

02

MODUŁ 02 / TECHNOLOGIA / 13.10.2026

AI Governance_

Moduł 2: prosto o technologii
Narzędzia, koszty i plan działania





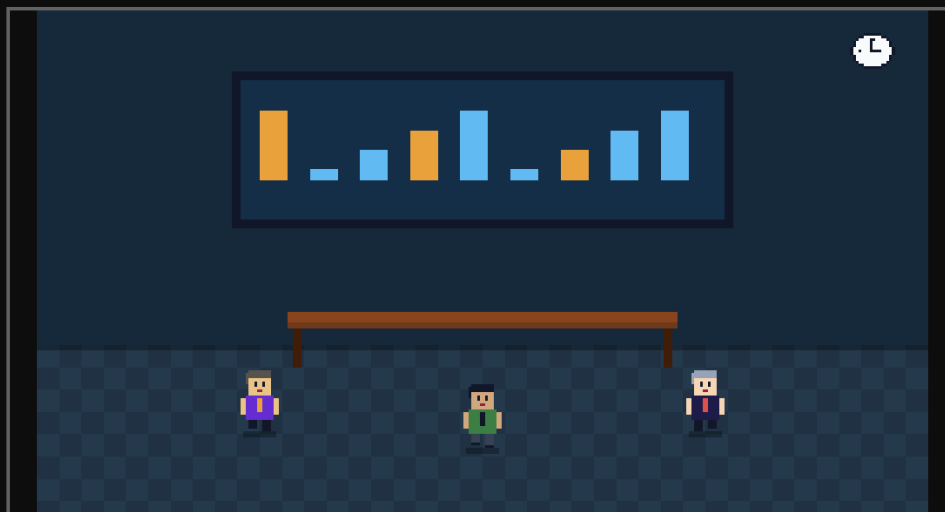
CZŁONEK ZARZĄDU - ALARM I DOWODZENIE

Alarm bez pełnego obrazu

Tryb tekstowy: wyłączony

Materiały (0)

Menu



Dzień 1, 03:00 - Alarm bez pełnego obrazu Postaci: Członek zarządu, Dyrektor IT, Prezes

Dyrektor IT

Dyrektor IT potwierdza blokadę systemu zleceń. Nie wiadomo jeszcze, czy zaatakowano pozostałe usługi. Masz wewnętrzne upoważnienie do zwołania sztabu i tymczasowych priorytetów, nie do zastąpienia uchwał zarządu.

Pomoc przed wyborem: sprawdź fakty, zakres upoważnień, korzyść, koszt i warunki. Materiały są fikcyjne, nie stanowią wymaganej prawem uniwersalnej listy.

Dalej

1 / 1

WSKAŹNIKI

Zgodność 50 / 100



Odporność 50 / 100



Zaufanie 50 / 100



ZEGAR PRAWNY - WARUNKOWY

Czas scenariusza od wykrycia: 0
godz. 0 min

UKSC: jeśli ma zastosowanie i incydent podlega zgłoszeniu do właściwego CSIRT sektorowego. Od wykrycia takiego incydentu.

Wczesne ostrzeżenie: niezwłocznie, do 24 godz.

Zgłoszenie incydentu: niezwłocznie, do 72 godz.

► Warunki i źródła

DZIENNIK INCYDENTU

Brak wpisów. Wpis pojawi się po pierwszej decyzji.

Polityka zarządzania relacjami z podmiotami trzecimi w obszarze AI

5. Segmentacja relacji (tiering)

5.1. Każdą relację objętą polityką klasyfikuje się do jednego z trzech tierów. Tier determinuje głębokość due diligence, wymagany katalog klauzul i częstotliwość przeglądów.

Tier	Kryteria (co najmniej jedno)	Konsekwencje
KRYTYCZNY	System wysokiego ryzyka wg AI Act (załącznik III); przetwarzanie danych poufnych lub szczególnych kategorii; wsparcie procesu krytycznego dla działalności; głęboka integracja z systemami organizacji; trudna zastępowalność; podleganie DORA - kluczowe usługi ICT	Pełne due diligence (sekcja 7) przed umową; pełny katalog klauzul (sekcja 8); przegląd co 12 mies. + plan wyjścia przetestowany; zatwierdzenie: zarzqd / Komitet AI .
ISTOTNY	Dane wewnętrzne lub osobowe zwykłych kategorii; zauważalny wpływ na klientów lub pracowników; średnia zastępowalność	Due diligence standardowe; klauzule podstawowe + adekwatne do ryzyk; przegląd co 24 mies.; zatwierdzenie: AIGO + właściciel biznesowy .
STANDARDOWY	Dane publiczne; narzędzia pomocnicze bez integracji; łatwa zastępowalność	Due diligence uproszczone (checklista - Załącznik A w wersji skróconej); klauzule minimalne; przegląd przy odnowieniu; zatwierdzenie: właściciel biznesowy, wpis do rejestru .

5.2. Tier nadaje AIGO na wniosek właściciela relacji przy pierwszej ocenie i weryfikuje przy każdym przeglądzie oraz przy istotnej zmianie zakresu usługi. W razie wątpliwości stosuje się tier wyższy.

7.2. Krok pierwszy: profil relacji

Przed zadaniem pytań dostawcy ustalamy profil, który wyznacza zakres badania:

- rola organizacji i dostawcy w łańcuchu wartości wg AI Act (dostawca / podmiot stosujący / importer / dystrybutor) oraz ryzyko wejścia w rolę dostawcy z art. 25;
- obszar zastosowania i czy mieści się w załączniku III AI Act (wysokie ryzyko) albo ociera o praktyki zakazane z art. 5;
- czy przetwarzane będą dane osobowe (i jakich kategorii) oraz jakie klasy informacji wg SZBI;
- czy organizacja podlega reżimom sektorowym DORA / NIS2 / inne - włączając one dodatkowe pytania i klauzule;
- wstępny tier relacji (sekcja 5).

