

TECHNOLOGIE DLA FINANSÓW



Bez porządných danych nie ma cyfrowej transformacji

Cyfrowa transformacja sektora finansowego od lat znajduje się w centrum strategicznych debat zarządców, regulatorów i dostawców technologii. Chmura, sztuczna inteligencja, automatyzacja procesów czy zaawansowana analityka obiecują większą efektywność, lepsze zarządzanie ryzykiem i szybsze decyzje biznesowe. W praktyce jednak wiele inicjatyw technologicznych nie przynosi oczekiwanych rezultatów. Przyczyna jest często wspólna i banalna zarazem – niska jakość danych.



KAROLINA PRASZEK-GOŁĘBIEWSKA

dyrektor zarządzający / CEO
Kancelarii Bezpieczeństwa,
prawniczka, ekspertka ds.
bezpieczeństwa informacji i ochrony
danych osobowych

Dane jako fundament, nie produkt uboczny

W instytucjach finansowych dane wciąż bywają traktowane jako efekt uboczny procesów operacyjnych, a nie jako strategiczne aktywo. Tymczasem technologie finansowe

są tak dobre, jak dane, na których pracują. Algorytmy sztucznej inteligencji, modele predykcyjne czy systemy automatycznego raportowania nie „naprawia” błędnych, niekompletnych lub niespójnych danych. Wręcz przeciwnie – automatyzują chaos, skalując błędy zamiast wartości.

Jakość danych obejmuje znacznie więcej niż ich poprawność. To także aktualność, kompletność, spójność pomiędzy systemami, jednoznaczność definicji oraz możliwość przesłania pochodzenia danych (data lineage). Bez tych elementów nie sposób mówić o data-driven finance ani o realnym wsparciu technologii w podejmowaniu decyzji zarządczych.

Legacy systems i silosy informacyjne

Jednym z największych wyzwań jakości danych w finansach są systemy legacy oraz silosy informacyjne. Dane o kliencie, transakcjach, ryzyku czy zgodności regulacyjnej funkcjonują równolegle w wielu systemach, często z odmiennymi definicjami i logiką biznesową. W takich warunkach integracja danych staje się projektem wysokiego ryzyka, a każda nowa technologia – kolejną warstwą komplikacji.

Cyfrowa transformacja nie polega wyłącznie na wdrożeniu nowego narzędzia, lecz na uporządkowaniu architektury informacyjnej organizacji. Bez standardów danych, centralnego zarządzania metadanymi i jasno przypisanej odpowiedzialności za jakość danych (data ownership), nawet najlepsze rozwiązania technologiczne pozostaną kosztownym eksperymentem.

Jakość danych a regulacje i bezpieczeństwo

W sektorze finansowym jakość danych ma również wymiar prawny i regulacyjny. Regulacje takie jak DORA, RODO, wymogi raportowe EBA czy KNF opierają się na

założeniu, że instytucja panuje nad swoimi danymi – wie, jakie dane przetwarza, gdzie są przechowywane, kto ma do nich dostęp i w jakim celu są wykorzystywane.

Niska jakość danych to nie tylko problem operacyjny, ale także realne ryzyko prawne i reputacyjne. Błędne dane mogą prowadzić do nieprawidłowego raportowania regulacyjnego, naruszeń ochrony danych osobowych czy nieskutecznego zarządzania incydentami bezpieczeństwa. W tym kontekście zarządzanie jakością danych staje się integralnym elementem systemu zarządzania bezpieczeństwem informacji i compliance.

AI, automatyzacja i iluzja „inteligentnych” systemów

Rosnące zainteresowanie AI w finansach często pomija fundamentalne pytanie – czy dane są gotowe na wykorzystanie przez algorytmy? Modele uczenia maszynowego wymagają dużych wolumenów danych wysokiej jakości, pozbawionych systemowych błędów i uprzedzeń. W przeciwnym razie instytucja ryzykuje podejmowanie decyzji na podstawie fałszywych wzorców, co w obszarze kredytowym, ryzyka czy przeciwdziałania nadużyciom

może mieć poważne konsekwencje. Podobnie automatyzacja procesów (RPA, IPA) bez uporządkowanych danych prowadzi do automatyzacji wyjątków i ręcznych obejść, zamiast do end-to-end automation. Technologia nie zastąpi braku ładu informacyjnego.

Od projektów IT do zarządzania danymi

Warunkiem sukcesu technologii finansowych jest zmiana perspektywy: od projektowego podejścia do IT w stronę długofalowego zarządzania danymi (data governance). Oznacza to inwestycję nie tylko w narzędzia, ale także w role, procesy i kulturę organizacyjną. CFO, CIO, CDO i zespoły prawne oraz bezpieczeństwa muszą współpracować przy definiowaniu standardów danych, priorytetów jakościowych i zasad odpowiedzialności.

Dopiero na takim fundamencie technologie mogą realnie wspierać transformację cyfrową, poprawiać efektywność i budować przewagę konkurencyjną. Bez porządných danych cyfrowa transformacja pozostaje hasłem – kosztownym, ryzykownym i pozbawionym trwałej wartości.

Banki przyspieszają cyfrową transformację, a regulatorzy patrzą uważnie

Chmura obliczeniowa coraz szybciej staje się istotnym elementem infrastruktury sektora finansowego. Banki i ubezpieczyciele widzą w niej sposób na zwiększenie efektywności, skalowalności i tempa innowacji. Jednocześnie rosną wymagania regulacyjne i presja związana z bezpieczeństwem danych. Jak wynika z raportu „Barometr cyfrowej transformacji polskiego biznesu 2025-2026” firmy Polcom, sektor finansowy wchodzi w fazę przyspieszonej, ale ostrożnej migracji do chmury.



PIOTR ZABOROWSKI
Managing Consultant z Polcom

pośredni wpływ synergii chmury, AI, automatyzacji i cyberbezpieczeństwa na zdolność do innowacji i rozwoju. W sektorze finansowym tempo tej zmiany jest wyższe niż w wielu innych branżach, co wynika zarówno z presji konkurencyjnej, jak i rosnących oczekiwań klientów.

Chmura przestaje być eksperymentem

Jeszcze kilka lat temu rozwiązania chmurowe w finansach wykorzystywano głównie do systemów pomocniczych. Dziś coraz częściej trafiają tam strategiczne procesy biznesowe – analityka danych, aplikacje klienckie czy środowiska wspierające automatyzację i sztuczną inteligencję.

Z danych raportu Polcom wynika, że 72 proc. firm dostrzega bez-

Dla instytucji finansowych chmura przestała być rozwiązaniem testowym i środowiskiem jedynie wspierającym procesy biznesowe. Stała się realnym narzędziem skalowania biznesu, skracania czasu wprowadzania nowych produktów i zwiększania elastyczności operacyjnej. Coraz częściej mówimy o przenoszeniu do chmury procesów o znaczeniu krytycznym. To oznacza zmianę podejścia zarządczego – z zawę-

żonego myślenia projektowego na skoncentrowanie się na podejściu uwzględniającym długofalowe efekty biznesowe. Dziś pytanie nie brzmi już „czy korzystać z chmury”, ale „na jaką skalę i w jakim modelu ją wdrożyć”.

