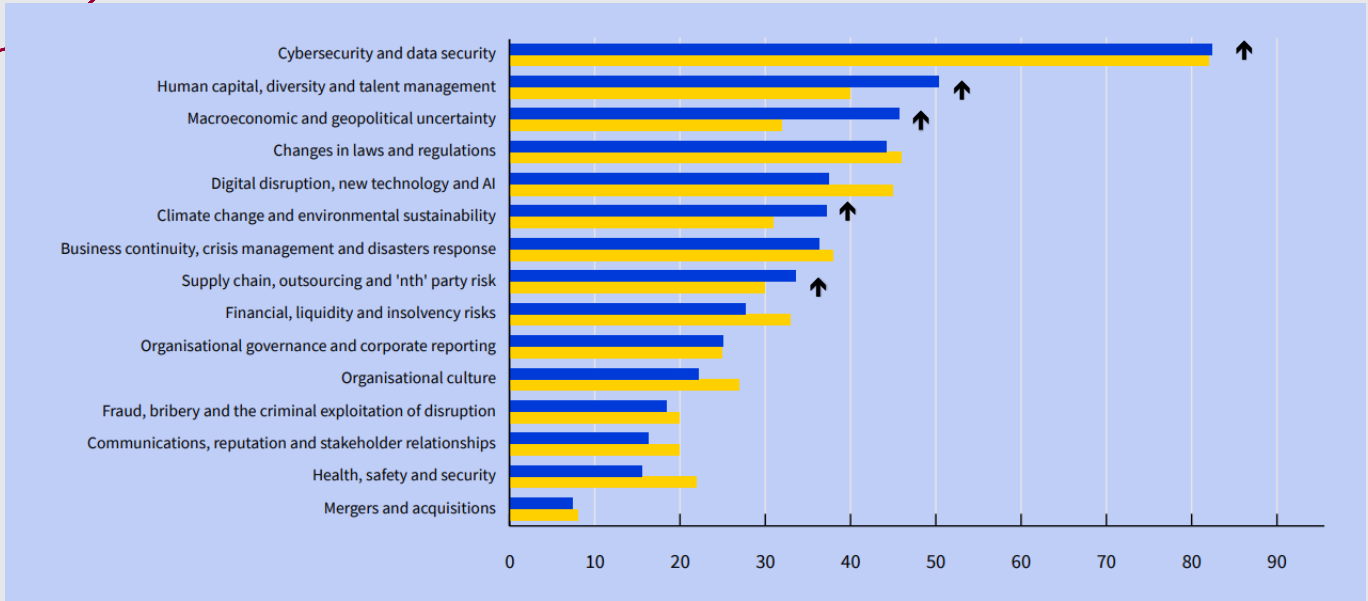
PIU
Polska Izba Ubezpieczeń

Kluczowe ryzyka a plan audytu 2023

Warszawa, 29.11.2022 r.