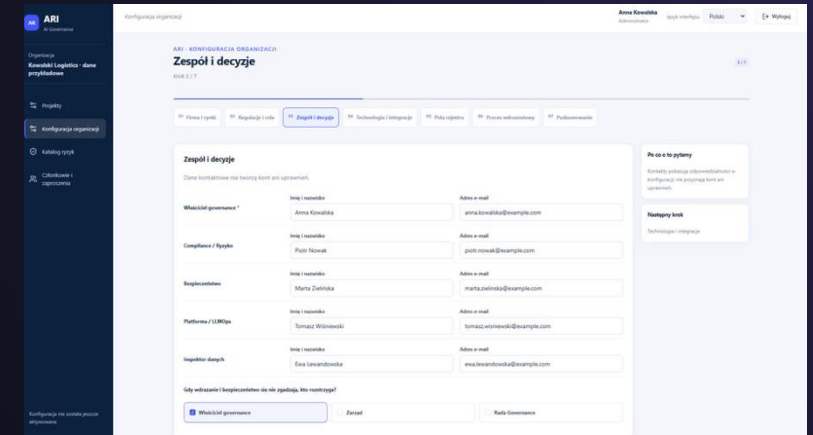
7.3. Krok drugi: ocena możliwości dostawcy

Badamy udokumentowane zdolności dostawcy w sześciu obszarach (katalog pytań - Załącznik A):

- transparentność i dokumentacja: karta modelu/systemu, dokumentacja techniczna (art. 11 i załącznik IV AI Act), instrukcja użytkowania i informacje dla podmiotu stosującego (art. 13);
- jakość i pochodzenie danych: zarządzanie danymi treningowymi, reprezentatywność, testy biasu (art. 10), gotowość do zawarcia DPA i wskazania lokalizacji przetwarzania (art. 28 RODO);
- nadzór ludzki i wyjaśnialność: mechanizmy nadzoru (art. 14), rejestrowanie zdarzeń umożliwiające audyt (art. 12);
- bezpieczeństwo i odporność: testy typu red teaming/TEVV (art. 15), zarządzanie podatnościami i aktualizacjami;
- przejrzystość treści syntetycznych: oznaczanie treści generowanych (art. 50) - dla rozwiązań GenAI;
- dojrzałość ładu i incydenty: wdrożone ramy (ISO/IEC 42001, NIST AI RMF), proces zgłaszania poważnych incydentów i współpracy (art. 73).

Cztery pytania o AI w firmie_

AI Governance: jasne zasady korzystania z AI i odpowiedzialność za jej działanie.



Co mamy?

Wiemy, gdzie pracownicy i klienci korzystają z AI.

Czy działa dobrze?

Sprawdzamy odpowiedzi i błędy na przykładach z naszej firmy.

Kto odpowiada?

Każde zastosowanie ma osobę, która podejmuje decyzje.

Ile to kosztuje?

Liczymy programy, uruchomienie i czas ludzi.

Przykład: AI pomaga obsługiwać reklamacje_

Firma Kowalskiego chce szybciej przygotowywać odpowiedzi klientom.

Zadanie AI

Czyta zgłoszenie i proponuje odpowiedź.

Zadanie człowieka

Sprawdza treść i zatwierdza zwrot pieniędzy.

Granica

AI nie wysyła wiadomości ani pieniędzy bez wymaganej zgody.

Early risk assessment

Human-in-the-loop

MLOps

Security

Na tym przykładzie pokażemy listę zastosowań, testy, historię działania i zgodę człowieka.

Pierwsze narzędzie: zwykła lista zastosowań_

Listę zastosowań przygotowujemy z IT i osobą odpowiedzialną za bezpieczeństwo.

Do czego używamy AI?	Kto odpowiada?	Jakie dane?	Czy można używać?
Szkice reklamacji	Kierownik obsługi	Zatwierdzone dane spraw	Tylko w próbie
Odpowiedzi z bazy wiedzy	Właściciel wiedzy	Dokumenty z dostępem	Po sprawdzeniu
Redagowanie tekstów	Kierownik zespołu	Treści bez tajemnic firmy	W ustalonym zakresie

Rejestr zasobów

Zapytaj IT/Sec

ARI

AI Governance Platform

1

AI Rejestr i Klasyfikacja

MODULE 1

3

Zgodność i dowody

MODULE 3

4

Roadmapa i korzyści

MODULE 4

5

Katalog ryzyk

MODULE 5

14

Portal pracownika

MODULE 14

16

Konsultacje eksperckie

MODULE 16

🔧

Konfiguracja organizacji

▼

👤

Członkowie i zaproszenia

Aktywna konfiguracja - wersja 8

👤

Konto i nawigacja

MODUŁ 1 · AI DISCOVERY AND REGISTRY

Rejestr systemów AI

Jedno źródło prawdy o systemach i agentach AI w SYNTHETIC ARI DEV.

KONFIGURACJA · FULL · 25 PÓŁ

Rola: wdrażający · UE, USA · RODO, NIST AI RMF, ISO/IEC 42001, NIST CSF 2.0, EU AI Act

Zmień pola

SYSTEMY W REJESTRZE

8

Cała organizacja · wczytane rekordy

WYSOKIE RYZYKO · CAŁA ORGANIZACJA

1

Tylko ręcznie zapisane wartości

BEZ PRZYPISANEGO WŁAŚCICIELA

0

Ręcznie zapisane dane · cała organizacja

PRZEGLĄD PO TERMINIE

0

Ręcznie zapisane dane · cała organizacja

🔍

Szukaj po nazwie, właścicielu, dostawcy, modelu lub opisie...

