



AI W AUDYCIE

JAN ANISIMOWICZ

PMP, CISM, CRISC, ESG

Chief Solutions Architect, C&F SA

>>> WPROWADZENIE

Sztuczna inteligencja (AI) rewolucjonizuje procesy audytowe, oferując nowe możliwości w zakresie automatyzacji, analizy danych oraz wykrywania nieprawidłowości. Jednakże, szybki rozwój AI budzi również liczne obawy wśród interesariuszy.

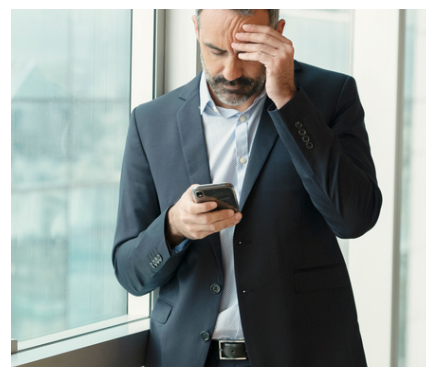


>>> KORZYŚCI AI W AUDYCIE

- **Automatyzacja Procesów:** AI pozwala na automatyzację rutynowych zadań, co zwiększa efektywność i redukuje błędy ludzkie.
- **Zaawansowana Analiza Danych:** Algorytmy AI analizują duże zbiory danych, identyfikując wzorce i anomalie, które mogą wskazywać na nieprawidłowości.
- **Ciągłe Monitorowanie:** Systemy AI umożliwiają ciągłe monitorowanie transakcji i działań, co pomaga w szybkim wykrywaniu oszustw i innych zagrożeń.

>>> OBAWY STAKEHOLDERÓW

- **Nieprzewidywalność Algorytmów:** Istnieje ryzyko, że AI może działać w sposób nieprzewidywalny, co może prowadzić do błędnych decyzji audytowych.
- **Prywatność i Ochrona Danych:** AI przetwarza duże ilości danych osobowych, co rodzi obawy o naruszenie prywatności i ochrony danych.
- **Ataki Cybernetyczne:** AI, będąc częścią infrastruktury IT, może stać się celem ataków cybernetycznych.
- **Brak Transparentności:** Algorytmy AI mogą działać jako "czarne skrzynki", co utrudnia zrozumienie, jak i dlaczego podjęły określone decyzje.
- **Odpowiedzialność Prawna:** Kwestie prawne i regulacyjne związane z odpowiedzialnością za decyzje podejmowane przez AI są wciąż niejasne.



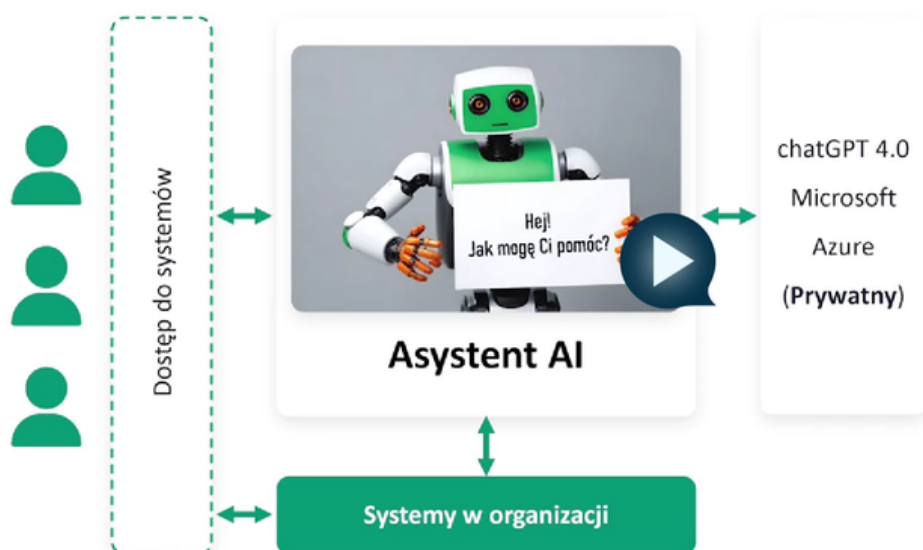
>>> REKOMENDACJE BEZPIECZEŃSTWA AI

- **Transparentność Algorytmów:** Dokumentowanie procesów decyzyjnych algorytmów.
- **Bezpieczeństwo Danych:** Ochrona danych wejściowych i wyjściowych przed nieautoryzowanym dostępem.
- **Zarządzanie Ryzykiem:** Regularna ocena ryzyka związanego z implementacją AI.
- **Ciągłe Monitorowanie i Audyt:** Regularne audyty i monitorowanie działania AI.
- **Szkolenie Personelu:** Edukowanie pracowników na temat zagrożeń i praktyk bezpieczeństwa.
- **Zgodność z Regulacjami:** Przestrzeganie regulacji prawnych i norm branżowych.
- **Etyka i Odpowiedzialność:** Ustanowienie zasad etycznych i określenie odpowiedzialności za decyzje AI.
- **Bezpieczeństwo Systemowe:** Implementacja technicznych środków zabezpieczających infrastrukturę IT.



>>> REGULACJE I STANDARDY

- **EU AI Act:** Klasyfikacja systemów AI na podstawie poziomu ryzyka oraz wymogi dotyczące przejrzystości i bezpieczeństwa.
- **ISO 42001:** Międzynarodowy standard zarządzania bezpieczeństwem AI, obejmujący ocenę ryzyka, ciągłe doskonalenie oraz zgodność z przepisami.



>>> PODSUMOWANIE

Dzięki odpowiedniemu podejściu do bezpieczeństwa, transparentności i zgodności z regulacjami, organizacje mogą bezpiecznie wdrażać AI, minimalizując ryzyko i maksymalizując korzyści.