Prestige Conferences
BO LICZY SIĘ JAKOŚĆ



KONFERENCJA

ZARZĄDZANIE RYZYKIEM OPERACYJNYM 2026

AKTUALNE TRENDY I WYZWANIA

23-24 CZERWCA 2026

WARSAW REGENT HOTEL



GRZEGORZ DRĄG
Head of Non-Financial Risk Management /ORM/ESG mBank S.A.



EWA KACZYŃSKA
Partner Associate, Deloitte Advisory



AGNIESZKA ŁAPIŃSKA
Ekspert ds. Cyberbezpieczeństwa



ARKADIUSZ KAWULSKI
Radca Prawny, Ekspert w zakresie Outsourcingu i Prawa Bankowego



JAKUB STOLARCZYK
Wiceprezes Zarządu, White Berg TFI



OLGA ADAMSKA
Expert Lead – Fraud Investigation, ING Bank Śląski



PIOTR CZERKAS
Dyrektor Departamentu Zwalczania Nadużyć, BNP Parribas



ADW. JAN ZIOMEK
ekspert Fintech/ AML



MARCIN DASZKIEWICZ
Kierownik ds. Defraudacji w Kanałach Zdalnych, Provident Polska S.A.



PIOTR JAWORSKI
Certyfikowany audytor wewnętrzny, mentor oraz trener biznesu



KAROL KONOPKA
Inspektor Nadzoru/ Menedżer ds. Zarządzania Ryzykiem, Erste Securities Polska S.A.



ŁUKASZ SAMBORSKI
Ex-Alior, Dyrektor Departamentu Zarządzania Ryzykiem Operacyjnym/ Lider Programu CK AI



MARCIN PYCKA
FCCA, CIA, CISA, CertDA, MANAGER Technology and Operations Audit, ING HUBS



RADOSŁAW PODGÓRSKI
Audytor , TÜV Nord Polska



TADEUSZ PEKSA
Senior Security Consultant/Cyber Security Division Sii Poland Senior Control Manager/GCIO HSBC



MACIEJ BUCZAK
Ekspert zarządzania ryzykiem modeli, ryzyka operacyjnego i kredytowego

ZAGADNIENIA

- Ryzyko geopolityczne
- Tradycyjne kierunki i nowe wymiary/Kanały transmisji ryzyka do sektora bankowego
- Pomiar ryzyka geopolitycznego i ograniczenia klasycznej kwantyfikacji
- Stress testy i analiza scenariuszowa
- Ryzyko dostawców ICT wobec wojen hybrydowych oraz cyberataków
- Taktyki państwowych grup hackerskich - APT wykorzystujących dostawców jako wektor ataku na sektor finansowy
- Wpływ dezinformacji na stabilność dostawców i zaufanie do sektora finansowego
- Zarządzanie ryzykiem stron trzecich (Third Party Risk Management – TPRM)
- Audyt Dora w organizacji
- Defraudacje w cyfrowych kanałach dostępu. Wybrane ataki na klientów banków - przykłady z życia wzięte.
- Oszustwa wewnętrzne
- Fraud w Płatnościach – problem technologiczny czy compliance
- People Risk Scan - Odporność Społeczna Organizacji
- Product Governance
- Zarządzanie produktowe a aktualne priorytety nadzorcze KNF w kontekście MIFiD 2
- Nowe podejście do ryzyka operacyjnego w CRR3- wyzwania w zakresie danych i ich wpływ na wymogi kapitałowe i raportowanie
- AI a ryzyko operacyjne /Taksonomia ryzyk generowanych przez systemy AI/ EU AI Act i inne regulacje a ryzyko operacyjne w banku/ AI governance w banku
- AI w monitoringu KRI i ryzyka stron trzecich
- Ryzyko operacyjne w IT: Wykorzystanie klasycznych metod AI do identyfikacji i oceny ryzyka
- Klasyczne metody AI w identyfikacji ryzyka
- Ocena i kwantyfikacja ryzyk
- Shadow AI — ryzyko, o którym zarząd nie wie
- Zarządzanie AI – Kontrola ryzyka technologicznego, cybernetycznego i modeli w ramach zastosowań Gen AI / Agentic AI
- Modelowanie ryzyka operacyjnego