/

🔍

Wyszukiwanie zaawansowane

▼

Wszystkie 8

Wysokie ryzyko 1

Do potwierdzenia 4

Produkcja 0

8 / 8

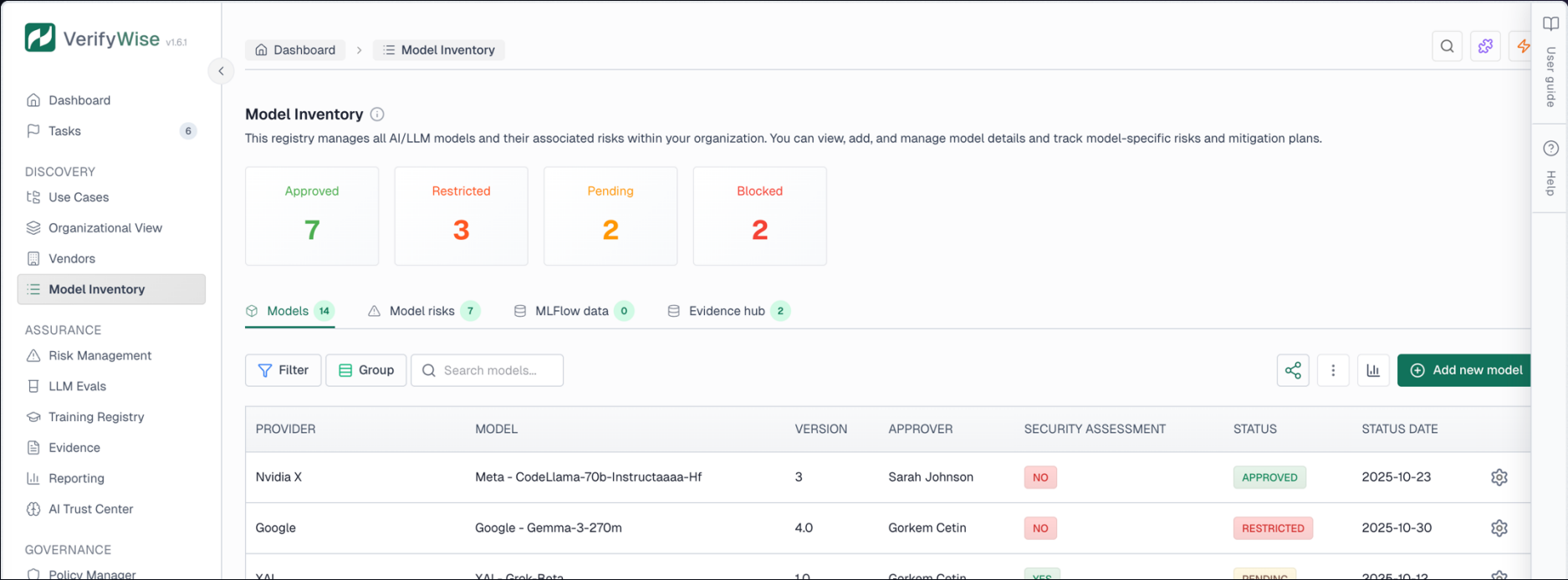
🔄

CSV

SYSTEM	ETAP PROCESU	WŁAŚCICIEL	RYZYKO WG AI ACT	AUTONOMIA	WDROŻENIE I MODEL	ŚRODOWISKO	UŻYTK.	PRZEGLĄD
DEMO — Weryfikacja jakości dokumentów DEMO: fikcyjny system wykrywa braki w syntetycznych dokumentach i wskazuje fragmenty do kontroli. Wysokie ryzyko jest wyłącznie wartością demonstracyjną do testu oznaczeń, nie oceną prawną. System nie decyduje o osobach ani nie łączy się z produkcją.	Nieznane	Karol Janulewicz	Wysokie Potwierdzony jako system AI	A2 — rekomendacje do kontroli	Analiza dokumentów Model dokumentowy DEMO	Pilotaż	8	Nieznane
DEMO — Klasyfikacja zgłoszeń serwisowych DEMO: klasyfikacja fikcyjnych zgłoszeń IT i podpowiedź kolejki obsługi. Wyłącznie syntetyczne dane. Klasyfikacje ryzyka i metryki są przykładowe; decyzję o przekazaniu zgłoszenia podejmuje człowiek.	Nieznane	Karol Janulewicz	Minimalne Potwierdzony jako system AI	A1 — rekomendacja	Klasyfikator ML Model klasyfikacyjny DEMO	Test	12	Nieznane
DEMO — Asystent procedur wewnętrznych DEMO: fikcyjny asystent odpowiada na pytania o syntetyczne procedury. Odpowiedzi zawierają źródła i wymagają kontroli człowieka. Dane demonstracyjne, bez klientów, informacji osobowych i produkcyjnych połączeń.	Nieznane	Karol Janulewicz	Ograniczone Potwierdzony jako system AI	A1 — wsparcie człowieka	Asystent RAG Model demonstracyjny / dostawca przykładowy	Pilotaż	24	Nieznane
xyz jakis tam cel	Nieznane	Karol Janulewicz	Nieznane Potwierdzony jako system AI	Nieznane	Nieznane Nieznane	Nieznane	—	Nieznane
SAMPLE — Asystent wiedzy wewnętrznej Fikcyjny projekt demonstracyjny. Asystent odpowiada na pytania na podstawie syntetycznych dokumentów szkoleniowych. Nie zawiera danych klientów ani danych	Nieznane	Karol Janulewicz	Nieznane Niepotwierdzony	Nieznane	Nieznane Nieznane	Nieznane	—	Nieznane

VerifyWise: porządek w używaniu AI

Przykład platformy zbierającej informacje o AI, ryzykach i zadaniach.



