoje operacyjne i dotkliwe kary wynikające z braku zgodności z regulacjami, które mogą sięgnąć nawet 7% globalnego obrotu firmy.

Te ryzyka przekładają się na bardzo konkretne koszty: niekontrolowane użycie AI przez pracowników podnosi średni koszt naruszenia bezpieczeństwa o 670 000 dolarów, a roczny, manualny koszt utrzymania zgodności pojedynczego systemu wysokiego ryzyka z unijnym AI Act to wydatek rzędu 116 000 - 137 000 euro. W rezultacie wiele inicjatyw AI, zamiast generować zyski, staje się ukrytym źródłem wydatków, które w efekcie obniża wartość początkowej inwestycji

Ten paraliż pokazuje jak na dłoni, że tradycyjne, reaktywne modele zarządzania ryzykiem są niewystarczające w obliczu AI. Staje się więc jasne, że organizacje na całym świecie pilnie potrzebują nowego, systemowego podejścia, aby pogodzić innowacyjność z bezpieczeństwem.

W odpowiedzi na te palące wyzwania, przedstawiamy konkretny plan działania – sprawdzony model 9 Filarów AI Governance.

Pokazujemy krok po kroku, jak przejąć kontrolę nad sztuczną inteligencją w firmie – od uporządkowania chaosu po pełną optymalizację. Udowadniamy jednocześnie, że zarządzanie AI nie musi być wyłącznie kosztownym obowiązkiem, ale może stać się narzędziem do szybszego i bezpieczniejszego wprowadzania innowacji.

Wprowadzenie

Paradoks inwestycji w AI. Dlaczego ogromne wydatki nie przekładają się na zyski?

Wdrożenie sztucznej inteligencji to dopiero początek. Prawdziwe wyzwanie polega na skutecznym zarządzaniu tą technologią, co wymaga zapewnienia odpowiedniego nadzoru i działania w zgodzie z nowymi regulacjami. Ten raport pokazuje, jak dzięki dojrzałemu zarządzaniu AI firmy budują realną i trwałą przewagę konkurencyjną.

Chociaż adaptacja AI postępuje gwałtownie – według Stanford HAI technologię tę wdrożyło już **78% organizacji** – to dane rynkowe pokazują fundamentalną sprzeczność. Jak wskazują badania IBM, średni zwrot z inwestycji w inicjatywy AI wynosi zaledwie **5,9%**. Pojawia się więc rozdźwięk między tempem wdrażania AI a poziomem przygotowania organizacji. W efekcie ta luka w zarządzaniu wprost przekłada się na realne straty finansowe.

Zaniedbania w zarządzaniu sztuczną inteligencją pociągają za sobą wiele zagrożeń, w tym finansowych. Potwierdzają to dane z raportu IBM, według których niekontrolowane wykorzystanie narzędzi AI przez pracowników skutkuje wzrostem średniego kosztu naruszenia bezpieczeństwa o **670 000 dolarów**. Równolegle, nowe regulacje, takie jak unijny AI Act, wprowadzają dotkliwe sankcje finansowe. Analiza firmy Holistic AI pokazuje, że mogą one sięgać nawet **35 milionów euro** lub **7% globalnego obrotu firmy**.

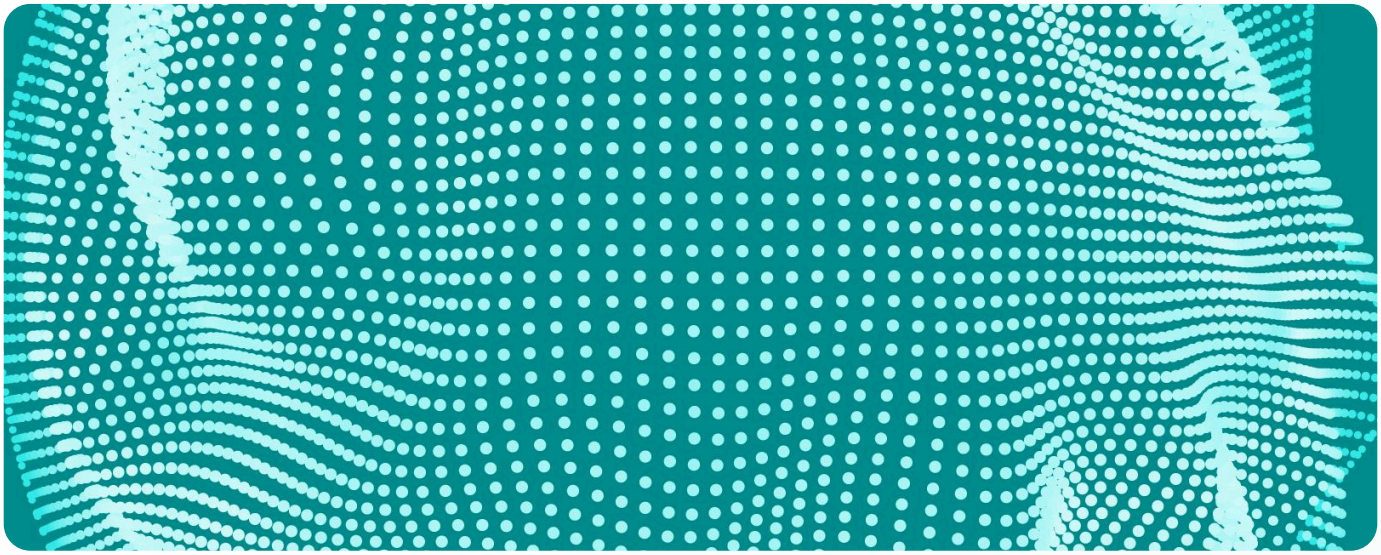
Poza karami nie mniejszym problemem są ukryte koszty związane z nieefektywnością. Zgodnie z analizą Speednet*, średni roczny koszt utrzymania zgodności z przepisami jednego systemu AI wysokiego ryzyka w unijnym sektorze bankowym wynosi od **116 000 do 137 000 euro**. Największą część tej kwoty - bo około **36%** - firmy przeznaczają na testowanie i walidację modeli.

Te liczby, zwielokrotnione przez liczbę systemów w organizacji, jasno pokazują, że manualne podejście do zarządzania jest nie tylko ryzykowne, ale i finansowo nieopłacalne.

W tym dokumencie przedstawiamy 9 kluczowych filarów dojrzałego zarządzania systemami AI, pogrupowanych w **trzy logiczne etapy**: od budowy fundamentów, przez wdrożenie strategii i ograniczanie ryzyka, aż po optymalizację i weryfikację.

ETAP I	Budujemy fundamenty i przejmujemy kontrolę
ETAP II	Wdrażamy strategię i zarządzamy ryzykiem
ETAP III	Optymalizujemy i weryfikujemy

Nowa rzeczywistość po wdrożeniu AI



Sztuczna inteligencja to, jak definiuje to IIA AI Auditing Framework, „systemy wyposażone w procesy intelektualne charakterystyczne dla ludzi, takie jak zdolność do rozumowania, odkrywania znaczeń, uogólniania czy uczenia się z doświadczeń". Obecny boom na aplikacje AI, zwłaszcza na zaawansowane systemy językowe, rewolucjonizuje sposób, w jaki funkcjonują przedsiębiorstwa.

Raport „The 2025 AI Index" opracowany przez Stanford HAI prognozuje, że globalny rynek AI wzrośnie pięciokrotnie w ciągu najbliższych pięciu lat, a adaptacja tej technologii w biznesie stała się powszechna i obejmuje już 78% firm.

Właśnie dlatego dojrzałe zarządzanie sztuczną inteligencją jest kluczowe, aby chronić i budować wartość firmy. Zasadę tę potwierdzają analizy firmy McKinsey. Wskazują one jasno, że największe korzyści z AI nie płyną z samej technologii, lecz z fundamentalnej przebudowy procesów w organizacji. Zignorowanie tego mechanizmu nieuchronnie prowadzi do porażek, które w istocie są porażkami biznesowymi, a nie technologicznymi.