DZIEŃ I , 23 CZERWCA 2026

8:00 – 8:50 *Powitalny poczęstunek. Rejestracja*

9:00 – 9:05 *Rozpoczęcie konferencji*

9:05 – 9:45

Ryzyko geopolityczne w bankowości – od definicji do strategii

- *Wprowadzenie – dlaczego dziś mówimy o ryzyku geopolitycznym*
- *Podstawowe definicje i ramy pojęciowe - czym jest obecnie ryzyko geopolityczne*
- *Źródła i czynniki ryzyka geopolitycznego – tradycyjne kierunki i nowe wymiary*
- *Kanały transmisji ryzyka do sektora bankowego*
- *Pomiar ryzyka geopolitycznego i ograniczenia klasycznej kwantyfikacji*
- *Ryzyko geopolityczne w ramach systemu zarządzania ryzykiem*
- *Stress testy i analiza scenariuszowa*
- *Ryzyko geopolityczne jako stały element dyskusji zarządczej*

***Grzegorz Drąg**, Head of Non-Financial Risk Management /ORM/ESG mBank S.A.*

9:45 –10:20

Nowe podejście do ryzyka operacyjnego w CRR3- wyzwania w zakresie danych i ich wpływ na wymogi kapitałowe i raportowanie

- *Zasady gromadzenia danych o zdarzeniach i stratach operacyjnych według CRR3*
- *Nowa taksonomia zdarzeń operacyjnych EBA*
- *Zmiany w zakresie raportowania zdarzeń operacyjnych*
- *Uwzględnienie strat operacyjnych w nowej metodzie standardowej kalkulacji wymogu kapitałowego*

***Ewa Kaczyńska**, Partner Associate, Deloitte Advisory*

10:20 - 10:35 *Przerwa Kawowa*

10:35 -11:20

Ryzyko dostawców ICT wobec wojen hybrydowych oraz cyberataków

- *Zarządzanie ryzykiem dostawców ICT w dobie konfliktów zbrojnych*
- *Taktyki państwowych grup hackerskich - APT wykorzystujących dostawców jako wektor ataku na sektor finansowy*
- *W jaki sposób dezinformacja i operacje psychologiczne maskują rzeczywiste ataki grup APT na infrastrukturę ICT*
- *Zniszczenia fizyczne związane z wojną, sabotażem, a ciągłość działania dostawców*
- *Wpływ dezinformacji na stabilność dostawców i zaufanie do sektora finansowego*

***Agnieszka Łapińska**, Ekspert ds. Cyberbezpieczeństwa*

11:20 -12:00

Zarządzanie ryzykiem stron trzecich (Third Party Risk Management – TPRM)

- *koncentracja dostawców ICT i cloud,*
- *rzeczywista kontrola podwykonawców 4th / 5th party,*
- *ryzyko zerwania łańcuchów dostaw,*
- *TPRM w świetle DORA i nadzoru onsite.*

***Arek Kawulski**, Radca Prawny, Ekspert w zakresie Outsourcingu i Prawa Bankowego*

12:00-12:30

AUDYT DORA w ORGANIZACJI - wdrożenia zrealizowane, czas na ocenę jakości tego wdrożenia.