Na ekranie: lista modeli, osoba zatwierdzająca i status.

Dodatkowy przykład: kod dostępny na BSL 1.1. To nie jest licencja open source.

Zrzut demonstracyjny z oficjalnego repozytorium. Status na liście sam nie blokuje użycia.

Przed uruchomieniem: kilka zwykłych prób_

Sprawdzamy również to, czego AI nie powinno zrobić.

Przykład do sprawdzenia	Oczekiwany wynik
Klient pyta o zasady zwrotu	Odpowiedź zgodna z regulaminem
Brakuje informacji o zakupie	AI prosi o dane lub przekazuje sprawę człowiekowi
Klient żąda danych innego klienta	AI nie ujawnia danych
W zgłoszeniu jest „pomiń zasady”	AI nie wykonuje niedozwolonej czynności

promptfoo: sprawdzanie odpowiedzi_

Pomaga porównać, która wersja AI lepiej radzi sobie z tymi samymi pytaniami.

Variables		Outputs	
name	question	openai:gpt-5.240.00% passing (2/5 cases) examples/self-grading/prompts.txt: You're an ecommerce chat assistant for a shoe company. Answer this user's question: {{name}}: "{{question}}" Requests: 5 Asserts: 14/20 passed Total Cost: \$0.0106 Total Tokens: 916 Avg Tokens: 183 Avg Latency: 3,550 ms Tokens/Sec: 42	openai:gpt-5.280.00% passing (4/5 cases) examples/self-grading/prompts.txt: You're a smart, bubbly customer service rep for a shoe company. Answer this user's question concisely: {{name}}: "{{question}}" Requests: 5 Asserts: 18/20 passed Total Cost: \$0.0068 Total Tokens: 666 Avg Tokens: 133 Avg Latency: 2,371 ms Tokens/Sec: 39
Bob	Can you help me find a specific product on your website?	4 PASS (0.90) Yes—I'd be happy to help. What product are you looking for? If you can share any of these details, I can pinpoint it fast: - Brand or model name (if you know it) - Men's/Women's/Kids - Size and width (e.g., 10, 10W, 42) - Color	4 PASS (0.98) Absolutely, Bob! Tell me the product name (or a few details like style, size, color, and whether it's men's/women's), and I'll help you track it down on our website with the right link.

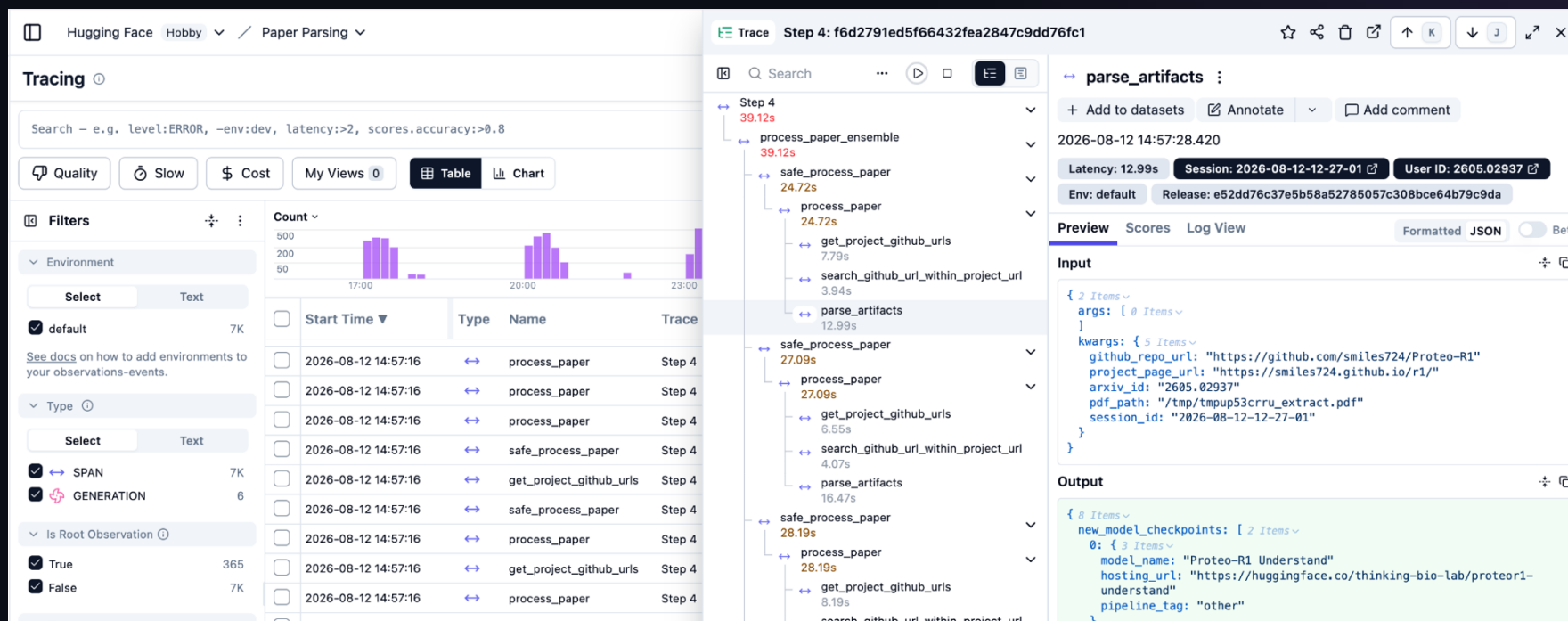
Na ekranie: odpowiedzi dwóch wersji i wyniki testów.