Wiele firm popełnia błąd, próbując jedynie „dokleić" moduł AI do istniejącego, często nieefektywnego procesu, licząc przy tym na jakościowy skok. Takie podejście jednak pomija kluczowy fakt. Prawdziwe korzyści płyną nie z samej automatyzacji, ale z fundamentalnej zmiany sposobu pracy, którą ta technologia dopiero umożliwia.

Jeśli zabraknie tej głębokiej przebudowy, sztuczna inteligencja staje się jedynie kosztowną i skomplikowaną nakładką na stary problem. Nie rozwiązuje go u źródła i ostatecznie nie przynosi oczekiwanych zysków.

9 kluczowych filarów dojrzałego zarządzania AI

Fundamentem dojrzałego i efektywnego systemu zarządzania sztuczną inteligencją jest dziewięć kluczowych filarów. Nie jest to przypadkowy zbiór zadań, lecz spójna, przemyślana ścieżka rozwoju. Podzieliliśmy ją na trzy logiczne etapy, które krok po kroku prowadzą organizację od chaosu do pełnej kontroli i optymalizacji.

Kluczowe jest tu zrozumienie dwóch zasad: chronologii i kompletności. Poszczególne etapy budują się na sobie nawzajem – nie można skutecznie optymalizować procesów (Etap III), jeśli wcześniej nie zbudowaliśmy solidnych fundamentów (Etap I) i nie nadaliśmy działaniom strategicznego kierunku (Etap II). Podobnie, każdy z dziewięciu filarów jest niezbędnym elementem całości. Zignorowanie choćby jednego z nich przypomina budowę mostu, w którym brakuje kluczowego przęsła – cała konstrukcja staje się niestabilna i grozi zawaleniem. Tylko kompleksowe wdrożenie wszystkich filarów w odpowiedniej kolejności gwarantuje stworzenie odpornego i skutecznego systemu zarządzania AI.

ETAP I

Budujemy fundamenty i przejmujemy kontrolę

- Filar 1 Ustanawiamy ramy organizacyjne i odpowiedzialność
- Filar 2 Wdrażamy ład danych
- Filar 3 Rozwijamy kulturę organizacyjną i świadomość etyczną
- Filar 4 Wdrażamy nadzór technologiczny

ETAP II

Wdrażamy strategię i zarządzamy ryzykiem

- Filar 5 Wdrażamy proaktywne zarządzanie ryzykiem
- Filar 6 Wdrażamy niezależną weryfikację i audyt
- Filar 7 Zapewniamy zgodność z ramami prawnymi

ETAP III

Optymalizujemy i weryfikujemy

- Filar 8 Mierzymy efektywność i optymalizujemy nadzór
- Filar 9 Weryfikujemy strategię i zwrot z inwestycji (ROI)

ETAP I ETAP II ETAP III

Budujemy fundamenty i przejmujemy kontrolę

Na tym etapie koncentrujemy się na przejęciu kontroli nad tym, co już działa w organizacji. Naszym celem jest zbudowanie solidnych podstaw organizacyjnych, proceduralnych i etycznych. Bez tego elementarnego fundamentu nasze kolejne wysiłki mogą przynieść bardzo ograniczone efekty.

- Filar 1 Ustanawiamy ramy organizacyjne i odpowiedzialność
- Filar 2 Wdrażamy ład danych
- Filar 3 Rozwijamy kulturę organizacyjną i świadomość etyczną
- Filar 4 Wdrażamy nadzór technologiczny

Filar **1**

Ustanawiamy ramy organizacyjne i odpowiedzialność

Dlaczego to jest istotne?

Brak formalnych ram to bezpośrednia przyczyna realnych strat. Dane z raportu IBM są w tej kwestii jednoznaczne: aż **63% organizacji**, które doświadczyły naruszenia bezpieczeństwa systemów AI, **nie miało wdrożonej żadnej formalnej polityki do zarządzania AI.** Co więcej, niemal wszystkie (97%) przyznały, że brakowało im odpowiednich mechanizmów kontroli dostępu. Dlatego absolutną podstawą jest ustanowienie jasnej struktury, czytelnych zasad i klarownego podziału obowiązków.

Jakie są kluczowe kroki?

Wdrażamy strukturę zarządczą.

Opieramy ją na sprawdzonym standardzie, takim jak Model Trzech Linii (zgodnie z IIA AI Auditing Framework). W praktyce oznacza to, że pierwsza linia, czyli zespoły biznesowe i deweloperskie, bezpośrednio zarządza ryzykiem swoich systemów AI w codziennej pracy. Druga linia, obejmująca działy ryzyka i compliance, tworzy ogólnofirmowe ramy i nadzoruje ich przestrzeganie, działając jako niezależny kontroler. Trzecia linia, czyli audyt wewnętrzny, przedstawia zarządowi obiektywną i niezależną ocenę, odpowiadając na pytanie, czy cały system działa skutecznie.

Tworzymy centralny rejestr systemów AI.

Przeprowadzamy wewnętrzny audyt, aby zmapować i skatalogować wszystkie zastosowania AI w firmie. Warto tu podkreślić, że nie mamy tu do czynienia ze statycznym rejestrem – to dynamiczne narzędzie, które dla każdego systemu określa właściciela biznesowego, kluczowe zbiory danych, na których operuje, formalną ocenę poziomu ryzyka (np. zgodnie z kategoryzacją EU AI Act) oraz jego cel i kluczowe metryki. Bez takiej centralnej ewidencji nie wiemy, co właściwie podlega kontroli, a zarządzanie staje się reaktywne i nieefektywne.

Opracowujemy politykę dopuszczalnego użycia (Acceptable Use Policy).

W tym dokumencie definiujemy i komunikujemy jasne "zasady gry". Polityka musi precyzyjnie określać, jakie kategorie narzędzi AI (zwłaszcza zewnętrznych, jak modele generatywne) są dozwolone, a jakie zakazane, jak pracownicy muszą postępować z danymi poufnymi i firmowymi podczas interakcji z AI oraz jakie są etyczne granice, których nie wolno przekraczać. Celem jest zapewnienie, że innowacyjność nie odbywa się kosztem bezpieczeństwa.

Wskazujemy odpowiedzialność.

Tworzymy klarowny dokument, często w formie np. RACI, który określa role poszczególnych osób w kluczowych procesach. Dzięki temu każdy wie, kto jest odpowiedzialny (Responsible) za codzienne monitorowanie modeli, kto podejmuje ostateczną decyzję (Accountable) w razie incydentu, z kim należy się skonsultować (Consulted) przed wdrożeniem zmiany, a kogo jedynie poinformować (Informed) o jej wynikach. To w praktyce eliminuje problem "rozmytej" odpowiedzialności.

Powołujemy międzyfunkcyjny zespół ds. AI.

Na koniec, aby zapewnić spójność działań w całej organizacji, tworzymy komitet sterujący (AI Steering Committee). W jego skład muszą wejść przedstawiciele kluczowych obszarów: technologii (CIO/CTO), działu prawnego, zarządzania ryzykiem, kluczowych jednostek biznesowych oraz działu HR (ze względu na wpływ AI na pracowników). Tak zróżnicowany zespół jest w stanie skutecznie ocenić wpływ AI z każdej perspektywy, nadzorując wdrażanie strategii.

Czym grozi brak działania?

Zignorowanie tego filaru naraża firmę na wysokie prawdopodobieństwo naruszeń bezpieczeństwa, niekontrolowane ryzyko związane z rozprzestrzenianiem się niezatwierdzonych narzędzi AI (co, jak podaje IBM, podnosi koszt naruszeń średnio o **670 000 dolarów**) oraz luki w odpowiedzialności, które w przypadku incydentu uniemożliwiają wskazanie osoby odpowiedzialnej.

