BO·IT·EGA
IT minds

# Program szkolenia:

# Zarządzanie ryzykiem w projektach związanych z AI dla managerów IT

## Informacje:

| | |
|---|---|
| **Nazwa:** | **Zarządzanie ryzykiem w projektach związanych z AI dla managerów IT** |
| **Kod:** | **pm-risk** |
| **Kategoria:** | Strefa PM |
| **Odbiorcy:** | liderzy techniczni, liderzy zespołów, architekci, management, analitycy, kierownicy projektów, Product Owners |
| **Czas trwania:** | 1 dzień |
| **Forma:** | 30% wykłady / 70% warsztaty |

Szkolenie zostało zaprojektowane z myślą o osobach zarządzających projektami, które chcą świadomie identyfikować, oceniać i ograniczać ryzyka związane z wdrażaniem sztucznej inteligencji.

Program rozpoczyna się od krótkiego, interaktywnego wprowadzenia, które pomaga uczestnikom zbudować wspólny język wokół pojęcia ryzyka AI oraz odnieść temat do własnych projektów i obaw. W części porannej omawiane są podstawowe podejścia do klasyfikacji ryzyk, w tym perspektywa EU AI Act oraz najczęściej wskazywane zagrożenia znane z branżowych frameworków. Uczestnicy poznają ryzyka związane m.in. z błędami modeli, uprzedzeniami algorytmicznymi, bezpieczeństwem, zgodnością prawną i reputacją organizacji.

Następnie, pracując na praktycznych scenariuszach z obszarów takich jak HR, sprzedaż, scoring czy chatboty wewnętrzne, uczą się identyfikować i porządkować ryzyka w przejrzyste kategorie. Warsztatowy charakter tej części pozwala uporządkować sposób myślenia o zagrożeniach i przełożyć teorię na realne przypadki biznesowe.

Po południu uczestnicy przechodzą do uporządkowanego procesu zarządzania ryzykiem AI, obejmującego definiowanie celu, identyfikację ryzyk, ocenę ich wagi, planowanie reakcji oraz monitorowanie. W ramach ćwiczeń zespoły tworzą własny mini rejestr ryzyk lub canvas dla rzeczywistego projektu AI, nad którym pracują lub który planują wdrożyć. Ważnym elementem szkolenia jest również moduł poświęcony monitoringowi i komunikacji, w którym uczestnicy projektują wskaźniki KPI i KRI oraz uczą się raportować ryzyka do sponsorów i zarządu. Dzięki temu szkolenie rozwija nie tylko wiedzę merytoryczną, ale także praktyczne kompetencje potrzebne do odpowiedzialnego prowadzenia projektów AI w organizacji.

Model kompetencji Dreyfus

W pięciopoziomowej skali Dreyfus: pracujemy z grupą jako novice(1)/advanced beginner(2) w ryzyku AI i kończymy na competent(3) w prostych projektach - czyli uczestnicy umieją samodzielnie zrobić podstawową analizę i zaplanować działania.

# Zalety szkolenia:

- Praktyczne podejście do realnych projektów AI – uczestnicy pracują na konkretnych scenariuszach i tworzą własny rejestr ryzyk dla rzeczywistych inicjatyw.

- Połączenie regulacji, bezpieczeństwa i biznesu – szkolenie pokazuje, jak łączyć wymagania EU AI Act, dobre praktyki zarządzania ryzykiem i potrzeby organizacji.
- Rozwój kompetencji komunikacyjnych managera IT – uczestnicy uczą się nie tylko identyfikować ryzyka, ale też skutecznie raportować je zarządowi i interesariuszom.

BOTTEGA IT minds

# Szczegółowy program:

**1. Zbudowanie wspólnego języka - każdy rozumie, „o czym mówimy”, gdy mówimy o ryzyku AI.**

1.1. Krótkie, interaktywne wprowadzenie: uczestnicy zaznaczają na tablicy swoje projekty AI(lub planowane) i największe obawy.

1.2. Mini-wykład z przykładami:

1.2.1. jak EU AI Act patrzy na ryzyko (unacceptable / high / inne systemy),

1.2.2. jakie typowe ryzyka widzą frameworki branżowe (błąd modelu, bias, bezpieczeństwo, reputacja).

**2. Przedpołudnie – case’y i kategoryzacja ryzyk**

2.1. Trzy do czterech scenariuszy (HR, sprzedaż, scoring, wewnętrzny chatbot) – w grupach:

2.1.1. identyfikacja ryzyk,

2.1.2. przypisanie do kategorii (dane, model, prawo, etyka, reputacja, security).

2.2. Prezentacje grup na plenum, doprecyzowanie kategorii i języka ryzyka (przejście wstronę „competent”).

**3. Proces zarządzania ryzykiem w AI, narzędzia i komunikacja**

3.1. Pięć kroków (zgodne z podejściami typu NIST AI RMF / dobre praktyki):

3.1.1. A. Zdefiniuj cel i interesariuszy.

3.1.2. B. Zidentyfikuj ryzyka.

3.1.3. C. Oceń (prawdopodobieństwo, wpływ, priorytety).

3.1.4. D. Zaplanuj reakcje i kontrole.

3.1.5. E. Ustal monitorowanie i odpowiedzialności.

3.2. Ćwiczenie: każdy zespół robi „mini AI Risk Register / Canvas” dla swojego realnego projektu.

**4. Monitoring i komunikacja**

4.1. Wprowadzenie: przykładowe KPI/KRI i dashboardy dla AI (np. liczba skarg, drift danych, anomalie, incydenty).

4.2. Ćwiczenie:

4.2.1. zespoły projektują 3–5 wskaźników + prosty format raportu,

4.2.2. role-play: 10-minutowe spotkanie statusowe z „zarządem / sponsorem” – przedstawienie ryzyk i planu.