Open source, MIT. Bez opłaty licencyjnej. Uruchomienie i użycie modeli kosztują.

Zrzut z dokumentacji. To testy odpowiedzi. Blokowanie niedozwolonych działań wymaga osobnych zabezpieczeń.

Langfuse: historia działania AI

Po uruchomieniu zapisujemy przebieg spraw, aby móc wyjaśniać błędy.



Na ekranie: lista działań, kolejne kroki oraz dane wejściowe i wynik.

Główna część open source, MIT. Część funkcji Enterprise ma osobne warunki.

Zrzut z dokumentacji. Historia pojawi się dopiero po połączeniu narzędzia z aplikacją.

MLflow: zapis wersji i wyników_

Gdy rozwijamy własny model, potrzebujemy też zapisu jego wersji i wyników testów.

> Description [Edit](#)

> Tags

▼ Versions [Compare](#)

New model registry UI ☒

Version	Registered at ↕	Created by	Tags	Aliases	Description
✓ Version 8	2023-09-25 12:38:44		validation_status: pending ✎	@ challenger ✎	Uses decision tree
✓ Version 7	2023-09-25 12:38:41		validation_status: approved ✎	@ champion ✎	Uses a CNN based approach
✓ Version 6	2023-09-25 12:38:38		validation_status: approved ✎	Add	
✓ Version 5	2023-09-25 12:38:35		Add	Add	
✓ Version 4	2023-09-25 12:38:32		Add	Add	

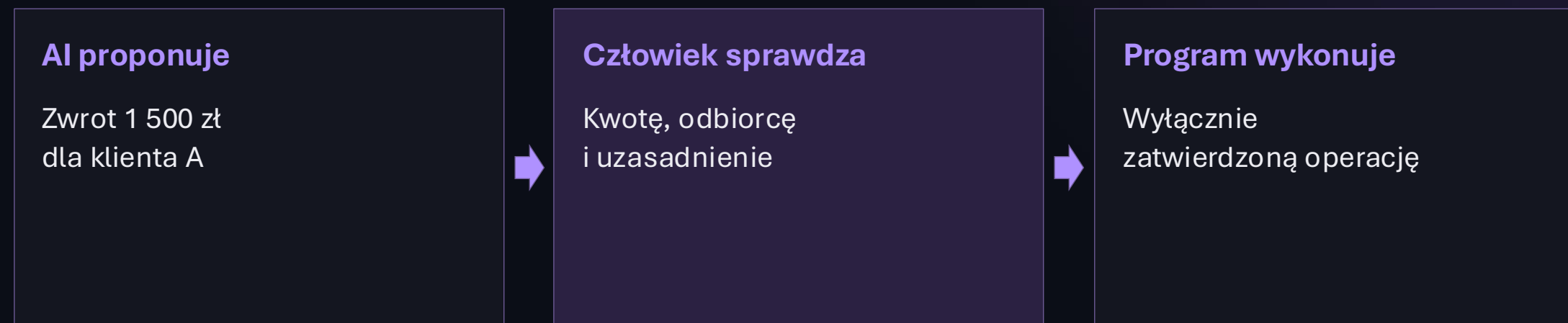
Na ekranie: kolejne wersje modelu i oznaczenia ich oceny.

Open source, Apache 2.0. Przydatne głównie przy własnych modelach i aplikacjach.

Zrzut z dokumentacji, starszy interfejs. Firma korzystająca tylko z gotowej usługi zwykle go nie potrzebuje.

Agent AI: propozycja, zgoda, wykonanie_

Agent AI może działać w innych programach. W naszym przykładzie wykonuje zwrot pieniędzy.



Zgoda dotyczy konkretnej operacji. Zmiana kwoty lub odbiorcy wymaga ponownej zgody.

Instrukcja etycznego projektowania systemów agentów AI

Wzorcowy szablon oparty na HLEG UE, IEEE 7000 i 7001, OECD, UNESCO, ISO/IEC TR 24368, NIST AI RMF oraz ramach zarządzania agentlic AI, zbieżny z AI Act

Pełna treść Podgląd dla kupujących

- Jak korzystać z szablonu
1. Cel i zakres

2. Definicje

3. Standardy odniesienia

4. Zasady etycznego projektowania agentów

5. Poziomy autonomii i nadzór człowieka

6. Proces etycznego projektowania (EI-E5)

7. Katalog wymagań projektowych (DE-01..DE-24)

Granice działania i nadzór

Tożsamość i przejrzystość

Pamięć i dane

Odporność i kontrola

Sprawdliwość i interakcja z

Tryb edycji (admin)

Historia zmian

Pobierz PDF

Drukuj

Wyczyść pola

Uzupełniono 0 pól - zapis wyłącznie w tej przeglądarce (localStorage), nic nie wysyłamy na serwer

Organizacja

Właściciel dokumentu

Zatwierdził

Wersja

Data wejścia w życie

Data kolejnego przeglądu

Klasyfikacja poufności

wpisz pełną nazwę i NIP/identyfikator

rola / imię i nazwisko - np. Koordynator AI / CTO

organ / osoba zatwierdzająca

7. Katalog wymagań projektowych (DE-01..DE-24)

7.1. Wymagania obowiązują proporcjonalnie do poziomu autonomii i klasyfikacji systemu; kolumna „Poziom” wskazuje minimum. Checklista weryfikacyjna - Załącznik A.