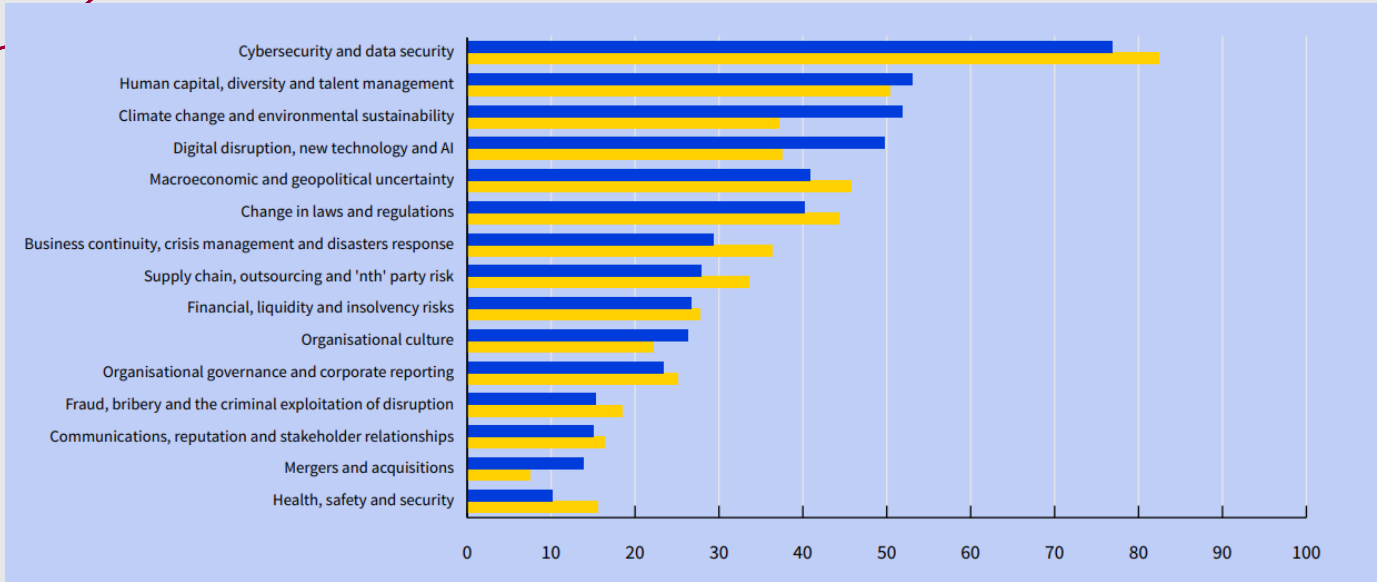
- Plan audytu 2023 – jakie ryzyka uwzględnić w analizie?
- Jak audytować kluczowe ryzyka? Przykłady tematów audytowych

Kluczowe ryzyka w 2023



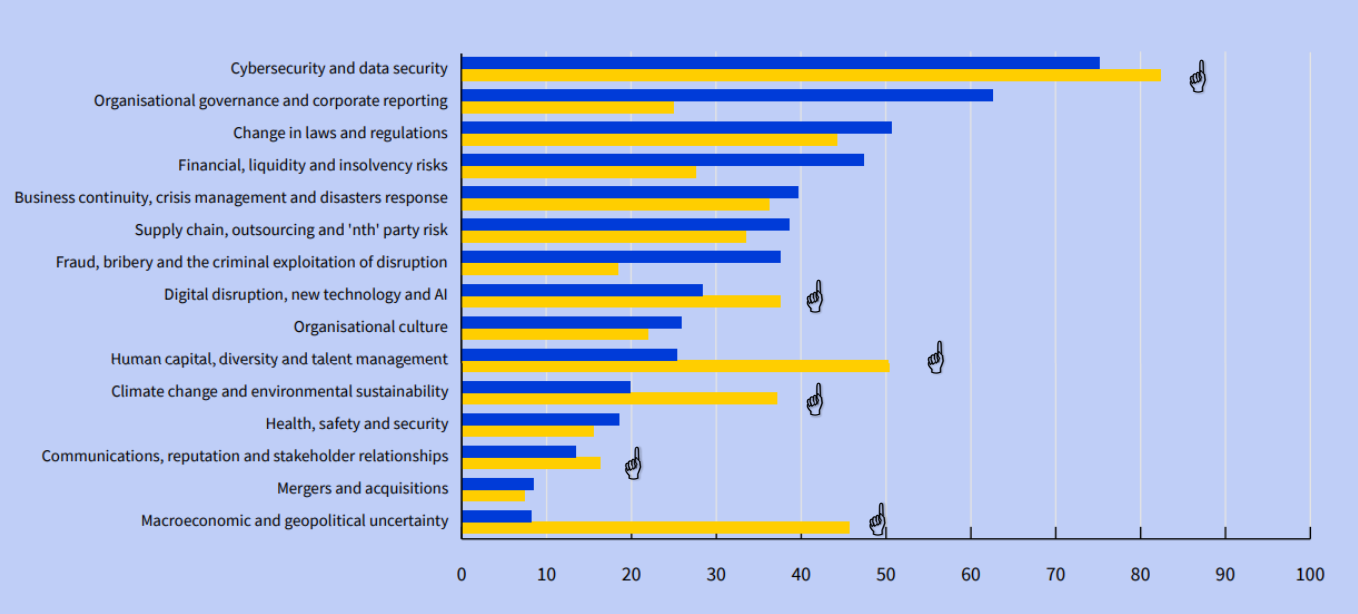
Źródło: 2023 Risk in focus. Hot topics for internal auditors. ECIIA