Regulacje spowalniają, ale nie zatrzymują zmian

Jednocześnie sektor finansowy działa w jednym z najbardziej regulowanych środowisk gospodarczych. Nowe wymogi, w tym unijne rozporządzenie DORA, stawiają przed instytucjami finansowymi obowiązek zapewnienia odporności cyfrowej, kontroli nad danymi oraz ciągłości działania systemów IT – również tych opartych na chmurze.

Raport Polcom pokazuje, że 81 proc. firm planuje zwiększyć wydatki na cyberbezpieczeństwo w latach 2025-2026, a pozostałe 19 proc. chce je utrzymać na obecnym poziomie. To sygnał, że bezpieczeństwo i zgodność regulacyjna stały się integralną częścią strategii technologicznych.

Regulatorzy nie blokują dziś rozwiązań chmurowych, ale bardzo wyraźnie oczekują, że będą one wdrażane w sposób kontrolowany, audytowalny i zgodny z wymogami nadzorczymi. Dla instytucji finansowych oznacza to

konieczność dokładnego projektowania architektury IT, w tym coraz częstsze sięganie po modele hybrydowe. Kluczowa staje się transparentność – zarówno wobec regulatorów, jak i klientów. Chmura musi dawać nie tylko elastyczność, ale też poczucie pełnej kontroli nad danymi i procesami. To znacząco podnosi poprzeczkę dla całego sektora.

Bezpieczeństwo jako warunek dalszej migracji

W finansach chmura nie może funkcjonować bez silnego zaplecza cybersecurity. Rosnąca liczba cyberataków oraz koncentracja usług u największych dostawców technologicznych sprawiają, że instytucje finansowe coraz częściej analizują ryzyka związane z dostępnością systemów i zależnością od jednego operatora.

Dane przedstawione w raporcie „Barometr cyfrowej transformacji polskiego biznesu 2025-2026” jasno wskazują, że cyberbezpieczeństwo jest dziś jednym z głównych obszarów inwestycyjnych, a nie kosztem operacyjnym. Dla banków i ubezpieczycieli to warunek dalszej cyfryzacji i migracji do chmury.

Chmura w sektorze finansowym przestała być wyłącznie kwestią

technologii – stała się kwestią odpowiedzialności biznesowej. Instytucje finansowe muszą dziś udowodnić, że potrafią nie tylko efektywnie korzystać z rozwiązań chmurowych, ale także zapewnić ciągłość działania i odporność na incydenty. Coraz większą rolę odgrywa przygotowanie na audyty regulatorów i scenariusze kryzysowe. Bez spełnienia tych warunków dalsza migracja do chmury po prostu nie będzie możliwa.

Ewolucja zamiast rewolucji

Choć tempo zmian rośnie, chmura w sektorze finansowym rozwija się raczej ewolucyjnie niż rewolucyjnie. Instytucje stopniowo przenoszą kolejne obszary działalności, testując rozwiązania, budując kompetencje i dostosowując się do oczekiwań nadzorców.

Najbliższe lata pokażą, które instytucje potrafią znaleźć równowagę między szybkim wdrażaniem innowacji a dyscypliną regulacyjną. Te, które zrobią to najlepiej, zbudują trwałą przewagę na rynku finansowym. Chmura nie jest dziś celem samym w sobie, ale fundamentem dalszej cyfrowej transformacji finansów. I to właśnie dojrzałość w jej wykorzystaniu będzie jednym z kluczowych wyróżników rynku.

AI w systemach transakcyjnych i CRM dla finansów

Sektor finansowy od lat opiera swoją działalność na zaawansowanych systemach transakcyjnych oraz platformach CRM, które wspierają obsługę klientów, sprzedaż produktów i zarządzanie relacjami. Sztuczna inteligencja przestaje być jednak dodatkiem technologicznym i staje się integralną częścią tej architektury, wspierając procesy, przewidywalność oraz decyzje operacyjne.



ŁUKASZ SUJKA
lider rynku, sektor bankowości i finansów, architekt rozwiązań IT

W systemach CRM, takich jak Pivotal CRM, AI otwiera nowe moż-

liwości automatyzacji procesów, poprawy jakości danych i personalizacji obsługi klienta. CRM pełni rolę centralnego repozytorium wiedzy o kliencie – integruje dane z systemów transakcyjnych i produktowych, kanałów cyfrowych oraz punktów kontaktu, takich jak call center czy oddziały. AI działa tu jako warstwa analityczno-decyzyjna: nie zastępuje systemów core'owych, ale znacząco zwiększa ich „inteligencję”.

temu banki mogą szybciej reago-

wać, ograniczać błędy i realnie poprawiać satysfakcję klientów oraz pracowników. Wdrożenia AI w Pivotal CRM realizowane są jako niezależna warstwa usług, integrowana z CRM przez API i zdarzenia (modele ML/LLM) oraz uruchamiana na platformach wybranych przez instytucje. Takie podejście zapewnia elastyczność, skalowalność oraz możliwość stopniowego rozszerzania funkcjonalności bez rewolucyjnych zmian w systemach core'owych. AI w systemach transakcyjnych i CRM nie jest już wizją przyszłości, lecz praktycznym narzędziem transformacji cyfrowej, które wzmacnia efektywność operacyjną, spójność danych oraz zdolność adaptacji do zmieniających się oczekiwań rynku.

temu banki mogą szybciej reago-

wać, ograniczać błędy i realnie poprawiać satysfakcję klientów oraz pracowników. Wdrożenia AI w Pivotal CRM realizowane są jako niezależna warstwa usług, integrowana z CRM przez API i zdarzenia (modele ML/LLM) oraz uruchamiana na platformach wybranych przez instytucje. Takie podejście zapewnia elastyczność, skalowalność oraz możliwość stopniowego rozszerzania funkcjonalności bez rewolucyjnych zmian w systemach core'owych. AI w systemach transakcyjnych i CRM nie jest już wizją przyszłości, lecz praktycznym narzędziem transformacji cyfrowej, które wzmacnia efektywność operacyjną, spójność danych oraz zdolność adaptacji do zmieniających się oczekiwań rynku.

Zapraszamy do kontaktu – zeskanuj kod QR i umów bezpłatną konsultację, podczas której wspólnie przeanalizujemy, jak warstwa AI w Pivotal CRM może wesprzeć kluczowe procesy w Twojej instytucji.



Pivotal Polska – lider w dostarczaniu zaawansowanych rozwiązań CRM dla sektora finansowego, które łączą technologię z efektywną i zgodną z regulacjami komunikacją z klientem. W bankowości liczy się nie tylko szybkość transakcji, ale przede wszystkim umiejętność budowania trwałych relacji.

materiał partnera



Modernizować IT w finansach bez ryzyka operacyjnego

W bankowości „czas to pieniądź” nie oznacza wyłącznie responsywności w reagowaniu na rynek. O wiele częściej to koszt odkładania decyzji inwestycyjnych, które z każdym rokiem robią się droższe, bardziej ryzykowne i trudniejsze organizacyjnie.