Granice działania i nadzór

ID	Wymaganie	Poziom
DE-01	Przestrzeń działań agenta jest zamknięta: agent może wywoływać wyłącznie narzędzia z jawnie zdefiniowanej listy (allowlista); każde narzędzie ma opisany cel, zakres i skutki.	A1+
DE-02	Uprawnienia agenta są minimalne dla zadania (least privilege) i odrębne od uprawnień ludzi; agent nie dziedziczy pełnych uprawnień użytkownika, w którego imieniu działa, lecz otrzymuje podzbiór wymagany do zadania.	A1+
DE-03	Granice twarde (zakazy) są egzekwowane poza modelem - w kodzie, uprawnieniach lub infrastrukturze; instrukcja w prompcie nie jest mechanizmem kontroli, tylko wsparciem.	A1+
DE-04	Agent ma budżety i limity: maksymalną liczbę akcji na zadanie, limity kosztów, czasu i częstotliwości; przekroczenie zatrzymuje agenta i eskaluje do człowieka.	A2+
DE-05	Katalog działań konsekwentnych jest zdefiniowany dla każdego agenta; obejmuje co najmniej: płatności i zobowiązania, komunikację zewnętrzną, zmiany uprawnień, usuwanie lub eksport danych, decyzje wobec osób uzupełnij . Działania konsekwentne wymagają zgody człowieka (HITL) do poziomu A3 włącznie.	A1+
DE-06	Mechanizm zgody jest zaprojektowany przeciw „zmęczeniu zatwierdzaniem”: opis działania i skutków jest zrozumiały, zgody nie są sztucznie rozdrabniane ani zbijane w nieczytelne paczki; odsetek odrzuceń jest monitorowany (stałe bliski zera sugeruje zgody mechaniczne).	A2+



Gdy coś pójdzie źle_

Jeśli AI popełni błąd, pracownik musi wiedzieć, gdzie go zgłosić i kto zatrzyma działanie.

Pracownik zgłasza

Podaje sprawę i opisuje problem.

IT ogranicza działanie

Wstrzymuje kolejne czynności i sprawdza historię.

Właściciel decyduje

Czy poprawić, ograniczyć użycie czy wyłączyć rozwiązanie.

Próbę zatrzymania warto wykonać jeszcze przed uruchomieniem.

Którego narzędzia potrzebuję?_

Wybór zaczyna się od problemu, który chcemy rozwiązać.

Potrzeba firmy	Możliwy początek
Nie wiemy, gdzie używamy AI	Arkusz lub lista zastosowań
Nie wiemy, czy odpowiedzi są dobre	Przykładowe pytania, potem np. promptfoo
Nie potrafimy wyjaśnić błędu	Historia w usłudze lub np. Langfuse
Gubimy wersje własnego modelu	Np. MLflow dla zespołu technicznego

Gdy AI pomaga pisać program

Osobny przypadek: firma buduje własne rozwiązanie lub zleca jego wykonanie.

„Vibe coding”

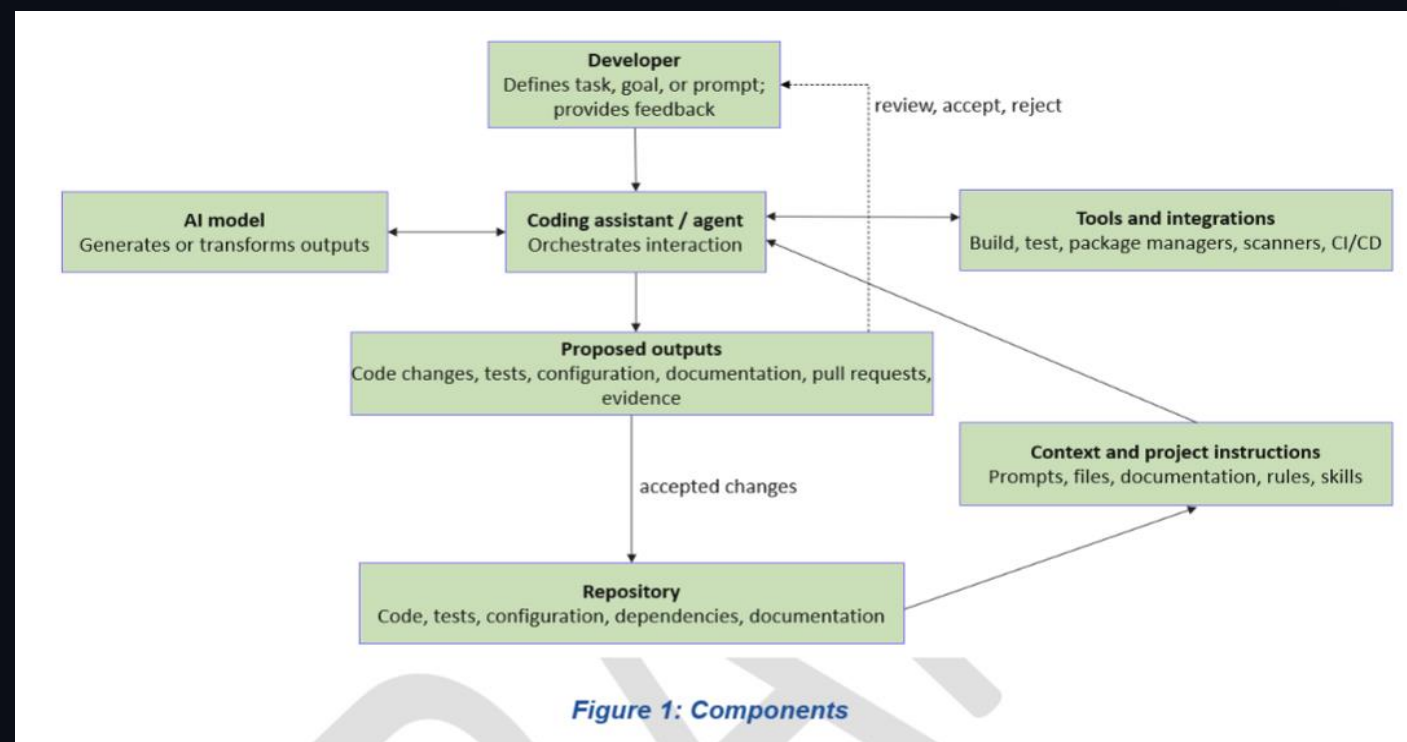
Opisujemy AI, jaki program ma powstać.
AI proponuje kod i poprawki.