Porada od eksperta

Próba zarządzania wszystkimi inicjatywami AI przez jeden, centralny komitet decyzyjny nieuchronnie prowadzi do paraliżu innowacji. Najbardziej świadome organizacje odchodzą od tego modelu na rzecz struktury, która inteligentnie dzieli odpowiedzialność na dwa uzupełniające się poziomy: strategiczny i operacyjny.

Na poziomie strategicznym działa wyspecjalizowany zespół ekspertów, najczęściej w formule Center of Excellence (Centrum Doskonałości AI). Nie grzęźnie on jednak w codziennych zadaniach projektowych. Jego rola polega na tworzeniu solidnych fundamentów dla całej organizacji – wyznacza standardy technologiczne, definiuje polityki bezpieczeństwa i określa granice akceptowalnego ryzyka. Działa jak architekt, który dostarcza precyzyjne plany, a nie jak kierownik budowy nadzorujący każdy ruch. Cały ciężar realizacji projektów spoczywa z kolei na niewielkich, dynamicznych zespołach, które są integralną częścią działów biznesowych, takich jak marketing, finanse czy operacje.

To przekazanie uprawnień w dół struktury generuje ogromne przyspieszenie, ale jednocześnie wymaga dużej dojrzałości organizacyjnej. Kluczowe staje się precyzyjne zdefiniowanie autonomii tych zespołów, by uniknąć chaosu kompetencyjnego i tarć na linii z zespołem centralnym.

Filar **2**

Wdrażamy ład danych

Dlaczego to jest istotne?

Algorytmy AI działają jak wzmacniacz: każdy błąd czy historyczne uprzedzenie w danych wejściowych zostanie przez nie nie tylko powielone, ale też wzmocnione i przeskalowane. Dlatego wprowadzenie do systemów danych o niskiej jakości prowadzi wprost do tworzenia wadliwych narzędzi. Jeśli wieć np. historyczne dane kredytowe kryły w sobie uprzedzenia, system AI nie tylko je powtórzy. Uczyni z nich fundament swojej logiki decyzyjnej i zacznie systematycznie dyskryminować całe grupy klientów na masową skalę. Uporządkowanie tego obszaru nie jest więc wyłącznie kwestią techniczną – to fundament, na którym opiera się rentowny i etyczny biznes.

Jakie są kluczowe kroki?

Zapewniamy jakość i spójność danych.

Wdrażamy procesy ciągłej weryfikacji informacji zasilających modele, w tym automatyczne testy kompletności i dokładności, co pozwala korygować błędy u samego źródła, zanim zdążą wpłynąć na “decyzje” algorytmu.

Obejmujemy kontrolą pełen cykl życia danych.

Definiujemy jasne zasady dotyczące tego, w jaki sposób dane są zbierane, przetwarzane, przechowywane i usuwane, co zapewnia pełną zgodność z regulacjami, zwłaszcza z RODO (GDPR).

Wdrażamy ścisłą kontrolę dostępu do danych.

Stosujemy zasadę minimalnych uprawnień (least privilege), gwarantując, że tylko upoważnione osoby i systemy mają dostęp do konkretnych zbiorów. Jak podkreśla IIA AI Auditing Framework, kluczowe staje się tu również wdrożenie mechanizmów odpowiedzialnych za podział obowiązków, dzięki czemu zapobiegamy ewentualnym nadużyciom.

Poświęcamy szczególną uwagę ochronie prywatności.

Aktywnie stosujemy techniki takie jak anonimizacja czy pseudonimizacja, aby skutecznie chronić dane osobowe i inne informacje poufne, zwłaszcza w systemach, do których dostęp ma szerokie grono użytkowników.

Dokumentujemy i śledzimy pochodzenie danych (Data Lineage).

Chcąc zapewnić pełną przejrzystość, wdrażamy rozwiązania, które pozwalają nam uzyskać wgląd w dane, na podstawie których system podjął konkretną decyzję. Jest to niezbędne, by móc przeprowadzać audyty i skutecznie zdobywać zaufanie.

Czym grozi brak działania?



Brak ładu danych prowadzi do serii problemów: od strat finansowych wynikających z błędnych decyzji biznesowych, przez ogromne ryzyko utraty reputacji, gdy algorytmy powielają historyczne uprzedzenia, aż po realne kary finansowe za naruszenie RODO. Co gorsza, te problemy często narastają po cichu. Model AI, który „żywi się" złymi danymi, zaczyna podejmować błędne decyzje, na które początkowo nikt nie zwraca na to uwagi. Gdy firma w końcu odkryje, że jej prognozy sprzedaży lub rekomendacje dla klientów są od dawna wadliwe, najprawdopodobniej będzie już musiała zmierzyć się z wielomiesięcznymi stratami.

Porada od eksperta

Dojrzałe organizacje nie reagują na problemy z danymi, lecz im zapobiegają, wykorzystując do tego data contracts (kontrakty danych). Są to zautomatyzowane umowy zapisane w kodzie, które definiują wymagany standard na styku systemów. Jeśli dane źródłowe – na przykład z systemu CRM – naruszą te reguły, kontrakt jest zrywany, a proces automatycznie blokowany. Chroni to model AI przed „zatruciem" wadliwą informacją.

To kluczowa zmiana, która przenosi odpowiedzialność za jakość danych z zespołów analitycznych z powrotem do ich źródła. Wymusza to dyscyplinę u podstaw i gwarantuje, że do analizy trafiają wyłącznie dane zgodne ze standardem.

Takie podejście to fundament nowoczesnego myślenia o danych jako o gotowych, wiarygodnych produktach. Zamiast za każdym razem ręcznie weryfikować jakość danych wejściowych otrzymywanych z innych działów, zespoły analityczne dostają sprawdzony zasób z gwarancją jakości.

Pozwala to skrócić czas potrzebny na budowę i wdrożenie nowych modeli AI, ponieważ eliminuje najbardziej czasochłonną i żmudną fazę pracy, czyli poszukiwanie, przygotowywanie i czyszczenie danych.

Filar **3**

Rozwijamy kulturę organizacyjną i świadomość etyczną

Dlaczego to jest istotne?

Skuteczność najlepszych nawet technologii i procedur zawsze zależy od czynnika ludzkiego. To właśnie postawy, zrozumienie i zaufanie pracowników decydują o powodzeniu całego przedsięwzięcia. Idealne ramy zarządcze pozostaną bezużyteczne, jeśli zespół nie będzie rozumiał ryzyk lub zacznie opierać się zmianom. Aktywne rozwijanie świadomości i promowanie odpowiedzialnych postaw jest kluczowym elementem całego systemu.

Jakie są kluczowe kroki?

Definiujemy i wdrażamy zasady etyczne AI.

Nasze zasady muszą być konkretne i mierzalne. Dlatego opieramy je na cechach, które IIA AI Auditing Framework wskazuje jako kluczowe dla każdego systemu: wyjaśnialność, brak stronniczości, niezawodność, odpowiedzialność i przejrzystość. W ten sposób tworzymy jednoznaczne standardy, według których oceniamy nasze technologie.

Wdrażamy programy szkoleniowe dla wszystkich pracowników.

Organizujemy obowiązkowe warsztaty, które koncentrują się na dwóch obszarach: praktycznym użyciu narzędzi oraz – co ważniejsze – na zrozumieniu i stosowaniu zasad firmowej polityki AI. Wyjaśniamy, jak rozpoznawać typowe ryzyka (np. związane z prywatnością danych) i przedstawiamy jasne procedury zgłaszania wszelkich incydentów czy wątpliwości.

Aktywnie komunikujemy i sprawnie przeprowadzamy zmianę.

Prowadzimy otwartą komunikację, aby budować zrozumienie wszystkich nowych procesów. Liderzy na każdym szczeblu muszą aktywnie tłumaczyć pracownikom cele i zasady zarządzania AI. W ten sposób “oswajamy” naszych pracowników z czymś, co jest nieznane i może budzić pewne obawy.