GRZEGORZ CHUDEK

dyrektor zarządzający, Cloud First
oraz Technology for Financial
Services Lead, Accenture w Polsce

Jak wykazały nasze badania, około 70 proc. wszystkich wydatków na technologię w bankach jest przeznaczanych wyłącznie na bieżące utrzymanie starych systemów oraz spełnianie wymogów regulacyjnych. Druga strona monety jest jeszcze gorsza, bowiem oznacza to, że na innowacje i rozwój pozostaje jedynie 30 proc. budżetu. W konsekwencji wiele banków funkcjonuje w trybie utrzymania zdolności operacyjnej, a nie w trybie budowania przewagi.

Aktualnie działające systemy przez lata były fundamentem stabilności sektora bankowego. Problem zaczyna się wtedy, gdy stabilność staje się kotwicą w podróży do rozwoju — w końcu zwinność i zmienność są dziś warunkiem konkurowania. Ograniczenia nie wynikają wyłącznie z wieku platform, ale z tego, jak trudno i jak kosztownie się je rozwija w świecie otwartych interfejsów,

integracji partnerskich, rosnącej liczby kanałów cyfrowych i coraz bardziej szczegółowych wymagań dotyczących danych i regulacji. Tylko w ciągu ostatnich 15–20 lat koszty technologii w sektorze bankowym rosły średnio czterokrotnie szybciej niż przychody. To sygnał, że dotychczasowy model wdrażania zmian traci na efektywności. Wiele instytucji z tego sektora wpadło w „pętlę zagłady”, czyli pułapkę, w której wydają coraz więcej na nowe oprogramowanie, a jednocześnie ponoszą rosnące koszty jego integracji z przestarzałym rdzeniem. Co warto podkreślić, to fakt, że taka sytuacja tworzy barierę, która nie tylko generuje coraz wyższe koszty utrzymania, ale także hamuje zdolność banków do konkurencji z nowymi graczami, takimi jak fintechy, które nie są obciążone długim technologicznym.

Spojrzenie z zewnątrz

Często organizacje działają w pewnym odurzeniu operacyjnym, akceptując niedoskonałości swoich systemów jako naturalny element

krajobrazu technologicznego. Dlatego modernizację IT w finansach warto zaczynać od szczerzej diagnozy aktualnego środowiska, rozumianej nie jako spis aplikacji i silosów danych, ale jako inwentaryzację zależności. Trzeba wziąć pod uwagę jednocześnie aplikacje, integracje, dane, procesy, uprawnienia, kontrakty, kompetencje zespołów oraz miejsca, w których proces działa wyłącznie dlatego, że ktoś na końcu steruje nim ręcznie. To pozwoli nam opracować także mapę ryzyka, która wskaże punkty krytyczne, gdzie brak kontroli jest mylony z ograniczeniem systemowym.

Często wewnętrzne zespoły dzielczą systemy razem z narracją o ich ograniczeniach. Z czasem ta narracja zaczyna być traktowana jak oczywistość i na długi czas zamyka pole do realnej zmiany. Dlatego w modernizacji kluczowa jest rola partnera z zewnątrz, który potrafi zadać niewygodne, ale porządkujące pytania: co w banku jest naprawdę krytyczne i dla kogo, jak długo i w jakim zakresie organizacja może tolerować pogorszenie działania, gdzie ryzyko wynika z technologii, a gdzie z braku monitoringu, testów i dyscypliny zarządzania zmianą, czy problemem jest jedna aplikacja, czy raczej cała sieć systemowych zależności.

Najlepszy moment na takie pytania jest przed wyborem technologii

— wtedy diagnoza nie musi być na siłę dopasowana do decyzji, która już zapadła, tylko realnie ją kształtuje. Dopiero na tej podstawie projekt architektury docelowej staje się użyteczny. Powinien opisywać, jak bank ma działać po modernizacji od strony IT i operacji, a jednocześnie wskazywać drogę dojścia tak, aby nie zakłócić bieżącej działalności. Jeśli bank modernizuje elementy w oderwaniu od całości, to istnieje ryzyko, że poprawa szybkości lub funkcjonalności w wąskim obszarze operacyjnym globalnie wywoła wzrost kosztów utrzymania systemu. Wówczas cały projekt staje się coraz bardziej kosztowny, nawet jeżeli każdy jego fragment wygląda sensownie osobno.



Okolo 70 proc. wszystkich wydatków na technologię w bankach jest przeznaczanych wyłącznie na bieżące utrzymanie starych systemów oraz spełnianie wymogów regulacyjnych.

Wielka suma małych zmian

W finansach elementy takie jak monitoring, kontrola wdrożeń, mechanizmy bezpieczeństwa, kopie zapasowe, odtwarzanie po awarii oraz testy kontrolne po zmianach muszą być stałą i regularną częścią projektu, a nie wyłącznie dodatkiem walidacyjnym na końcu. To one decydują, czy organizacja będzie w stanie dostarczać zmiany bez wzrostu liczby incydentów, czy też każde wdrożenie będzie zwiększać napięcie związane z integralnością systemu. W tym kontekście modernizacja jest równocześnie projektem technologicznym i projektem operacyjnym, ponieważ ryzyko rodzi się na styku kodu, danych, procesów, ludzi i legislacji.

W praktyce oznacza to konieczność fazowania wdrożeń. Bank nie może sobie pozwolić na jednorazowy, daleki skok rozwojowy, bo musi działać bez przerw, a tolerancja na zakłócenia jest mocno ograniczona. Każda faza powinna mieć jasny zakres, zdefiniowane dane i procesy, które będą migrowane, oraz warunki przejścia do kolejnego etapu. Istotny jest też model realizacji. Oddanie całej modernizacji jednemu wykonawcy upraszcza start, ale z czasem zamyka bank w rosnącej zależności, ogranicza elastyczność i kumuluje ryzyko w jednym miejscu. Rozproszenie prac bez wspólnych reguł integracji i spójnych standardów wykonania kończy się z kolei rozmyciem odpowiedzialności i środowiskiem, którego nikt nie kontroluje w całości. Dywersyfikacja działa tylko wtedy, gdy jest świadomie zaprojektowana wokół logicznych obszarów odpowiedzialności, a zespoły grają według tych samych zasad. Inaczej przyspieszenie będzie iluzją, a realny rachunek zostanie podliczony w utrzymaniu.

Dawkowanie innowacji

Na końcu pozostaje horyzont czasu. Modernizacja w finansach trwa lata i w praktyce nigdy się nie kończy, ponieważ dotyka procesów krytycznych, danych historycznych, zgodności, audytu i praktyk operacyjnych, a na dodatek unikanie wpadania w dług technologiczny wymaga permanentnych inwestycji. Dlatego potrzebny jest stabilny model finansowania, realne kamienie milowe oraz sposób pokazywania efektów po drodze. Dojrzałe i świadome organizacje nie pytają dziś, czy modernizować, lecz czy przewidzieliśmy odpowiednie zasoby na późniejsze, niezbędne utrzymanie i modernizację.

Technologie w sektorze finansowym – trendy na 2026 r.