- *Rola i zadania audytu w zakresie DORA jako trzeciej linii obrony w organizacji*
- *Charakterystyka komórki audytu, zasoby, plan audytu*
- *Obszary podatne na deficyty - obserwacje praktyczne.*

***Jakub Stolarczyk**, Wiceprezes Zarządu White Berg TFI*

12:30-12:45

Dyskusja

12:45 – 13:30 *LUNCH*

13:30 – 14:20 **Defraudacje w cyfrowych kanałach dostępu. Wybrane ataki na klientów banków - przykłady z życia wzięte.**

- *Phishing/Smishing/Quishing, czyli dystrybucja fałszywych linków,*
- *Vishing/Spoofing, czyli telefoniczne podszycie pod pracownika banku,*
- *NFC Relay Attack, czyli kradzież sygnału płatności zbliżeniowej kartą,*
- *Oszustwo na płatność OLX/Vinted,*
- *Oszustwo „na zadania", czyli fałszywe oferty pracy,*
- *Oszustwo inwestycyjne,*
- *Deepfake,*
- *Oszustwo na znajomego z Facebook'a,*
- *Oszustwa „na legendę" (wnuczka, policjanta, Fafika, amerykańskiego żołnierza),*
- *Jak poczuć się jeszcze bezpieczniej?.*

***Olga Adamska**, Expert Lead – Fraud Investigation, ING Bank Śląski*

14:20 – 15:05 **Oszustwa Wewnętrzne**

- *Najczęściej występujące rodzaje nadużyć wewnętrznych,*
- *Nadużycie wewnętrzne - skutki*
- *Postępowania dot. nadużyć wewnętrznych*
- *Jak mitygować ryzyko?*

***Piotr Czerkas**, Dyrektor Departamentu Zwalczania Nadużyć, BNP Parribas*

15:05 -15:15 *przerwa kawowa*

15:15-15:45 **Fraud w Płatnościach – problem technologiczny czy compliance**

***Adw. Jan Ziomek**, Ekspert Fintech/ Aml*

15:45 - 16:15 **Fraud never sleeps — wyzwania antyfraudowe na rynku pożyczkowym .**

- *Jakie schematy fraudowe dominują dziś w branży lendingowej.*
- *Klasyczne i nieklasyczne metody obrony.*
- *Realne wyzwania, z którymi mierzy się zespół antyfraudowy Provident Polska.*
- *Konkretne przypadki i podejścia, które sprawdzają się w praktyce, i te, które okazały się lekcją pokory.*
- *Zamiast teorii - perspektywa ludzi budujących fraud detection na żywym portfelu.*

***Marcin Daszkiewicz**, Kierownik ds. Defraudacji Kanałach Zdalnych, Provident Polska*

16:15 - 16:30 **Dyskusja**

Zakończenie I DNIA KONFERENCJI

DZIEŃ II , 24 CZERWCA 2026

8:15 – 8:55 *Poranny poczęstunek*

9:00 – 9:50

People Risk Scan - Odporność Społeczna Organizacji

***Piotr Jaworski** , Certyfikowany audytor wewnętrzny, mentor oraz trener biznesu*

9:50 – 10:40

Zarządzanie produktowe a aktualne priorytety nadzorcze KNF w kontekście MIFiD 2

- *Aktualne priorytety nadzorcze*
- *Omówienie ostatnich kar i akcji nadzorczych*
- *Prawidłowe zarządzanie produktowe w świetle MIFiD2 – na co zwracać uwagę , jak prawidłowo konstruować sprzedaż i systemy premiowe*