Tworzymy bezpieczne kanały do zgłaszania obaw.

Stworzenie procedur to pierwszy krok. Drugim, ważniejszym, jest zachęcenie ludzi do ich stosowania. W tym celu uruchamiamy proste kanały komunikacji oferujące anonimowość. Dzięki nim pracownicy mogą zgłaszać swoje wątpliwości czy incydenty, bez obawy o negatywne konsekwencje.

Czym grozi brak działania?



Brak dbałości o kulturę i świadomość prowadzi do serii powiązanych ze sobą problemów. Wszystko zaczyna się od błędów ludzkich – niewyszkolony pracownik może niewłaściwie zinterpretować wyniki AI i popełnić błąd, prowadzący do powstania incydentu. To z kolei droga do utraty zaufania klientów i pracowników.

Ta rzeczona utrata zaufania nie jest teoretycznym problemem wizerunkowym. Jak pokazujują liczne przykłady z rynku, bezpośrednio przekłada się na wyniki finansowe. Klienci, którzy poczują się potraktowani niesprawiedliwie przez algorytm mogą odejść do konkurencji. Jednocześnie pracownicy, którym każe się polegać na narzędziach, których zwyczajnie nie rozumieją, szybko znajdą sposoby, by je omijać. Całkowicie zniweczy to zakładany zwrot z inwestycji.

Porada od eksperta

Tradycyjne szkolenia z etyki AI zawodzą, ponieważ teoria rozmija się w nich z praktyką. Dlatego liderzy rynku stawiają na dwutorowe podejście do budowy odpowiedzialnej technologii.

Z jednej strony powołują wyspecjalizowane, wewnętrzne zespoły ethical red teaming (etycznych zespołów uderzeniowych), które niczym „etyczni hakerzy" testują firmowe systemy, szukając w nich ukrytych uprzedzeń i luk.

Z drugiej strony angażują całą organizację, rozszerzając istniejące programy bug bounty (nagród za błędy) o gratyfikacje za wykrywanie problemów natury etycznej. Takie połączenie specjalistycznego audytu z zaangażowaniem wszystkich pracowników sprawia, że etyka AI przestaje być abstrakcyjnym pojęciem, a staje się realnym i mierzalnym elementem kultury firmy.

Taki model ma jeszcze jedną, kluczową zaletę – całkowicie zmienia pozycję firmy w rozmowach z klientami i regulatorami. Zamiast jedynie deklarować i przedstawiać certyfikaty ze szkoleń, organizacja może udowodnić, że posiada aktywny, wewnętrzny mechanizm do wykrywania i naprawiania własnych błędów. Proaktywne poszukiwanie problemów etycznych, zanim staną się one publicznym incydentem, buduje kapitał zaufania, którego nie da się podrobić. Jest to najsilniejszy dowód na poważne traktowanie odpowiedzialności.

Filar **4**

Wdrażamy nadzór technologiczny

Dlaczego to jest istotne?

Same zasady i procedury, choć często wyglądają dobrze na papierze, nie wystarczą. Bez odpowiednich narzędzi do ich egzekwowania, dają nam tylko fałszywe poczucie bezpieczeństwa. Dlatego w tym filarze budujemy niezbędne zaplecze technologiczne, które pozwoli nam przejść od reagowania na problemy do proaktywnego, zautomatyzowanego nadzoru. To właśnie technologia w praktyce przekształca naszą strategię w działający i mierzalny system.

Jakie są kluczowe kroki?

Zapewniamy odpowiednie zasoby IT, co stanowi warunek wstępny dla profesjonalnych działań w obszarze AI.

Obejmuje to nie tylko samą infrastrukturę – moc obliczeniową do trenowania modeli i pamięć masową do przechowywania danych – ale również, co często jest pomijane, wysoko wykwalifikowanych specjalistów, zdolnych nią zarządzać. Inwestycja w sprzęt bez inwestycji w ludzi to prosta droga do frustracji i zmarnowanych pieniędzy.

Wdrażamy narzędzia do automatyzacji procesów (MLOps).

Platformy te pozwalają nam ujednolicić i zautomatyzować cały cykl życia modeli, od ich tworzenia po wdrożenie. W praktyce MLOps drastycznie skraca czas potrzebny na wdrożenie nowego modelu, co daje zespołom więcej czasu na innowacje, a nie na walkę z procesem wdrożeniowym.

Uruchamiamy systemy ciągłego monitoringu.

Raz wdrożony model AI jest systemem dynamicznym – jego skuteczność może z czasem spadać. Ciągły monitoring pozwala nam automatycznie śledzić kluczowe wskaźniki wydajności i otrzymywać alerty, zanim model zacznie podejmować decyzje, które wprowadzają w błąd naszych pracowników lub klientów.

Wdrażamy zautomatyzowane narzędzia do śledzenia pochodzenia danych (Data Lineage).

W przypadku kontroli regulacyjnej, zamiast nerwowego, wielotygodniowego poszukiwania dowodów, systemy te pozwalają nam błyskawicznie udowodnić, na jakich danych trenowaliśmy dany model.

Uzupełniamy nasz zestaw narzędzi o rozwiązania z obszaru Explainable AI (XAI).

Sama decyzja AI to często za mało, ponieważ ludzie z natury nie ufają procesom, których nie rozumieją. Zarówno klienci, jak i wewnętrzni menedżerowie muszą rozumieć, dlaczego system podjął konkretną decyzję, co jest kluczowe dla zdobywania zaufania.

Czym grozi brak działania?



Brak technologicznych podstaw prowadzi wprost do poważnych zakłóceń operacyjnych. Początkowo objawia się to niską wydajnością, która spowalnia kluczowe procesy w firmie - manualne zarządzanie modelami szybko zaczyna blokować jakikolwiek rozwój. Najgorsze jest jednak to, co niewidoczne. Mówimy w tym momencie o stopniowym spadku dokładności algorytmów, który sprawia, że miesiącami możemy podejmować błędne decyzje biznesowe, nawet o tym nie wiedząc.

Porada od eksperta

Sprawne wdrażanie AI wymaga czegoś więcej niż dostępu do danych – wymaga pewności, że technologia działa w ramach ustalonych zasad. Tę gwarancję daje podejście znane jako governance as code (zarządzanie jako kod), które zamienia firmowe standardy i polityki w zestaw aktywnych, zautomatyzowanych reguł. Dzięki temu wytyczne – na przykład dotyczące limitu stronniczości modelu czy obowiązku dokumentacji – przestają być martwym zapisem. System automatycznie pilnuje ich przestrzegania na każdym etapie prac, zdejmując ten ciężar z barków analityków i programistów.

W ten sposób organizacja rozwiązuje fundamentalny konflikt pomiędzy szybkością a kontrolą. W tym przypadku dział zgodności przestaje pełnić rolę „hamulcowego", który ręcznie sprawdza projekty tuż przed wdrożeniem. Zamiast tego staje się partnerem, który dostarcza zespołom deweloperskim mechanizmy kontrolne. To daje analitykom swobodę i autonomię oraz pozwala im szybko eksperymentować w bezpiecznym, automatycznie kontrolowanym środowisku.

ETAP I ETAP II ETAP III

Wdrażamy strategię i zarządzamy ryzykiem

Gdy mamy już kontrolę nad fundamentami, możemy przejść od działań porządkowych do strategicznych.

Na tym etapie skupiamy się na świadomym kształtowaniu roli AI w naszej organizacji.

Celem jest zapewnienie, że nasze inicjatywy w obszarze sztucznej inteligencji są ściśle dopasowane do celów biznesowych, że proaktywnie zarządzamy związanym z nimi ryzykiem oraz że działamy w pełnej zgodności z ramami prawnymi.

- Filar 5 Wdrażamy proaktywne zarządzanie ryzykiem
- Filar 6 Wdrażamy niezależną weryfikację i audyt
- Filar 7 Zapewniamy zgodność z ramami prawnymi

Filar **5**

Wdrażamy proaktywne zarządzanie ryzykiem

Dlaczego to jest istotne?