MONICA SASSO

dyrektor Red Hat ds. transformacji cyfrowej sektora finansowego

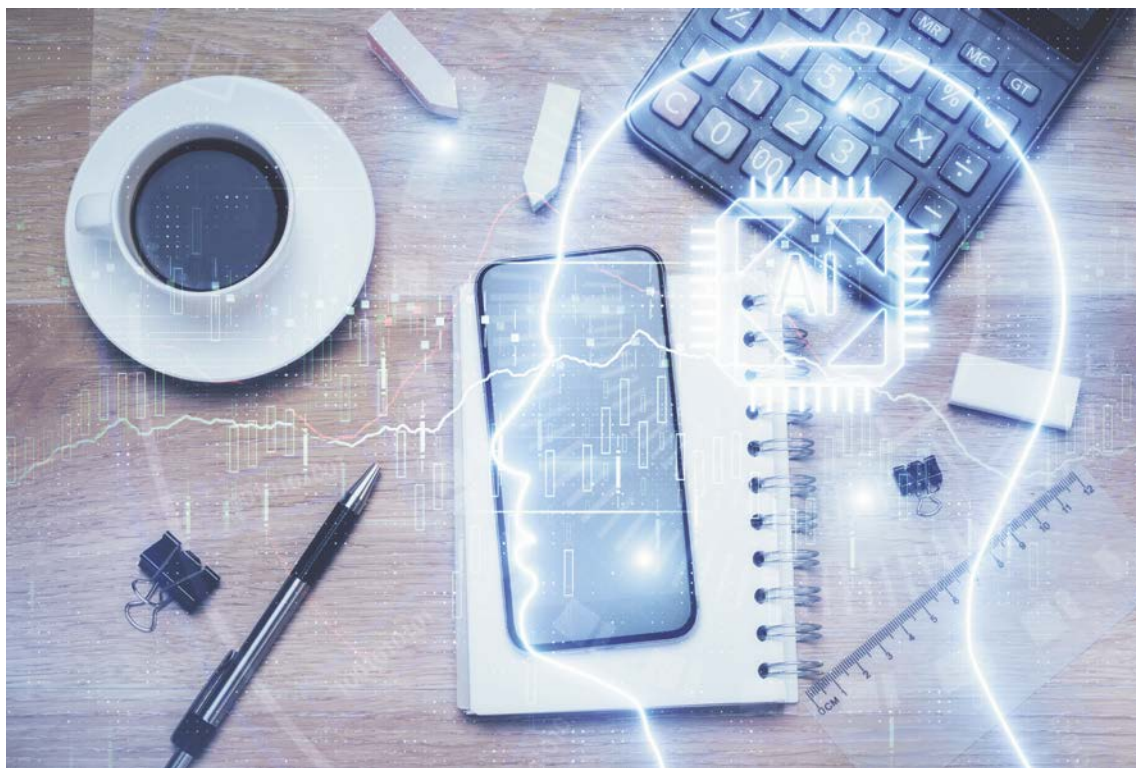
Transparentna i kontrolowalna AI

W obszarze sztucznej inteligencji uwaga przedsiębiorstw koncentruje się dziś przede wszystkim na generatywnej oraz agentowej AI, w miarę jak predykcyjna AI już od dawna znajduje szerokie zastosowanie w sektorze finansowym. Firmy wciąż mierzą się z wyzwaniem wdrażania sztucznej inteligencji w sposób kompleksowy, przejrzysty i kontrolowany, z wykorzystaniem zabezpieczeń bazujących na ramach zarządzania ryzykiem AI (z ang. AI Risk Framework). Takie podejście jest niezbędne, aby móc zaufać tej technologii oraz wykazać wobec regulatorów, klientów i rynku, że jest ona wykorzystywana w sposób właściwy, uczciwy i etyczny. Jednocześnie z obserwacji rynku widzimy, że firmy coraz częściej szukają rozwiązań, które pozwolą im równoważyć fazę eksperymentów innowacji z osiąganiem realnych korzyści biznesowych, takich jak zwrot z inwestycji i wzrost efektywności. Badanie MIT wskazuje, że aż 95 proc. inicjatyw związanych z AI kończy się niepowodzeniem. W tym kontekście w 2026 r. można spodziewać się, że firmy będą



Uwaga przedsiębiorstw koncentruje się dziś przede wszystkim na generatywnej oraz agentowej AI, w miarę jak predykcyjna AI już od dawna znajduje szerokie zastosowanie w sektorze finansowym.

Sektor finansowy od lat należy do gałęzi gospodarki, w których tempo wprowadzania innowacji oraz przełomowych zmian jest szczególnie wysokie. Można się spodziewać, że dynamiczny rozwój technologiczny, jaki zauważalny był w ubiegłym roku, doczeka się w 2026 r. kontynuacji. Krajobraz rozwiązań IT dla finansów będzie kształtowany przez sztuczną inteligencję, cyfrową transformację oraz niezmiennie silny trend wdrażania chmury hybrydowej przy zwróceniu bacznego uwagi na bezpieczeństwo, a także cyfrową suwerenność i odporność.



wprowadzać sztuczną inteligencję w sposób bardziej przemyślany i zaplanowany, już na etapie projektu starając się odpowiedzieć na szczególnie istotne pytania, takie jak „dlaczego wykorzystujemy AI” oraz „w jaki sposób zastosowanie tej technologii wpisuje się w strategię naszej firmy”.

Proaktywna cyberochrona

W obliczu rosnących możliwości generatywnej sztucznej inteligencji i postępującej demokratyzacji kodowania, cyberbezpieczeństwo pozostaje jednym z głównych powodów niepokoju na poziomie zarządów firm finansowych. Krajobraz zagrożeń stale się rozszerza obejmując m.in. technologie kwantowe, generatywną AI, kradzież danych, ataki na łańcuch dostaw, ryzyka związane z chmurą, a także ransomware, phishing, inżynierię społeczną czy zwiększającą się liczbę ataków DDoS.

To z kolei wymusza na firmach odejście od podejścia reaktyw-

nego na rzecz proaktywnego, co w praktyce oznacza konieczność inwestowania w kompetencje zespołów oraz dbania o to, by nie były one przeciążone w obliczu nowo pojawiających się zagrożeń. Jednocześnie dużym wyzwaniem pozostaje wdrażanie nowych technologii w szybkim tempie, przy zachowaniu bezpieczeństwa i zgodności regulacyjnej – zwłaszcza, że cyberprzestępcy nie poruszają się w żadnych regulacyjnych ramach.

Dane to nowe złoto

W kontekście cyfrowego bezpieczeństwa w sektorze finansowym trudno pominąć trzy ściśle powiązane z nim obszary: suwerenność cyfrową, zarządzanie danymi oraz odporność – zarówno cyfrową, jak i operacyjną. Można by sprowadzić tę dyskusję do regulacji takich jak RODO czy DORA, jednak takie uproszczenie niewiele wnosi do praktycznego spojrzenia na wyzwania, z jakimi mierzą się dziś firmy finansowe. Zarządzanie danymi



Coraz częściej odporność cyfrowa i operacyjna jest łączona z pojęciem suwerenności cyfrowej.

pozostaje bowiem nie tylko wyrażnym trendem technologicznym czy regulacyjnym, ale także koniecznością biznesową. Dane to nowe złoto i wszyscy oczekują, że będą one traktowane jak zasoby przechowywane w skarbcu, podczas gdy w rzeczywistości są – dosłownie i w przenośni – „rozsiane wszędzie”. Wyciek informacji z firmy natychmiast trafia na pierwsze strony gazet: audytorzy pukają do drzwi przedsiębiorstw, a te tracą klientów i udziały w rynku.