***Karol Konopka**, Inspektor Nadzoru/ Menedżer ds. Zarządzania Ryzykiem, Erste Securities Polska S.A.*

10:40 -11:00 *Przerwa Kawowa*

11:00– 11:45

AI a OpRisk: między innowacją a nową kategorią ryzyka

- *AI risk — nowa kategoria ryzyka operacyjnego. Taksonomia ryzyk generowanych przez systemy AI: błędy agentów, halucynacje modeli, bias algorytmiczny, zależność od danych i dostawców. Jak identyfikować, klasyfikować i mitygować ryzyka, których jeszcze pięć lat temu nie było.*
- *EU AI Act i inne regulacje a ryzyko operacyjne w banku Klasyfikacja systemów AI w banku według poziomów ryzyka, obowiązki dokumentacyjne i nadzorcze wynikające z AI Act, DORA i wytycznych EBA. Co konkretnie zmienia się w pracy departamentów ryzyka operacyjnego i compliance.*
- *AI governance w banku — wplecenie AI w enterprise risk management Modele organizacyjne nadzoru nad AI (3 linie obrony), budowanie polityki AI governance i integracja z istniejącym frameworkiem zarządzania ryzykiem.*
- *AI jako narzędzie w rękach zarządzającego ryzykiem operacyjnym Automatyzacja monitoringu ryzyka, analityka predykcyjna wykrywająca zaburzenia operacyjne zanim wystąpią, AI w monitoringu KRI i ryzyka stron trzecich. Od reaktywnego zarządzania incydentami do ciągłego, proaktywnego nadzoru.*

***Łukasz Samborski**, Ex-Alior, Dyrektor Departamentu Zarządzania Ryzykiem Operacyjnym/Lider Programu CK AI*

11:45 -12:30

„Ryzyko operacyjne w IT: Wykorzystanie klasycznych metod AI do identyfikacji i oceny ryzyka”

- *Kontekst ryzyka operacyjnego w IT: Definicja i specyfika ryzyka operacyjnego w środowisku technologicznym, uwzględniająca kwestie ciągłości działania i bezpieczeństwa systemów.*
- *Klasyczne metody AI w identyfikacji ryzyka: Omówienie zastosowania tradycyjnych technik uczenia maszynowego (np. algorytmy klasyfikacyjne, regresja, drzewa decyzyjne) do analizy historycznych danych o incydentach operacyjnych.*
- *Wykrywanie anomalii i wzorców: Praktyczne przykłady wykorzystania klasycznej analityki do automatycznego identyfikowania nietypowych zdarzeń i potencjalnych źródeł ryzyka operacyjnego w IT.*
- *Ocena i kwantyfikacja ryzyka: Prezentacja, jak proste modele predykcyjne mogą wspierać ocenę prawdopodobieństwa i wpływu zdarzeń ryzyka IT, w tym monitorowanie wskaźników KRI.*

***Marcin Pycka** FCCA, CIA, CISA, CertDA, MANAGER Technology and Operations Audit, ING Hubs*

12:30 -13:00

Dyskusja

13:00 -13:50 *Lunch*

13:50 – 14:35

Zarządzanie AI – Kontrola ryzyka technologicznego, cybernetycznego i modeli w ramach zastosowań Gen AI / Agentic AI

- *Jak szybko i bezpiecznie wdrożyć Agentic AI w sektorze bankowym?*
- *Jakie są kluczowe kontrole w obszarze ryzyka modelowego, technologicznego i cybernetycznego?*
- *Jak radzić sobie z Vibe Coding lub Mythos nowej generacji?*

***Tadeusz Peksa** , Senior Security Consultant/Cyber Security Division Sii Poland Senior Control Manager/GCIO HSBC*

14:35 – 15:15

MODELOWANIE RYZYKA OPERACYJNEGO

Dlaczego modele nie radzą sobie z przewidywaniem katastrof?"

- *Czym jest katastrofa w świecie natury, a czym w finansach?*
- *Trudności w modelowaniu natury*
- *Błędne interpretacje zdarzenia rzadkiego?*
- *Modele zdarzeń skrajnych w ekonomii?*
- *Czy kryzysy da się przewidzieć?*

***Maciej Buczak**, Ekspert ds. Zarządzania Ryzykiem Modeli, ryzyka operacyjnego i kredytowego*

15:15 – 16:00

Shadow AI — ryzyko, o którym zarząd nie wie

- *Czym jest Shadow AI i skąd się wzięło*
- *Katalog ryzyk*
- *Dlaczego klasyczne zabezpieczenia zawodzą?*
- *Podsumowanie i Q&A*

***Radosław Podgórski** , Audytor , TÜV Nord Polska*

16:00

Zakończenie konferencji



ZAPRASZAMY!