Wiele firm podchodzi do ryzyka związanego z AI reaktywnie, analizując problemy dopiero wtedy, gdy narastają do tego stopnia, że powodują realne straty. To kosztowna i niebezpieczna strategia, zwłaszcza że błędy systemów AI często powiększają się po cichu i przez długi czas. Ten filar całkowicie zmienia to podejście. Nie czekamy, aż problemy wystąpią. Zamiast tego systematycznie je identyfikujemy, oceniamy i ograniczamy, zanim zdążą zaszkodzić naszej działalności.

Jakie są kluczowe kroki?

Ryzyka związane z AI muszą stać się integralną częścią systemu zarządzania ryzykiem w całej firmie.

W tym celu wpisujemy je do centralnego rejestru ryzyk, ustalamy akceptowalny poziom ryzyka dla inicjatyw AI i przypisujemy za nie odpowiedzialność menedżerom biznesowym.

Analizujemy głośne przypadki i błędy innych firm.

Są one cennym źródłem wiedzy. Badamy znane problemy, takie jak dyskryminacja w algorytmach rekrutacyjnych (Amazon) czy przy przydzielaniu limitów kredytowych (Apple Card). Wyciągnięte wnioski służą nam jako praktyczna lista kontrolna dla naszych własnych zabezpieczeń.

Przeprowadzamy systematyczną Ocenę Wpływu (AI Impact Assessment) dla każdego nowego systemu AI, zanim zostanie on wdrożony.

Taka analiza obejmuje wpływ na prywatność danych, potencjalne nadużycia, sprawiedliwość wobec różnych grup społecznych czy odporność na ataki. To pozwala nam zaplanować i wdrożyć działania zaradcze, zanim system zacznie działać produkcyjnie.

Zarządzamy ryzykiem związanym z brakiem przejrzystości w modelach, których działanie jest trudne do zinterpretowania.

Nie możemy po prostu akceptować tego faktu. Naszym zadaniem jest aktywne

identyfikowanie tych luk, a następnie, zgodnie z rekomendacjami IIA AI Auditing Framework, wprowadzanie dodatkowych zabezpieczeń – na przykład poprzez wprowadzenie ludzkiego nadzoru nad najważniejszymi decyzjami.

Prowadzimy ciągły przegląd i aktualizację map ryzyka.

Nasza ocena ryzyka musi być procesem ciągłym, ponieważ krajobraz zagrożeń stale się zmienia. Wymaga to od nas reakcji na nowe regulacje, głośne incydenty w naszej branży czy planowane użycie AI w nowych, wrażliwych obszarach (jak HR).

Czym grozi brak działania?

Początkowo największym zagrożeniem są "niewidoczne" ryzyka. Są to subtelne błędy. Narastają one po cichu, często przez wiele miesięcy, i prowadzą do skumulowanych strat. Zwykle odkrywamy je, gdy jest już za późno. Kiedy problem w końcu staje się widoczny, okazuje się, że firma jest na niego całkowicie nieprzygotowana. Chaotyczna, doraźna reakcja często tylko pogarsza sytuację. W przypadku sporu prawnego, firmie, która nie ma udokumentowanej oceny ryzyka, trudno jest udowodnić, że podjęła odpowiednie kroki, by zapobiec problemom.

Porada od eksperta

Aby nadać ocenie ryzyka realny wymiar, należy przejść od ogólnych określeń do twardych danych finansowych.

Zamiast posługiwać się jakościową skalą „wysokie/średnie/niskie", eksperci wdrażają „probabilistyczne modelowanie ryzyka finansowego". Wykorzystują metody statystyczne, takie jak symulacje Monte Carlo, do oszacowania oczekiwanej rocznej straty (w złotówkach czy euro) w przypadku konkretnej awarii systemu AI. Pytanie zmienia się z „czy to jest ryzykowne?" na „jaka jest prawdopodobna strata przychodów, jeśli dokładność naszego silnika rekomendacji spadnie o 3% w ciągu roku?".

Taka kwantyfikacja pozwala przełożyć abstrakcyjne ryzyko na konkretny język finansów, co z kolei ułatwia priorytetyzację działań naprawczych i precyzyjne obliczenie zwrotu z inwestycji w jego ograniczenie.

Filar **6**

Wdrażamy niezależną weryfikację i audyt

Dlaczego to jest istotne?

Samo wdrożenie mechanizmów kontrolnych nie gwarantuje jeszcze bezpieczeństwa. Musimy także zyskać pewność, że wdrożone mechanizmy kontrolne nie tracą swojej skuteczności z biegiem czasu. Ten filar wprowadza właśnie niezależną weryfikację. Pozwala ona obiektywnie potwierdzić skuteczność naszych działań.

Jakie są kluczowe kroki?

Definiujemy zadania audytu wewnętrznego.

Audyt wewnętrzny ma dwa podstawowe zadania. Po pierwsze, działa doradczo, pomagając od samego początku projektować skuteczne mechanizmy kontrolne. Po drugie, działa weryfikująco, przeprowadzając formalne audyty, które oceniają, czy wdrożone kontrole faktycznie działają.

Opracowujemy regularny plan audytów AI.

Podstawą tego planu jest analiza ryzyka. Oznacza to, że w pierwszej kolejności koncentrujemy się na systemach AI o największym potencjalnym wpływie na działalność firmy. Plan jest regularnie aktualizowany, aby uwzględniać nowe wdrożenia i zmieniające się zagrożenia.

Przeprowadzamy dogłębną weryfikację i testowanie.

W trakcie audytu idziemy o krok dalej niż tylko sprawdzanie dokumentacji. Audytorzy muszą weryfikować, czy dane wejściowe zasilające modele są kompletne i dokładne. Testują również, czy wyniki generowane przez AI są zgodne z celami biznesowymi, dla których dany system został stworzony.

Wyniki przedstawiamy bezpośrednio zarządowi i zespołowi ds. audytu.

Prezentujemy najwyższemu kierownictwu zwięzłe i zrozumiałe raporty. Każdy raport musi jasno wskazywać zidentyfikowane słabości i zawierać konkretne rekomendacje. Do każdej rekomendacji przypisujemy osobę odpowiedzialną i termin realizacji.

Czym grozi brak działania?



Ignorowanie niezależnej weryfikacji prowadzi do poważnych, narastających zagrożeń. Największym z nich jest złudne poczucie bezpieczeństwa. Możemy być przekonani, że nasze mechanizmy kontrolne działają, podczas gdy w rzeczywistości są one od dawna nieefektywne. To z kolei prowadzi do utraty wiarygodności w oczach partnerów i regulatorów. Nie jesteśmy wtedy w stanie w obiektywny sposób udowodnić, że poważnie traktujemy zarządzanie AI.

Problem sięga jednak głębiej. Brak zewnętrznej weryfikacji nieuchronnie prowadzi do rozluźnienia wewnętrznej dyscypliny. Zespoły programistów, pracujące bez systematycznego audytu, zaczynają (często w dobrej wierze) iść na skróty, na przykład pomijając testy skrajnych przypadków. Audyt nie służy więc tylko do znajdowania błędów – sama jego obecność działa zapobiegawczo i jest kluczowa dla utrzymania wysokich standardów jakości i etyki w całej organizacji.

Porada od eksperta

Aby audyt był konkretny i techniczny, a nie jedynie proceduralny, warto wdrożyć koncepcję „metryki komponentów AI" (AI Bill of Materials, AIBOM).