Co więcej równie istotna jest jakość danych – jeśli są one niekompletne lub niewłaściwie zarządzane, trudno wykazać, że klienci otrzymują odpowiednio dopasowane do swoich potrzeb produkty, a ich interesy są odpowiednio chronione. Wraz z rosnącym wykorzystaniem sztucznej inteligencji wyzwania te dodatkowo się nasilają, czyniąc porządkowanie, klasyfikację, zabezpieczanie i kontrolę danych nie tylko źródłem przewagi konkurencyjnej, ale także wymogiem bezpieczeństwa i przedmiotem rosnącej uwagi regulatorów.

Sektor odporny i suwerenny

Odporność pozostaje jednym z kluczowych tematów ostatnich lat i wszystko wskazuje na to, że prędko się to nie zmieni. Przykładem są regulacje takie jak DORA w Unii Europejskiej, brytyjskie wymogi odporności operacyjnej czy analogiczne przepisy w Australii, Nowej Zelandii, Kanadzie, Japonii, Hongkongu, Singapurze oraz na Bliskim Wschodzie. U podstaw tych regulacji leży pięć wspólnych założeń: zapewnienie pełnej widoczności łańcucha dostaw technologii, traktowanie dostawców zewnętrznych jak wewnętrznych usługodawców, planowanie scenariuszy awaryjnych i ciągłości działania, unikanie uzależnienia od jednego dostawcy (z ang. vendor lock-in) oraz regularne podnoszenie poziomu bezpieczeństwa poprzez tzw. testy penetracyjne.

Coraz częściej odporność cyfrowa i operacyjna jest łączona z pojęciem suwerenności cyfrowej. W odpowiedzi na rosnące oczekiwania regulatorów firmy muszą dziś jasno zdefiniować, co termin ten oznacza w ich przypadku oraz jaki poziom ryzyka są gotowe zaakceptować. Podobnie jak odporność operacyjna, także suwerenność cyfrowa nie jest stanem zero-jedynkowym, lecz procesem, który wymaga świadomych decyzji technologicznych. W tym kontekście podkreśla się, że przejrzystość wbudowana w oprogramowanie open source, otwarte modele AI i metody pracy mogą wspierać zarówno suwerenność, jak i odporność, m.in. dzięki możliwości przenoszenia aplikacji i elastyczności w wyborze dostawców.

CFO–CIO–CTO: trójkąt mocy czy pole konfliktu? Jak przełamać silosy w cyfrowej transformacji

Hasło „cyfrowa transformacja” znaczy dziś więcej niż jeszcze w czasach „mobile first” czy „Internet of Things”. Automatyzacja procesów, migracja do chmury, wdrażanie sztucznej inteligencji czy cyberbezpieczeństwo to dziś elementy strategicznej układanki, od której zależy konkurencyjność firm.

MIROSŁAW GAMLA

Chief Financial Officer & Enterprise Value Practice Lead w Accenture w Polsce, Insurance & Banking Executive

W tym nowym porządku kluczową rolę odgrywa współpraca trzech funkcji: finansowej (CFO), informatycznej (CIO) i technologicznej (CTO). To właśnie od jakości tej relacji coraz częściej zależy sukces lub porażka transformacji. A relacje trójstronne rzadko bywają proste. Jak się porozumieć? Jak znaleźć wspólny język?

Jak współpracować tak, by budować synergii, zamiast gasić wewnętrzne problemy? Poniżej przedstawiam swój punkt widzenia, oparty na wieloletnim doświadczeniu doradczym we współpracy z klientami.

Trzy perspektywy – jeden cel?

Zacznijmy od weryfikacji, kto zasiada przy naszym stole. CFO koncentruje się na zwiększaniu przychodu, planowaniu, efektywności kosztowej, rentowności inwestycji i zarządzaniu ryzykiem. CIO odpowiada za stabilność systemów, bezpieczeństwo danych i architekturę IT, a CTO za innowacje, rozwój produktów oraz wdrażanie nowych technologii. I tu pojawiają się pierwsze wyzwania. Każda z tych osób posługuje się bowiem innym językiem, mierzy sukces własnymi wskaźnikami i działa w odmiennym horyzoncie czasowym. W efekcie zamiast synergii często obserwujemy napięcia w tych relacjach: finanse oczekują szybkiego zwrotu z inwestycji, IT stawia na stabilność, kontrolę ryzyka i bezpieczeństwo, a technologia chce eksperymentować i przyspieszać zmiany.

Dla mnie pojawia się tu pierwszy „red flag” – taki układ sprzyja bowiem powstawaniu silosów, które niestety blokują realną trans-

formację. Dlaczego? Ponieważ projekty cyfrowe zaczynają być realizowane fragmentarycznie, decyzje zapadają wolniej, a organizacje nie potrafią wówczas w pełni wykorzystać potencjału nowych technologii. Tymczasem skuteczna transformacja (a nie wymiana pojedynczego systemu na nowszy) wymaga myślenia systemowego, w którym finanse, IT i technologia działają jak jeden, zdrowy organizm.

Dlaczego silosy są dziś szczególnie groźne?

W erze dynamicznych zmian rynkowych i rosnącej presji konkurencyjnej tempo adaptacji decyduje o przetrwaniu. Firmy, które nie potrafią szybko integrować strategii biznesowej z technologiczną, tracą zdolność skalowania, obniżania kosztów i wprowadzania innowacji. Brak współpracy między CFO, CIO i CTO prowadzi do paradoksów: firmy inwestują miliony w nowe systemy, których wdrożenie nie generuje oczekiwanej wartości albo – z obawy przed przekroczeniem budżetu – blokują innowacyjne projekty.

Dodatkowo pojawienie się sztucznej inteligencji jeszcze bardziej komplikuje ten obraz. AI wymaga jednocześnie wysokiej jakości danych, nowoczesnej infrastruktury (w tym chmury), kompetencji technologicznych oraz precyzyjnego rachunku ekonomicznego. Bez ścisłej współpracy triady zarządzającej projekty AI szybko stają się kosztownymi eksperymentami, zamiast realnym źródłem przewagi konkurencyjnej.

Jak sprawnie działać?

W praktyce powtarzają się trzy mechanizmy: wspólne cele, wspólne KPI i wspólne forum decyzji. Coraz więcej organizacji przechodzi od klasycznego modelu „trzech silosów” do kon-



cepcji wspólnego przywództwa transformacyjnego. W tym podejściu CFO, CIO i CTO współtworzą jedną strategię cyfrową, opartą na jasno zdefiniowanych celach biznesowych, wspólnych priorytetach inwestycyjnych i mierzalnych efektach.

Kluczową zmianą jest wprowadzenie wspólnych wskaźników sukcesu. Zamiast osobnych KPI dla finansów, IT i technologii organizacje definiują cele nadrzędne, takie jak skrócenie czasu wprowadzania produktów na rynek, wzrost produktywności czy redukcja kosztów operacyjnych. Taki model sprzyja podejmowaniu decyzji, które optymalizują wynik całej firmy, a nie poszczególnych działów, i angażują wszystkie trzy funkcje w podobnym stopniu. Istotną rolę odgrywają również stałe komitety decyzyjne, w których CFO, CIO i CTO wspólnie

priorytetyzują projekty, alokują budżety i oceniają postępy. Dzięki temu transformacja przestaje być serią rozproszonych inicjatyw, a staje się spójnym programem zmian.