Działający prototyp wymaga jeszcze
sprawdzenia i bezpiecznego
połączenia z systemami firmy.



AI pomaga pisać kod. Kto go sprawdza?

ENISA, unijna agencja ds. cyberbezpieczeństwa, opisuje rolę człowieka i kontroli zmian.



Zasady pracy z kodem tworzonym przez AI

Polskie objaśnienie schematu ENISA. Projekt v0.4, wrzesień 2026.

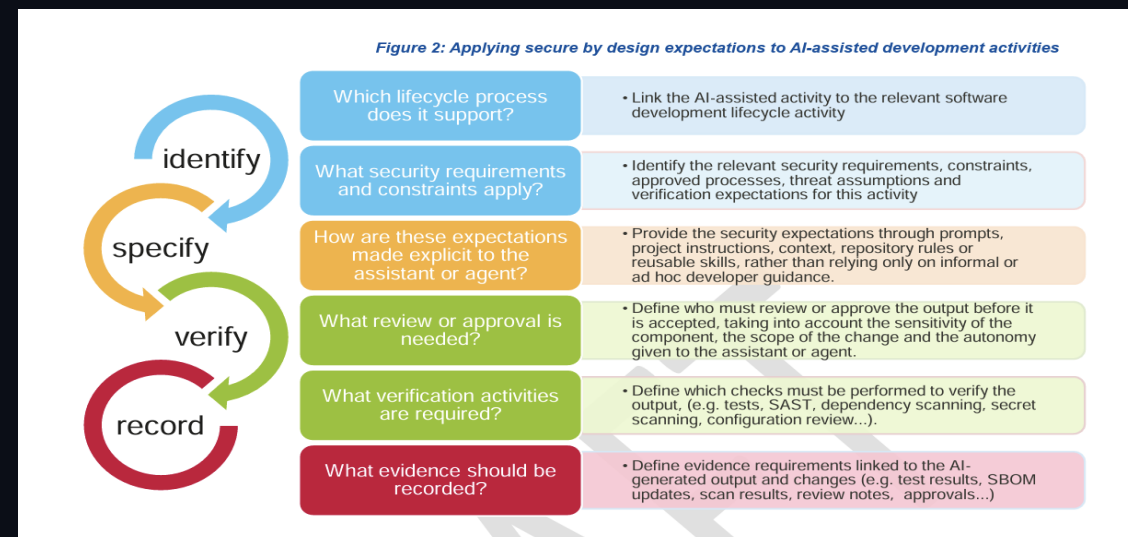


Table 4: Governance and assurance risks

Governance / assurance risk	Example in AI-assisted software development
Unclear accountability	It is unclear who is responsible for AI-generated outputs, especially where an agent performs multi-step tasks across several files or tools.
Uncontrolled autonomy	Assistants or agents are allowed to modify code, install dependencies, run commands, change configuration or prepare pull requests without clear limits or approval points.
Inconsistent security instructions	Security expectations are applied inconsistently because prompts, project instructions, rules or skills are missing, outdated, conflicting or not treated as authoritative.
Weak traceability	It is difficult to link AI-assisted changes to requirements, design decisions, security requirements, review outcomes, tests or evidence.
Insufficient review capacity	Developers or reviewers cannot effectively assess the volume, complexity or scope of AI-generated changes.
Unsupported security claims	AI-generated statements such as "this is secure", "the issue is fixed" or "all checks passed" are accepted without supporting evidence.

Zakres

Co AI może zmieniać?

Instrukcje

Jakie zasady ma stosować?

Sprawdzenie

Kto oceni kod i wyniki testów?

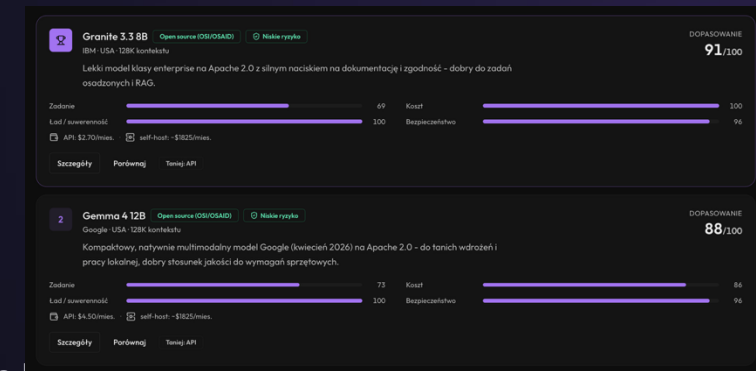
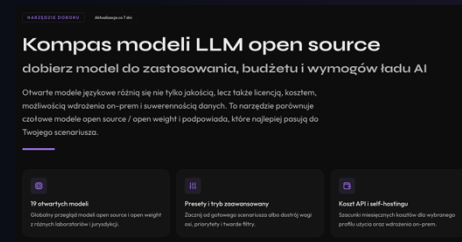
Zapis

Gdzie zachowamy wyniki i zgodę?