W praktyce oznacza to utrzymywanie dla każdego kluczowego systemu AI szczegółowego, wersjonowanego dokumentu, który działa jak szczegółowa specyfikacja techniczna. Taki AIBOM zawiera listę wszystkich „składników" systemu: dokładną wersję modelu, zbiory danych użyte do jego treningu (wraz z ich cyfrowymi sygnaturami), kluczowe parametry uczenia, listę wykorzystanych bibliotek open-source oraz udokumentowane wyniki testów na stronniczość i wydajność. W tym modelu zadaniem audytora nie jest już tylko ocena procesu na papierze, ale techniczna weryfikacja integralności i odtwarzalności tej metryki. To sprawia, że audyt staje się w pełni mierzalny i znacznie bardziej wiarygodny.

Wartość AIBOM widzimy także w innych miejsach. Staje się on bowiem podstawowym narzędziem do zarządzania ryzykiem związanym z komponentami, z których składa się system AI. Nowoczesnych systemów rzadko kiedy buduje się od zera – firmy często korzystają z zewnętrznych zbiorów danych, gotowych modeli podstawowych (np. open-source) czy dziesiątek bibliotek. AIBOM pozwala audytorowi precyzyjnie prześledzić to „pochodzenie" i ocenić przejmowane wraz z nimi ryzyko – na przykład ukryte uprzedzenia w danych od dostawcy, luki bezpieczeństwa w konkretnej bibliotece czy ograniczenia licencyjne modelu. Daje to firmie pełen wgląd nie tylko w to, co sama zbudowała, ale także w to, co pobrała z zewnątrz i włączyła do swoich systemów.

Filar **7**

Zapewniamy zgodność z ramami prawnymi

Dlaczego to jest istotne?



Unijny AI Act wprowadza nową rzeczywistość prawną. Za jego nieprzestrzeganie grożą wielomilionowe kary. To sprawia, że zgodność z prawem staje się sprawą strategiczną, omawianą na poziomie zarządu i kluczowym elementem ochrony firmy przed stratami. Ten filar to praktyczny przewodnik po tej nowej rzeczywistości.

Jakie są kluczowe kroki?



Analizujemy luki w naszych obecnych systemach.

Szczegółowo porównujemy naszą dokumentację i procesy z konkretnymi wymogami AI Act. To często żmudna, ale konieczna praca. Jej wynikiem jest precyzyjna lista zadań, dzięki której wiemy, co dokładnie musimy poprawić.

Mapujemy nasze systemy AI, przypisując je do kategorii ryzyka.

Ten krok jest kluczowy, bo pozwala uniknąć niepotrzebnej pracy. Warto pamiętać, że najbardziej rygorystyczne wymagania dotyczą systemów "wysokiego ryzyka", więc dzięki tej klasyfikacji kierujemy nasze zasoby tam, gdzie są naprawdę potrzebne.

Stosujemy normę ISO/IEC 42001 jako praktyczne ramy wdrożeniowe.

Zamiast wymyślać procesy od zera, opieramy się na sprawdzonym standardzie. Norma ta dostarcza nam gotowej struktury i konkretnych wytycznych. Przy okazji daje naszym zespołom pewność, że budują system zarządzania AI w sposób zgodny z wymogami prawnymi.

Automatyzujemy proces tworzenia dokumentacji technicznej.

Ręczne wykonywanie dokumentacji jest nieefektywne i zwykle prowadzi do kosztownych błędów, zwłaszcza przy dużej liczbie modeli. Dlatego wdrażamy narzędzia, które robią to automatycznie i odciążają nasze zespoły.

Czym grozi brak działania?



Problemy ze zgodnością z przepisami AI grożą przede wszystkim dotkliwymi karami finansowymi. Analizy Holistic AI wskazują, że mogą one sięgać nawet **7% globalnego rocznego obrotu.** To jednak nie wszystko. Regulatorzy mogą również nakazać natychmiastowe wyłączenie systemu, co w praktyce oznacza zatrzymanie kluczowych procesów biznesowych.

Często nie doceniamy, co w praktyce oznacza taki „nakaz wyłączenia" systemu. Wyobraźmy sobie, że kluczowy system, który ocenia zdolność kredytową, zostaje wyłączony z dnia na dzień. Bank traci w ten sposób możliwość udzielania kredytów, co uderza w samo serce jego działalności.

Porada od eksperta

Pogoń za stale zmieniającymi się przepisami to walka z wiatrakami. Dlatego inteligentne firmy odwracają logikę: zamiast tworzyć kolejne procedury, wdrażają podejście Compliance by Design.

Polega ono na budowaniu biblioteki gotowych komponentów technologicznych, z których każdy ma już „zaszytą" zgodność z prawem i akceptację działu prawnego. W praktyce, zamiast dziesięciu zespołów interpretujących RODO na własną rękę, firma dostarcza im jeden, gotowy do użycia moduł anonimizacji. Podobniew kontekście AI Act, zespoły korzystają z szablonu, który automatycznie uzupełnia większość dokumentacji. Zgodność z prawem jest więc wbudowaną, automatyczną cechą narzędzi, z których na co dzień korzystają zespoły.

ETAP I ETAP II ETAP III

Optymalizujemy i weryfikujemy

Ostatni etap pozwala nam osiągnąć tzw. doskonałość operacyjną.

Celem jest mierzenie efektywności wdrożonych procesów, ich ciągła optymalizacja oraz niezależna weryfikacja, czy inwestycje w AI przynoszą oczekiwany zwrot. Pozwala to naszej organizacji skalować inicjatywy AI w sposób powtarzalny i bezpieczny, z zachowaniem wszelkich procedur.

Filar 8	Mierzymy efektywność i optymalizujemy nadzór
Filar 9	Weryfikujemy strategię i zwrot z inwestycji (ROI)

Filar **8**

Mierzymy efektywność i optymalizujemy nadzór

Dlaczego to jest istotne?

Wdrożenie ładu AI to spora inwestycja. Biznes - swoją drogą - słusznie zapyta więc: "co z tego będziemy mieć?". Jeśli nie umiemy dostatecznie umotywować naszej propozycji, biznes zawsze będzie postrzegał nasze działania jako zbędny koszt. Ten filar pokazuje, jak za pomocą prostych danych udowodnić realną wartość ładu i stale go ulepszać.

Jakie są kluczowe kroki?

Definiujemy kluczowe wskaźniki efektywności (KPI).

Abstrakcyjne pojęcia, takie jak "etyka" czy "bezpieczeństwo", przekuwamy na konkretne, mierzalne wskaźniki. Mogą to być proste liczby, takie jak procent modeli z pełną dokumentacją, średni czas reakcji na incydent czy wskaźnik wykrywania stronniczości, co w swoich materiałach rekomenduje Relyance AI. Taka karta wyników pozwala obiektywnie śledzić postępy.

Mierzymy zwrot z inwestycji (ROI).

Obliczamy go na dwa sposoby. Z jednej strony pokazujemy, ile pieniędzy oszczędzamy, unikając kar i problemów prawnych. Z drugiej, udowadniamy, jak dobre zarządzanie pomaga szybciej wprowadzać na rynek nowe produkty i zdobywać zaufanie klientów – co, jak dowodzą analizy z California Management Review, jest kluczowym elementem generowania wartości.

Przekładamy dane techniczne na wartość biznesową.

Dane techniczne tłumaczymy na język finansów. Jeśli monitoring wykrył spadek dokładności modelu o 5%, naszym zadaniem jest policzyć, jakie straty przychodów może to generować każdego dnia. Analizujemy też całkowity koszt ładu, wliczając czas pracy specjalistów.

Identyfikujemy wąskie gardła.

Zebrane dane pozwalają nam znaleźć miejsca, w których marnujemy czas i pieniądze. Jeśli nasi najlepsi specjaliści poświęcają 40% czasu na powtarzalne kontrole, jest to sygnał, że ten obszar wymaga pilnej automatyzacji.

Czym grozi brak działania?