Wspólna droga

Jednym z największych wyzwań jest zmiana narracji wokół technologii. Zamiast mówić o migracji do chmury, modernizacji systemów czy wdrażaniu AI, liderzy powinni koncentrować się na wartości biznesowej: skróceniu cyklu produkcyjnego, poprawie jakości obsługi klienta, zwiększeniu elastyczności operacyjnej czy ograniczeniu kosztów. Taki język jest zrozumiały zarówno dla finansów, jak i dla zarządu, a jednocześnie nadaje projektom technologicznym realny sens strategiczny.

Warto dodać, że przełamywanie silosów to nie tylko kwestia struktur i procesów, ale przede wszystkim kultury organizacyjnej. Skuteczne firmy budują środowisko, w którym CFO, CIO i CTO uczą się od siebie nawzajem: finanse lepiej rozumieją technologię, IT poznaje mechanizmy controllingowe, a technologia zyskuje szerszą perspektywę biznesową. Taka wzajemna edukacja sprzyja podejmowaniu odważniejszych, ale bardziej świadomych decyzji.

Zgoda buduje.

Niezgoda rujnuje

Cyfrowa transformacja nie dzieje się w prezentacjach ani w centrach danych. Rozstrzyga się przy stole zarządu – w sposobie podejmowania decyzji, ustalania priorytetów i rozliczania efektów. Tam, gdzie CFO, CIO i CTO potrafią ze sobą rozmawiać, szybciej zapadają decyzje, łatwiej jest testować nowe pomysły i skuteczniej kontrolować koszty. Tam, gdzie każdy broni własnego obszaru, transformacja zamienia się w serię kosztownych projektów bez realnej zmiany. A tam, gdzie pojawia się prawdziwa współpraca, technologia zaczyna wreszcie pracować na wynik biznesowy, a nie tylko na kolejne wdrożenia – i to niezależnie od branży.

W praktyce nie chodzi już o to, kto ma nowocześniejszą technologię, lecz kto potrafi lepiej z niej korzystać. A to wymaga wspólnej wizji, zaufania i gotowości do wyjścia poza własny silos. Bo dziś prawdziwa przewaga konkurencyjna rodzi się nie w kodzie, systemach czy arkuszach Excela, lecz na styku finansów, IT i technologii – tam, gdzie kończą się kompetencyjne granice, a zaczyna odpowiedzialność za całość biznesu.



Skuteczne firmy budują środowisko, w którym CFO, CIO i CTO uczą się od siebie nawzajem.

Cyberbezpieczeństwo element strategii finansowej

Cyfrizacja finansów zmieniła sposób, w jaki firmy zarządzają kapitałem, danymi i ryzykiem. Coraz większa część operacji finansowych odbywa się w środowisku cyfrowym – od płatności i rozliczeń, przez inwestycje, po zarządzanie aktywami. Wraz z tym procesem cyberbezpieczeństwo przestało być wyłącznie kwestią techniczną, a stało się jednym z kluczowych filarów strategii finansowej organizacji.

SŁAWEK ZAWADZKI

Co-CEO Kanga

Szczególne znaczenie ten temat zyskuje w obszarze kryptowalut i technologii blockchain, które z jednej strony wprowadzają nową jakość w zakresie bezpieczeństwa i transparentności, z drugiej – wymagają dojrzałego podejścia do zarządzania ryzykiem operacyjnym i edukacji użytkowników.

Cyberzagrożenia jako realne ryzyko finansowe

Ataki cybernetyczne coraz częściej uderzają bezpośrednio w obszar finansów. Ransomware, phishing, przejęcia kont, manipulacje transakcjami czy wycieki danych nie są dziś incydentami marginalnymi, lecz systemowym zagrożeniem dla stabilności firm. Skutki takich zdarzeń wykraczają daleko poza dział IT – wpływają na płynność finansową, reputację,

relacje z klientami i zdolność do kontynuowania działalności. W przypadku rynku kryptowalut skala odpowiedzialności jest jeszcze większa. Transakcje są nieodwracalne, a użytkownicy często samodzielnie odpowiadają za dostęp do swoich środków. To sprawia, że bezpieczeństwo staje się fundamentem zaufania do całego ekosystemu, a nie jedynie dodatkiem do oferty technologicznej.

Blockchain jako odpowiedź na część wyzwań

Technologie oparte na blockchainie wprowadzają rozwiązania, które w wielu aspektach podnoszą poziom bezpieczeństwa finansów cyfrowych. Rozproszony rejestr, kryptografia i brak pojedynczego punktu awarii znacząco utrudniają manipulację danymi czy fałszowanie zapisów transakcyjnych. Transparentność blockchaina pozwala na audytowalność operacji, co ma istotne znaczenie

zarówno dla użytkowników, jak i instytucji.

Jednocześnie warto podkreślić, że technologia sama w sobie nie eliminuje wszystkich zagrożeń. Najczęstszym celem ataków pozostaje człowiek – jego błędy, brak wiedzy lub pochopne decyzje. Dlatego bezpieczeństwo w świecie kryptowalut musi łączyć rozwiązania technologiczne z edukacją oraz odpowiednimi procedurami organizacyjnymi.

Ciągłość działania w świecie finansów cyfrowych

Z perspektywy strategii finansowej kluczowym pojęciem staje się dziś ciągłość działania. Firmy muszą być przygotowane na funkcjonowanie w warunkach zakłóceń – zarówno technologicznych, jak i regulacyjnych czy geopolitycznych. W obszarze kryptowalut oznacza to m.in. zabezpieczenie infrastruktury, redundancję systemów, odpowiednie procedury reagowania na incydenty oraz przejrzyste zasady zarządzania środkami klientów.

Coraz więcej organizacji postrzega odporność cyfrową jako element przewagi konkurencyjnej. Zdolność do nieprzerwanego działania, nawet w warunkach kryzysowych, przekłada się bezpośrednio na zaufanie użytkowników i stabilność biznesową.

Regulacje i bezpieczeństwo użytkowników

Wraz z dojrzewaniem rynku kryptowalut rośnie znaczenie regulacji, które mają na celu ochronę użytkowników i zwiększenie stabilności sektora. Kluczowe jest jednak, aby regulacje te były proporcjonalne i wspierały rozwój bezpiecznych technologii, zamiast ograniczać innowacyjność lub wypychać działalność do szarej strefy.

Z punktu widzenia cyberbezpieczeństwa skuteczne prawo powinno wzmacniać standardy ochrony danych, przejrzystość działania podmiotów oraz odpowiedzialność za zarządzanie środkami klientów. Jednocześnie żadna regulacja nie zastąpi świadomego korzystania z technologii i podstawowych zasad bezpieczeństwa po stronie użytkowników.



Firmy muszą być przygotowane na funkcjonowanie w warunkach zakłóceń – zarówno technologicznych, jak i regulacyjnych czy geopolitycznych.