Kluczowe ryzyka w 2026



Źródło: 2023 Risk in focus. Hot topics for internal auditors. ECIIA

Istotność ryzyka a czas poświęcony audytom w danym obszarze



Źródło: 2023 Risk in focus. Hot topics for internal auditors. ECIIA

Spędzony czas

Istotność/priorytet ryzyka

Wybrane ryzyka – kluczowe wyzwania i przykładowe obszary do audytu

Cyberbezpieczeństwo

Przykłady zagrożeń/wyzwań:

- Malware czyli złośliwe oprogramowanie, stworzone z myślą o uszkodzeniu sprzętu lub kradzieży danych (np. uszkodzenie podstawowych funkcjonalności systemu, skasowanie danych, otworzenie, tzw. tylnych drzwi do kolejnych ataków, blokady komputera lub atakowania reklamami):
  - wirusy, robaki, konie trojańskie – programy albo fragmenty kodu, które pasożytujące na programach wykorzystywanych przez sprzęt i zajmujące jego zasoby; wirusy dołączają się do innych programów i modyfikują je tak, żeby się powielać
  - ransomware, złośliwe oprogramowanie, szyfrujące ważne pliki przechowywane na dysku lokalnym i sieciowym lub instalowane w celu żądania okupu za ich rozszyfrowanie
  - spyware – oprogramowanie szpiegujące (zbiera informacje o aktywności użytkownika, np. odwiedzanych stronach internetowych)
  - adware – odpowiadające za natrętnie wyświetlane reklamy
- Inżynieria społeczna i wyłudzanie informacji, poprzez wykorzystania zaufania osób, w celu nakłonienia ich do przekazania informacji o koncie lub pobrania złośliwego oprogramowania

Przykłady tematów audytowych / obszarów do audytu:

- Audyty techniczne w obszarze cybersecurity objemujące architekturę i konfigurację systemów bezpieczeństwa oraz procesów zapewniających ochronę przed cyberbezpieczeństwem (np. zarządzanie podatnościami, wykonywanie testów penetracyjnych)
- Audyt bezpieczeństwa przed ransomware, w tym w szczególności ochrona backupów przed ransomware
- Testy procedur Distaster Recovery (DR) w kontekście ransomware (plany IT na konieczność odtworzenia systemów po ataku ransomware - konieczność odtworzenia systemów z backup, nie tylko przełączenie systemu).

Wybrane ryzyka – kluczowe wyzwania i przykładowe obszary do audytu

Bezpieczeństwo danych

Przykłady zagrożeń/wyzwań:

- Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników, np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, nieukrywanie adresów mailowych przy wysyłce masowej, nieprawidłowe usunięcie / anonimizowanie danych – prowadzące do udostępnienia danych osobowych lub wrażliwych np. klientów
- Brak nadzoru nad dostępem uprzywilejowanym (np. współdzielenie kont, niemonitorowanie sesji użytkowników uprzywilejowanych mogące prowadzić do nieidentyfikowalnych anomalii / nadużyć)
- Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów, prowadzące do utraty nośników danych
- Nieodpowiednie zabezpieczenie sprzętu IT czy oprogramowania przed wyciekiem lub utratą danych osobowych

Przykłady tematów audytowych / obszarów do audytu:

- Audyt procesu zarządzania incydentami i problemami
- Proces zbierania, przetwarzania, archiwizacji, retencji i anonimizacji danych
- Audyt dostępu fizycznego (np. do biura, sal konferencyjnych, gabinetów)
- Kontrole dostępu do danych (np. w systemach, w folderach sieciowych)
- Mechanizmy kontrolne po stronie zewnętrznych dostawców usług
- Audyt nadawania i odbierania uprawnień
- Audyt DLP (Data Leakage Prevention)
- Audyt w zakresie zgód marketingowych oraz uprawnionego kontaktu z klientem

Wybrane ryzyka – kluczowe wyzwania i przykładowe obszary do audytu

Digital disruption, Artificial Intelligence (rozwój nowych technologii)

Przykłady zagrożeń/wyzwań:

- Wyzwania na poziomie projektów strategicznych w zakresie robotyki/automatyzacji: np. nieskuteczna analiza kosztów i korzyści, niewystarczające umiejętności pracowników na poziomie definiowania wymagań
- Niewystarczające oceny technologii i niewłaściwy wybór dostawcy (np. w młodych start-up'ach brak kompetencji, rotacja personelu, braku trwałości i stabilności biznesu)
- Niewystarczające testowanie rozwiązań i wpływy na obsługę klienta / odczucia klienta (np. klienci skarżący się na chat-boty)
- Błędy technologiczne (np. niewystarczające mechanizmy szyfrowania, brak logiki lub błędy algorytmu, brak dokładności i integralności danych, niewystarczające testy regresji, nieautoryzowane zmiany produkcyjne)
- Niejednoznaczna odpowiedzialność za szkody spowodowane przez urządzenie lub usługę sterowane przez sztuczną inteligencję

Przykłady tematów audytowych / obszarów do audytu:

- Zarządzanie innowacjami i R&D (w tym business case – akceptacja i rozliczenie po projekcie, powiązanie inicjatyw ze strategią)
- Zarządzanie projektami oraz rozwojem systemów i technologii informatycznych (w tym aspekty jakości/bezpieczeństwa danych, RODO)
- Zarządzanie architekturą systemów IT (strategia IT i docelowa roadmapa IT oraz digitalizacji organizacji, dług technologiczny)
- Zarządzanie danymi (w tym mapowanie kluczowych danych na potrzeby procesów decyzyjnych, analiza źródeł danych, przepływów danych, jakości)
- Robot Processing Automation & Artificial Intelligence (w tym proces oceny technologii i wyboru partnera, walidacja wymagań, proces oceny ryzyka i wpływu, przeglądy logiki i testowanie, testowanie integralności)
- Audyt Chmury
- Wykorzystanie data analytics w procedurach audytowych

Wybrane ryzyka – kluczowe wyzwania i przykładowe obszary do audytu

Human Capital (Zarządzanie Kapitałem Ludzkim)

Przykłady zagrożeń/wyzwań:

- Brak dostępności zasobów ludzkich oraz problem z utrzymaniem kluczowych pracowników (wysokie wskaźniki rotacji)
- Rozwój hybrydowych i zdalnych modeli pracy mający wpływ zmniejszanie lojalności i przywiązania do marki, zespołu, zmniejszenie zaangażowania, produktywności i efektywności pracy
- Konieczność zaadresowania konkretnych potrzeb pracowników („work-life balance", elastyczność środowiska pracy, możliwości rozwoju kariery i szkoleń, zrozumienia dla indywidualnych celów zatrudnionych czy kwestii społecznej odpowiedzialności biznesu, zbieżność wartości i misji firmy z potrzebami i wartościami pracownika)

Przykłady tematów audytowych / obszarów do audytu:

- Proces strategicznego zarządzania zasobami ludzkimi (krótko- i długoterminowego), predykcyjnego planowania zapotrzebowania na zasoby (z uwzględnieniem krytycznych/kluczowych kompetencji potrzebnych firmie do realizacji celów. np. programistów, analityków, itd.)
- Proces planowania sukcesji/zastępowalności („succession planning"), analizy porównawcze w zakresie systemów wynagrodzeniowych oraz programów benefitowych. Przegląd programów „wellbeing" (komunikacja, dopasowanie do potrzeb pracowniczych, wykorzystanie, informacja zwrotna od pracowników)
- Proces szkolenia, rozwoju i utrzymania talentów oraz kluczowych kompetencji
- Proces rekrutacji (przegląd założeń dotyczących rekrutacji w tym narzędzi i kanałów rekrutacyjnych, analiza planów retencyjnych, analiza otwartych pozycji, czasu rekrutacji, ocena ryzyk w zakresie niezrealizowanych rekrutacji – wpływ na biznes)

Wybrane ryzyka – kluczowe wyzwania i przykładowe obszary do audytu

Zmiany makroekonomiczne i geopolityczne

Przykłady zagrożeń/wyzwań:

- Zagrożenie realizacji celów wzrostowych oraz finansowych związane ze światową recesją, skutkami inwazji Rosji na Ukrainę, inflacja (np. ryzyko większych kosztów, mniejszego zysku, wydłużonego okresu zwrotu z inwestycji)
- Zmiany wyceny instrumentów lub zmiany otwartych pozycji w instrumentach finansowych (np. akcji, obligacji), których ceny wprost zależą od sytuacji na rynkach lokalnych/zagranicznych
- Inflacja i wzrost kosztów w obszarze likwidacji szkód wpływające na wzrost wysokości świadczeń oraz kosztów obsługi likwidacji szkód
- Klienci skłonni do rezygnacji z ubezpieczania pewnych ryzyk w celu redukcji kosztów
- Zmiany polityki kapitałowej właścicieli (spółek matek) wobec krajowych ubezpieczycieli (spółek zależnych)

Przykłady tematów audytowych / obszarów do audytu:

- Proces zarządzania aktywami, płynnością, strategicznej alokacji aktywów
- Optymalizacja kosztowa (ocena wpływu działań nastawionych na obniżenie/optymalizację kosztów na realizację innych celów/procesów biznesowych, wpływ na obsługę klienta, wpływ na realizację kontroli w różnych obszarach, wpływ na obciążenie pracowników i poziom nadgodzin)
- Audytu procesu zarządzania produktami (z uwzględnieniem walidacji kluczowych parametrów ekonomicznych dla produktów,
- Przegląd założeń w procesie kalkulacji rezerw techniczno - ubezpieczeniowych
- Przegląd strategii reasekuracyjnej (w uwzględnieniem ratingów i spójności ratingów reasekuratorów)
- Audyt modelu ryzyka oraz procedur zarządzania ryzykiem i wyceny ryzyka

Wybrane ryzyka – kluczowe wyzwania i przykładowe obszary do audytu

Environmental sustainability (społeczna odpowiedzialność biznesu)

Przykłady zagrożeń/wyzwań:

- Konieczność przemodelowania procesów zarządzania produktem, zbudowania procesów raportowych dla potrzeb ujawnień (np. obowiązek publikacji strategii dotyczących wprowadzania do działalności ryzyk dla zrównoważonego rozwoju)
- Konieczność uwzględniania pozafinansowych ryzyk w procesach inwestycyjnych i finansowych
- Brak lub ograniczona dostępność danych na temat kontrahentów w zakresie ESG, niska jakość ujawnień i świadomości kontrahentów dotycząca inicjatyw zrównoważonego rozwoju, brak finalnych, przejrzystych regulacji

Przykłady tematów audytowych / obszarów do audytu:

- Weryfikacja i ocena gotowości i zgodności w zakresie wdrożenia wymogów ESG oraz oceny wpływu na biznes
- Audyt strategii ESG oraz egzekwowania deklarowanych założeń
- Przegląd dokumentacji wewnętrznej oraz klienckiej
- Weryfikacja procesów raportowania niefinansowego oraz rozszerzonych obowiązków sprawozdawczych
- Przegląd strategii produktowych

Wybrane ryzyka – kluczowe wyzwania i przykładowe obszary do audytu

Business Continuity

Przykłady zagrożeń/wyzwań:

- Ryzyko awarii zasilania (blackout'u), braku dostaw energii, a w konsekwencji zagrożenie kontynuacji działania (np. utrudniony dostęp do sieci/serwerów, ograniczone korzystanie z wszelkich urządzeń wymagających zasilania, nieogrzewane biura, brak dostęp pracowników do biur, problemy z komunikacją publiczną, komunikacją telefoniczną)
- Ryzyko przerwania łańcuchów dostaw (np. usługi chmurowe, usługi około ubezpieczeniowe, obsługa klienta, call center)

Przykłady tematów audytowych / obszarów do audytu:

- Analiza gotowości na wypadek awarii zasilania, ocena ryzyka, plan działań
- Analiza kluczowych dostawców oraz usług krytycznych (w tym np. weryfikacja zapisów umownych, planów awaryjnych po stronie dostawców, zgodności/spójności BIA (Business Impact Analysis) zakładu i testów dostawcy)
- Plany Ciągłości Działania i Plany Awaryjne z uwzględnieniem analizy wpływu zdarzeń na biznes (Business Impact Analysis), wskaźników dotyczących docelowego czasu odtworzenia procesu i zasobów (Recovery Time Objective – RTO i Recovery Point Objective – RPO)

Dziękujemy za uwagę