Po pierwsze, generujemy w ten sposób ukryte koszty, ponieważ marnujemy czas wysoko opłacanych specjalistów na powtarzalne, manualne zadania kontrolne. Po drugie, takie manualne podejście jest nieskalowalne i po prostu nie da się go utrzymać przy całym, rosnącym portfelu systemów AI. Co jednak najgorsze, bez mierzalnych danych pozbawiamy się możliwości ciągłego doskonalenia. Nie wiedząc, co działa, a co nie, nie jesteśmy w stanie systematycznie ulepszać naszego podejścia do zarządzania.

Porada od eksperta

Ostatecznym celem ładu korporacyjnego nie jest jedynie redukcja ryzyka, ale przede wszystkim przyspieszenie bezpiecznego wdrażania innowacji. Dlatego kluczową metryką, którą należy mierzyć, jest „prędkość innowacji w ramach ładu". Zamiast skupiać się wyłącznie na spadku liczby incydentów, organizacja powinna śledzić, jak skraca się średni czas od powstania pomysłu na model AI do jego produkcyjnego wdrożenia, które pomyślnie przeszło wszystkie zautomatyzowane bramki kontrolne.

Systematycznie skracający się czas jest najlepszym dowodem na to, że dobrze zaprojektowany ład staje się akceleratorem, a nie hamulcem biznesu. To z kolei stanowi najsilniejszy argument za dalszymi inwestycjami w jego rozwój.

Filar **9**

Weryfikujemy strategię i zwrot z inwestycji (ROI)

Dlaczego to jest istotne?

Inicjatywy AI, pozbawione ścisłego powiązania z celami biznesowymi, łatwo mogą stać się kosztownym "laboratorium badawczym". Generują ciekawe technologie, ale nie przynoszą firmie realnej wartości. Ten filar gwarantuje, że nasze inwestycje w sztuczną inteligencję nie są sztuką dla sztuki. Zamiast tego, dbamy o to, by przekładały się na konkretne, mierzalne korzyści dla organizacji.

Jakie są kluczowe kroki?

Angażujemy kadrę zarządzającą w definiowanie celów.

Dbamy o to, aby cele dla każdej inicjatywy AI były zdefiniowane w konkretny, mierzalny, osiągalny sposób i określony w czasie (SMART). Przykładowo, zamiast ogólnego celu "usprawnimy obsługę klienta", definiujemy cel SMART: "zmniejszymy średni czas odpowiedzi na zapytanie o 30% w ciągu 6 miesięcy, wdrażając chatbota AI".

Opracowujemy strategię AI spójną z celami firmy.

Tworzymy dokument, który jasno odpowiada na pytanie: w jaki sposób konkretne działania AI mają wspierać realizację głównych celów biznesowych organizacji. Strategia ta określa również akceptowalny poziom ryzyka dla różnych typów inicjatyw, przez co unikamy ryzyka, że decyzje podejmowane przez poszczególne zespoły będą nieodpowiedzialne i nietrafne.

Mierzymy materialne i niematerialne korzyści z wdrożenia.

Analizujemy nie tylko bezpośrednie korzyści finansowe, które można łatwo policzyć (np. redukcja kosztów, wzrost przychodów, co potwierdzają dane IBM). Równie uważnie przyglądamy się korzyściom niematerialnym, takim jak wzrost satysfakcji klienta (mierzony np. wskaźnikiem NPS) czy poprawa satysfakcji pracowników, którzy dzięki AI mogą zająć się bardziej kreatywnymi zadaniami.

Porównujemy nasze wyniki z rynkiem.

Regularnie analizujemy publicznie dostępne informacje o tym, jak inne firmy w naszej branży wykorzystują AI i jaką wartość dzięki temu osiągają. Daje nam to ważny punkt odniesienia i pozwala ocenić, czy nasze własne wyniki są satysfakcjonujące, czy też pozostajemy w tyle za konkurencją.

Dążymy do przebudowy procesów, by maksymalizować wartość.

Jak wskazuje McKinsey, największe korzyści z AI osiągamy nie wtedy, gdy automatyzujemy stary proces, ale gdy używamy technologii, by całkowicie przemyśleć i przeprojektować sposób, w jaki pracujemy. To jest ostateczny cel, który pozwala osiągnąć prawdziwą transformację, a nie tylko kosmetyczne usprawnienia.

Czym grozi brak działania?

Widzimy tutaj trzy główne problemy. Pierwszym i najbardziej oczywistym są nieefektywne inwestycje – finansujemy projekty, które nigdy nie przynoszą zwrotu. To z kolei prowadzi do utraty wsparcia ze strony zarządu, który, nie widząc wymiernych korzyści, staje się niechętny do finansowania kolejnych inicjatyw. W efekcie dynamika rozwoju innowacji spada – AI jest implementowana dla samej technologii, bez większego powiązania z realnymi potrzebami biznesu.

Porada od eksperta

Wiele firm wpada w pułapkę finansowania dziesiątek małych, odizolowanych od siebie projektów AI. Każdy z nich może wyglądać obiecująco, ale ich łączny wpływ na wynik finansowy firmy często jest niewielki. Dlatego dojrzalsze organizacje odchodzą od tego modelu na rzecz strategicznej transformacji opartej na domenach.

Podejście to opiera się na prostej zasadzie: zamiast dzielić budżet, firma świadomie koncentruje niemal całość inwestycji w AI na kompleksowej przebudowie kilku (2-3) kluczowych obszarów, jak marketing czy logistyka. Każdy z nich funkcjonuje jak osobna jednostka biznesowa z własnym rachunkiem zysków i strat oraz precyzyjnie określonym celem ROI. Korzyści biznesowe płynące z tak głębokiej przebudowy jednego obszaru są nieporównywalnie większe niż suma zysków z dziesiątek drobnych usprawnień, które giną w skali całej organizacji.

Wnioski i kluczowe rekomendacje

Analiza dziewięciu filarów udowadnia, że organizacje podchodzą do ładu korporacyjnego AI na dwa sposoby. Większość traktuje go jako zbiór regulacyjnych obowiązków i koszt, który trzeba ponieść, aby uniknąć problemów. Jednak liderzy rynku postrzegają go nieco inaczej: widzą w nim mechanizm budujący trwałą przewagę.

Przedstawiona przez nas ścieżka pokazuje, jak przejść z pierwszej grupy do drugiej. W trakcie pierwszego etapu (Fundamenty i Kontrola) porządkujemy chaos. Przejmujemy kontrolę nad narzędziami, danymi, procesami i ludźmi, tworząc stabilną i przewidywalną podstawę do dalszych działań. Na tym etapie celem nie jest jeszcze innowacja, ale zbudowanie bezpiecznego środowiska, w którym innowacja może się w przyszłości rozwijać.

Dopiero na tej podstawie, w trakcie drugiego etapu (Strategia i Zarządzanie Ryzykiem), możemy nadać naszym działaniom strategiczny kierunek. To tutaj zapewniamy, że nasza technologia jest bezpieczna, zgodna z prawem i pracuje na rzecz realnych celów biznesowych, a nie jest tylko technologicznym eksperymentem. Ład korporacyjny zaczyna pełnić rolę kompasu, który wskazuje właściwy kierunek.

Ostatni etap (Optymalizacja i Weryfikacja) poświęcimy na przekształcanie ładu korporacyjnego w mierzalny i wydajny system. Udowadniamy tutaj jego wartość finansową i automatyzujemy go, aby działał taniej i skuteczniej. Naszym celem jest sytuacja, w której solidne zarządzanie pozwala nam wdrażać innowacje oparte na AI szybciej i pewniej niż nasi konkurenci.

Następny krok

Droga do zautomatyzowanego zarządzania

Dlaczego manualne podejście jest nieopłacalne?

Manualne wdrożenie i utrzymanie wszystkich dziewięciu filarów jest ekstremalnie drogie, powolne i niemożliwe do skalowania w całej organizacji. Jak pokazują dane Speednet*, średni roczny koszt utrzymania zgodności jednego systemu AI wysokiego ryzyka waha się od **116 000 do 137 000 euro**. Kwota ta, zwielokrotniona przez liczbę posiadanych modeli, jasno pokazuje, że kluczem do sukcesu w zarządzaniu AI nie jest zatrudnianie kolejnych analityków, ale mądra automatyzacja.