Bezpieczeństwo jako fundament zaufania do finansów przyszłości

W świecie finansów cyfrowych zaufanie nie buduje się wyłącznie poprzez deklaracje, lecz poprzez realne standardy bezpieczeństwa, transparentność i konsekwentne działania. Kryptowaluty i blockchain pokazują, że technologia może być narzędziem zwiększającym odporność systemów finansowych, pod warunkiem że jest wdrażana w sposób odpowiedzialny i długofalowy.

Cyberbezpieczeństwo staje się dziś jednym z kluczowych elementów strategii finansowej – równie istotnym jak zarządzanie kapitałem czy zgodność regulacyjna. To od decyzji podejmowanych na poziomie rządów zależy, czy technologie finansowe będą źródłem stabilności i rozwoju, czy dodatkowym obszarem ryzyka.

Przyszłość finansów jest cyfrowa, ale jej fundamentem musi pozostać bezpieczeństwo. W świecie kryptowalut ochrona danych, środków i ciągłości działania nie jest dodatkiem, lecz warunkiem funkcjonowania całego ekosystemu. Firmy, które już dziś traktują cyberbezpieczeństwo jako strategiczny element finansów, będą najlepiej przygotowane na wyzwania nadchodzących lat.

AI w finansach: od automatyzacji do predykcji

Świadomość potencjału sztucznej inteligencji rośnie. Mimo to wciąż zadajemy sobie pytanie, w jaki sposób wykorzystać możliwości AI w praktyce – tak, by pomagała zwiększać efektywność, ograniczać koszty i ryzyko, skutecznie zmniejszać liczbę błędów oraz przyspieszać podejmowanie decyzji.



ŁUKASZ WRÓBEL
CBDO WEBCON

Choć skuteczne wdrożenia AI nie są jeszcze powszechne, jak przekonuje McKinsey, sztuczna inteligencja może być już dziś z sukcesem wykorzystywana w procesach

operacyjnych. Celem działów finansowych jest wykorzystanie AI do szybszej analizy danych oraz automatyzacji prowadzącej do odciążenia pracowników od powtarzalnych, rutynowych zadań. Kluczowym wyzwaniem jest to, by modele językowe i agenci AI stali się częścią ekosystemu firmowych systemów informatycznych i procesów – uzyskując bezpieczny dostęp do danych, a co za tym idzie, niezbędny do budowania wartości kontekst.

Jak wdrożyć AI, by wspierała zadania?

Dziś największe wyzwania związane z wykorzystaniem sztucznej inteligencji polegają na jej ukontekstowaniu. By móc skutecznie wspierać wykonywanie zadań i ułatwiać podejmowanie decyzji finansowych, modele językowe i agenci AI muszą funkcjonować w oparciu o rzeczywiste dane przedsiębiorstwa. Problem w tym, że wiele inicjatyw dotyczących procesów finansowych rozbija się o jakość danych lub możliwość uzyskania do nich bezpiecznego dostępu. Tymczasem bez dostępu do spójnych, kompletnych i aktualnych danych wartość sztucznej inteligencji jest ograniczona.

Dlatego coraz większego znaczenia nabierają platformy, których celem jest orkiestracja agentów AI w połączeniu z warstwą klasycznej automatyzacji procesów biznesowych

i workflow. Pozwalają one połączyć możliwości szybkiej digitalizacji procesów biznesowych – koniecznej w obszarach, które wciąż funkcjonują na papierze, w wiadomościach e-mail i arkuszach Excela – z funkcjonalnością analizy informacji pochodzących z istniejących systemów informatycznych.

Nasi klienci eksplorują możliwości automatycznej analizy treści przychodzących dokumentów i ich kategoryzacji z wykorzystaniem modeli językowych, po to, by skrócić czas od wpłynięcia dokumentu do podjęcia właściwego działania. Dzięki agentom AI umieszczonym w obrębie procesu są w stanie zautomatyzować część decyzji, w których podjęciu klasyczna automatyzacja dostępna dotychczas nie była w stanie skutecznie ich wesprzeć. Tam, gdzie decyzję podejmuje człowiek, dzięki wsparciu agen-

tów AI, modeli językowych i sieci neuronowych, może on skorzystać z obserwacji opartych na rzeczywistych danych historycznych oraz bieżącym kontekście.

Sztuczna inteligencja zapewnia również ogromne wsparcie w analizie i łączeniu informacji – na przykład w procesie uzgadniania dokumentów kosztowych z zamówieniami i umowami. Z drugiej strony AI bardzo skutecznie pomaga dbać o jakość wprowadzanych informacji, udostępniając nowe możliwości walidacji oraz analizy wyjątków.

Osadzenie AI w obrębie zdefiniowanych procesów i workflow pozwala szeroko wykorzystać nowe możliwości automatyzacji. Dzięki temu działom finansowym łatwiej reagować na zmiany, planować strategicznie i odpowiadać na potrzeby całej organizacji.

Real-time finance jako nowy standard funkcjonowania przedsiębiorstw

Jeszcze do niedawna sprawne raportowanie finansowe oznaczało terminowe zamknięcie miesiąca i rzetelne podsumowanie wyników. Dziś to za mało.

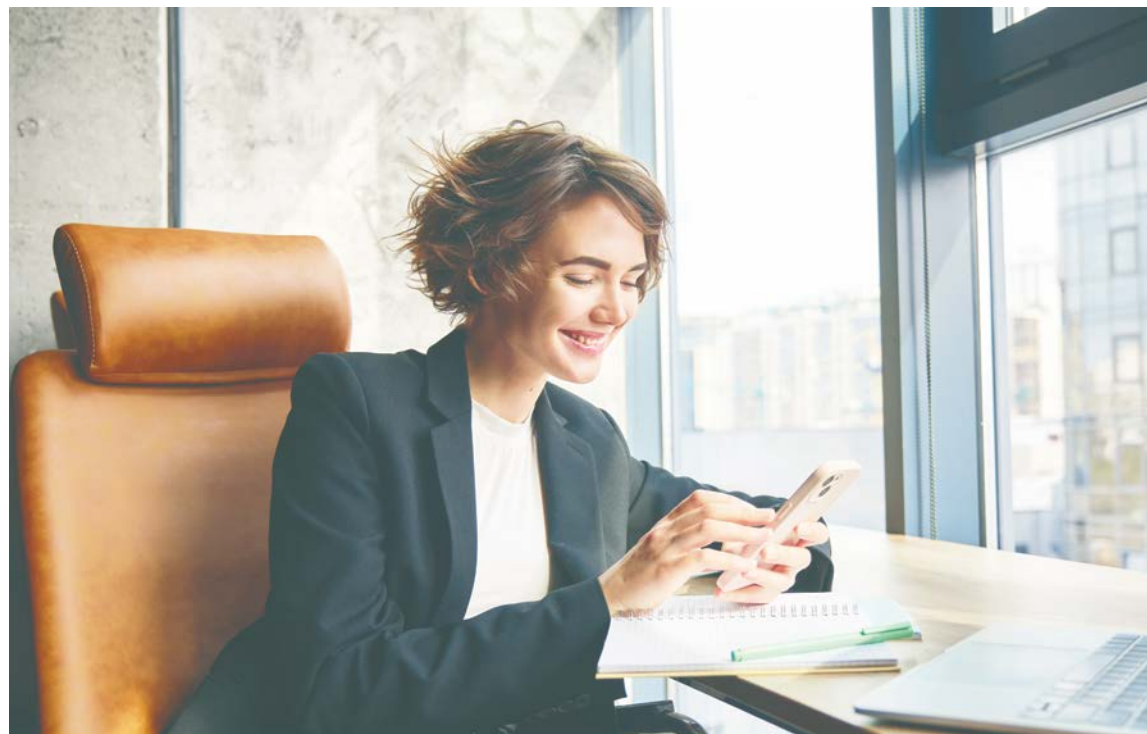


ALEKSANDRA ZAWADZKA
CFO w Alsendo

W warunkach rosnącej zmienności rynkowej, presji kosztowej i coraz szybszych decyzji działy finansowe nie mogą już pełnić wyłącznie roli „kronikarza” zdarzeń. W nowoczesnych organizacjach oczekuje się od nich czegoś więcej: zdolności do szybkiej interpretacji bieżącej sytuacji i realnego wsparcia w procesie podejmowania decyzji, zanim konsekwencje wyborów zarządu staną się widoczne w wynikach biznesowych firmy.

Istota ewolucji

Ma to odzwierciedlenie w samej ewolucji roli dyrektora finansowego w firmie. Aż 92 proc. badanych w raporcie KPMG „Perspektywy i wyzwania CFO na 2026 rok” wskazuje na istotne rozszerzenie zakresu swoich obowiązków w ostatnich latach o obszary pozafinansowe, takie jak analiza danych, IT czy zarządzanie zakupami. Ta zmiana to odpowiedź na fakt, że decyzje



finansowe coraz rzadziej dotyczą wyłącznie liczb, a częściej całego modelu funkcjonowania firmy. Finanse stają się punktem styku danych sprzedażowych, operacyjnych i logistycznych, a rola dyrektora finansowego zmierza w kierunku architekta systemu decyzyjnego, który pozwala zarządowi działać szybciej i świadomie.

To podejście jest szczególnie istotne w środowiskach o wysokiej dynamice operacyjnej, gdzie decyzje finansowe są ściśle powiązane z bieżącymi działaniami biznesu. W branżach takich jak e-commerce, gdzie sprzedaż, logistyka i obsługa klienta funkcjonują w czasie rzeczywistym, opóźnienie w dostępie do danych oznacza nie tylko ograniczoną widoczność, ale często realną utratę marży lub płynności. Finanse patrzące retrospektywnie na dane, nie są w stanie skutecznie wspierać decyzji podejmowanych tu i teraz.

Kluczowy elementem strategii działania CFO

Dlatego technologia – kiedyś wykorzystywana w działach finansowych jako narzędzie wspierające – staje się kluczowym elementem strategii działania CFO. Automatyzacja nie służy już tylko redukcji kosztów

czy upraszczaniu pojedynczych procesów, lecz uwolnieniu czasu i zasobów na analizę predykcijną. Narzędzia RPA, integracje API i automatyczny przepływ danych eliminują opóźnienia informacyjne, a transparentność procesów pozwala szybciej identyfikować ryzyka i odchylenia od planów. Zespoły finansowe zyskują możliwość bieżącego monitorowania sytuacji i pełnienia funkcji partnerów biznesowych dla CEO, zarządów i udziałowców poprzez aktywne doradztwo.

Kolejnym etapem tej technologicznej transformacji jest wykorzystanie zaawansowanej analityki i sztucznej inteligencji. Algorytmy AI i modele predykcyjne potrafią przetwarzać miliony rekordów w czasie rzeczywistym, identyfikując kluczowe trendy, potencjalne zagrożenia i możliwości wzrostu, pozwalając organizacji szybciej się rozwijać. W tradycyjnym modelu raportowania takie informacje pozostawałyby poza zasięgiem organizacji. W praktyce obejmuje to zaawansowane scenariusze analityczne, takie jak aktualizowane automatycznie i uwzględniające bieżące odchylenia prognozy, analizy cash flow uwarunkowane sezonowością, opóźnieniami płatności

„
Rolą CFO i zarządów będzie nadzór, interpretacja i podejmowanie decyzji strategicznych w oparciu o wiedzę, której tradycyjne modele raportowania nie były w stanie dostarczyć.

i zmiennymi makroekonomicznymi, a także wskazywanie jednorazowych zdarzeń, od błędnych faktur po nieoczekiwane ekspozycje kosztowe. Coraz ważniejsze stają się symulacje potencjalnych scenariuszy, dzięki którym można ocenić konsekwencje decyzji, zanim zostaną zaimplementowane, i ograniczyć ryzyko operacyjne. W efekcie AI przekształca kontroling w obszar proaktywny, który zamiast wyjaśniać wyniki, realnie wspiera kształtowanie przyszłych kierunków i strategicznych decyzji.

Nowy tryb funkcjonowania

Połączenie technologii, automatyzacji i zaawansowanej analizy danych w działach finansowych umożliwia przechodzenie organizacji na nowy tryb funkcjonowania: real-time finance. To podejście do zarządzania finansami, w którym dane finansowe i operacyjne są dostępne na bieżąco, a analiza i reakcja następują w czasie zbliżonym do rzeczywistego. Model real-time finance oznacza odejście od cyklicznego „zamrażania” danych na potrzeby raportów na rzecz ciągłego monitorowania kluczowych wskaźników, płynności i ryzyk. Dzięki temu finanse mogą nie tylko informować o wynikach, ale aktywnie wspierać decyzje w momencie ich podejmowania, a zarządy reagować na problemy zanim staną się krytyczne.

Rosnące znaczenie danych i technologii w firmach sprawia, że współpraca CFO z CTO i CIO staje się niezbędnym elementem skutecznego zarządzania. Finanse i technologia coraz częściej pracują nad wspólnym celem: zapewnieniem CEO i zarządowi aktualnego, wiarygodnego obrazu sytuacji oraz narzędzi do szybkiego reagowania na zmiany rynkowe. To na tym styku powstaje dziś realna przewaga konkurencyjna.

W perspektywie najbliższych lat real-time finance będzie coraz bardziej przypominać finansowego „autopilota” – zintegrowany system, który na bieżąco monitoruje kluczowe wskaźniki, identyfikuje ryzyka i rekomenduje możliwe działania, w konsekwencji realnie kształtując wartość spółki. Ostateczna odpowiedzialność pozostanie jednak po stronie ludzi. Rolą CFO i zarządów będzie nadzór, interpretacja i podejmowanie decyzji strategicznych w oparciu o wiedzę, której tradycyjne modele raportowania nie były w stanie dostarczyć. Firmy, które już dziś inwestują w ten sposób myślenia o finansach, zyskują nie tylko większą efektywność, ale przede wszystkim zdolność świadomego kształtowania swojej przyszłości.

„
Algorytmy AI i modele predykcyjne potrafią przetwarzać miliony rekordów w czasie rzeczywistym, identyfikując kluczowe trendy, potencjalne zagrożenia i możliwości wzrostu, pozwalając organizacji szybciej się rozwijać.