Warto pamiętać o ty, ze ręczne podejście jest nieopłacalne, ponieważ tworzy wąskie gardło i przerywa zautomatyzowany cykl MLOps. Zamiast płynnego wdrożenia, nasze zespoły inżynierów danych (ML Engineers) muszą wstrzymać prace i ręcznie przeprowadzać walidację – na przykład generować raporty dotyczące dryfu konceptu, sprawdzać odporność modelu na ataki (tzw. adversarial attacks) czy dokumentować pochodzenie danych treningowych. W efekcie marnujemy czas wysoko wykwalifikowanych specjalistów na zadania, które są jednocześnie kosztowne i obarczone ryzykiem błędu.

Jak uzasadnić inwestycję?

Potrzebujesz solidnych argumentów, by uzasadnić inwestycję w platformę do zarządzania AI? Oprzyj swój plan na konkretnych danych. Skorzystaj z naszej analizy, która pozwoli Ci oszacować potencjalne oszczędności i zwrot z inwestycji (ROI) w oparciu o parametry Twojej organizacji.

Zobacz naszą metaanalizę kosztów, w której znajdziesz dokładne wyliczenia oparte na benchmarkach z ponad 50 europejskich firm z sektora finansowego.

Metaanaliza kosztów →

Chcesz przejść od teorii do działania?

Porozmawiajmy o tym, jak możemy pomóc Twojej organizacji wdrożyć te filary.

Kontakt →

Bibliografia i dodatkowe źródła

- THE IIA'S Artificial Intelligence Auditing Framework
- IBM: How to maximize ROI on AI in 2025
- IBM Report: 13% Of Organizations Reported Breaches Of AI Models Or Applications, 97% Of Which Reported Lacking Proper AI Access Controls
- Penalties of the EU AI Act: The High Cost of Non-Compliance
- The 2025 AI Index Report
- The state of AI in 2025: Agents, innovation, and transformation
- Shaping Europe's digital future: AI Act
- ISO/IEC 42001: a new standard for AI governance
- On the ROI of AI Ethics and Governance Investments: From Loss Aversion to Value Generation
- Measuring AI governance metrics that matter
- Koszty AI Governance w bankowości: Metaanaliza

Autorzy



Tymoteusz Olszewski
Head of AI



Adam Rasiewicz
Senior Business Development Manager

SPEEDNET

Technologia, która napędza nowoczesne finanse.



Krótszy czas wejścia na rynek i bardziej przewidywalny zwrot z inwestycji dla Twoich cyfrowych produktów finansowych – dostarczane w oparciu o nasz model outcome-based oraz bogate doświadczenie w sektorze BFSI.

mBank · VELO BANK · Santander · Bank Pekao · ALIOR BANK · Bank BPH · POP Pankki · GET IN BANK · ICA Banken · saar LB · Genossenschaftsverband Verband der Regionen · BANCOVO. · ringier axel springer · GENERALI · creditstar · paytree · cash·· · FICO · Wolters Kluwer

Nasza oferta | Kluczowe produkty | Usługi delivery acceleration

Kluczowe produkty



Gotowe rozwiązania cyfrowe zaprojektowane dla szybkiego wejścia na rynek

Nasze portfolio łączy sprawdzone IP, silniki oparte na AI oraz kompletne frameworki, które odpowiadają na najważniejsze wyzwania w finansach i technologii.

Przyspieszenie regulacji i zgodności, wzbogacanie danych

obniż koszty audytu i AI oraz zapewnij gotowość na AI Act, DORA i inne. Wzbogacaj dane transakcyjne.

Auditor™ · Data Enrichment

Innowacje w obszarze integracji, kredytów i płatności

zintegrowany zestaw usług integracyjnych, silników pożyczkowych, AI do oceny kredytowej, procesów BNPL oraz akceleratorów płatności - wszystko po to, by skrócić time-to-market o miesiące i zmniejszyć koszty operacyjne.

Microloan Origination Engine · SnapCredit AI · UnderwriterAI · Payments Accelerator · Integration Services Accelerator

Bankowość cyfrowa nowej generacji

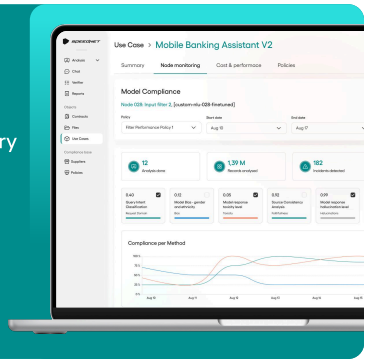
platformy, które pomagają bankom pozyskiwać nowych klientów i wyróżniać swoje kanały mobilne usługami VAS oraz zaangażowaniem na poziomie superaplikacji.

Youth banking platform · Superapp VAS Enablement

SPEEDNET

Auditor™

AI Management System, który umożliwia prowadzenie kluczowych procesów AI Governance w organizacji oraz monitorowanie i zapewnianie zgodności wszystkich Systemów AI.



Usługi delivery acceleration

Wprowadź do swoich procesów szybkość, elastyczność i najwyższe standardy techniczne

Nasze usługi zostały zaprojektowane tak, by eliminować wąskie gardła, modernizować architektury i przyspieszać rozwój produktów cyfrowych.

Speedflow™

nasz autorski AI framework, który przyspiesza cały cykl tworzenia oprogramowania.

Gemini · GitLab · slack · REDMINE

AI MVP & PoC development

zminimalizuj ryzyko dzięki szybkim MVP i działającym demo w ciągu tygodni, a nie miesięcy.

Agile delivery PODs

cross-functional zespoły, które dostarczają produkty cyfrowe 4,5x szybciej.

Compose + KMP LaunchPad

budowa produkcyjnych aplikacji mobilnych z 60–80% współdzielonego kodu i natywną jakością.

OpsView 360

zintegrowany monitoring i observability – skrócenie czasu rozwiązywania incydentów do 70%.

Velocity pipeline services

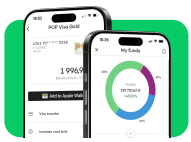
optymalizacja pipeline'ów CI/CD umożliwiająca codzienne releasy i szybszy feedback.

Współpraca ze Speednet oznacza:

- Wykorzystanie gotowych modeli i zespołów - szybszy rozwój bez utraty jakości.
- Dostęp do zespołu, który rozumie sektor BFSI i jego wymagania regulacyjne.
- Elastyczne skalowanie - możliwość zwiększania lub zmniejszania zasobów w trakcie projektu.
- Modernizację technologii, która zapewnia innowacyjność, zgodność i bezpieczeństwo.

Obszary doświadczenia i wiedzy

Bankowość mobilna (detaliczna i korporacyjna) | Cyfrowe produkty finansowe (web i mobile) | Usługi o wartości dodanej | API i integracje systemowe | Warstwa logiki biznesowej (middleware) | Systemy CMS i CRM | Kredyty i hipoteki | Adaptacja AI i AI-driven SDLC | Płatności | Core silniki w finansach i ubezpieczeniach



Zmiany, które wprowadziliśmy w aplikacji mobilnej fińskiego POP Pankki, przełożyły się na **20% wzrost liczby klientów** oraz **126% wzrost całkowitego zysku**, przy najwyższym poziomie satysfakcji klientów w całej Skandynawii.

EUVIC

30+ firm

5000+ inżynierów

Jesteśmy centrum kompetencji bankowych EUVIC.

Chcesz osiągać konkretne wyniki bez żmudnych wdrożeń?
Z Speednet zyskasz zwinnego partnera do szybkiej i skutecznej transformacji cyfrowej.

Umówmy się na rozmowę



Adam Rasiewicz
Senior Business Development Manager
adam.rasiewicz@speednetsoftware.com
+48 880 319 710

speednetsoftware.com →