ENISA, projekt v0.4. Schematy: CC BY 4.0.

Open source też ma koszty_

Wracamy do budżetu narzędzi. Open source pozwala używać i zmieniać kod na warunkach licencji.



Uruchomienie

Instalacja, połączenie z aplikacją i ustawienie dostępu.

Utrzymanie

Serwer, aktualizacje, kopie i usuwanie usterek.

Codzienna obsługa

Przygotowanie testów, ocena błędów i podejmowanie decyzji.

Samo użycie AI

Opłaty za model lub zasoby potrzebne do jego działania.

Mały pilotaż: przykład budżetu 9 000 zł

Próba asystenta do szkiców odpowiedzi, bez samodzielnych działań.

Praca lub wydatek	Przyjęte założenie	Koszt
Spis zastosowań i proste zasady	2 dni × 1 000 zł	2 000 zł
Ustawienia i podłączenie narzędzi	3 dni × 1 300 zł	3 900 zł
Przygotowanie i wykonanie prób	2 dni × 1 300 zł	2 600 zł
Dodatkowy serwer na próbę	Założony limit	500 zł

Ilustracja sposobu liczenia, nie wycena. Bez licencji usługi AI, użycia modelu i dalszego utrzymania.

Dwa różne budżety_

Mały pilotaż to jeden zakres prac. Własny produkt dla klientów to znacznie szerszy zakres.

Korzystam z AI

Kupuję gotową usługę do pracy mojej firmy.

Płacę za dostęp, zasady, ustawienia i nadzór.

Dostarczam system AI

Oferuję własny system klientom pod swoją nazwą.

Budżet obejmuje także przygotowanie produktu do wymagań jego rynku.

Arkusz kosztów dotyczy drugiej sytuacji: dostawcy systemu wysokiego ryzyka.

Budżet dostawcy: przykładowe prace

Zrzuty pokazują zakres prac technicznych. Kwoty i założenia wyjaśniają kolejne slajdy.

T-37	Techniczny	art. 12, 19	Rejestrowanie i przechowywanie zdarzeń	Logi adekwatne do przeznaczenia, kontrola dostępu, retencja i eksport. Konkretna technologia oraz niezmiennosc są wyborem projektu, nie uniwersalnym wymogiem ustawowym.
T-38	Techniczny	art. 11, 17	Rejestr modeli, wersjonowanie, odtwarzalność	MLflow + DVC, podpisy artefaktów, lineage danych do modelu, generowanie kart modelu z metadanych
T-39	Techniczny	art. 10	Katalog danych i walidacja jakości	Katalog z pochodzeniem (OpenMetadata lub lżejszy), walidacja w pipeline (Great Expectations), wykrywanie i pseudonimizacja danych osobowych (Presidio)
T-40	Techniczny	art. 15, 9	Framework ewaluacji, fairness i red-team w CI	Automatyzacja ewaluacji, testów stronniczości i odporności właściwych dla modelu. Narzędzia LLM tylko wtedy, gdy architektura ich wymaga. Wykonywanie i analiza testów w O-26.
T-41	Techniczny	art. 72, 15	Monitoring produkcyjny i dryf	Metryki jakości, dryfu i alerty. Dostęp do informacji od klientów na właściwej podstawie prawnej i kontraktowej. Analiza wyników w O-29.
T-42	Techniczny	art. 14	Konsola nadzoru i wyjaśnialność	Interfejs nadzoru (kolejka, pewność, wyjaśnienia SHAP/cytowania, override, stop), zdarzenia nadzoru w logach
T-43	Techniczny	art. 15	Techniczne zabezpieczenia modelu i danych	Kontrola dostępu do danych i modelu, izolacja, ochrona sekretów i skanowanie. Rozszerzenie istniejących mechanizmów ISO 27001. W bazie brak generatywnego LLM.
T-44	Techniczny	art. 17	CI/CD z kontrolą zmian i kontrolowane wdrażanie	Bramki w pipeline, canary/shadow, rollback, podpisany release, dziennik zmian zasilający dokumentację



T-45	Techniczny	art. 18	Archiwum dokumentacji i dowodów (10 lat)	Repozytorium dokumentacji technicznej z wersjonowaniem, dziennik dowodów, eksport pakietu dla organu
T-46	Techniczny	art. 73	Narzędzia obsługi incydentów i komunikacji z klientami	Kanał zgłoszeń, klasyfikacja, zegary terminów, portal informacji dla podmiotów stosujących
T-47	Techniczny	-	Infrastruktura wspólna i środowiska	Dodatkowa moc do testów zgodności i izolowanego środowiska walidacji. Bez produkcyjnego hostingu, tokenów i usług już ujętych w T-37-T46.

Co dokładnie wyceniono w arkuszu?_

Jeden istniejący system wysokiego ryzyka, który firma dostarcza klientom.

Firma	Firma programistyczna, 80-150 osób, z podstawami bezpieczeństwa.
Przykład produktu	System do wstępnej selekcji kandydatów do pracy.
Zakres kosztu	Przygotowanie do wymagań i utrzymanie zgodności.
Poza budżetem	Budowa samego produktu i opłaty za użycie modeli.

Szacunek ekspercki z załączonego arkusza. Zakres trzeba dopasować do konkretnego systemu.

Dostawca systemu wysokiego ryzyka: koszty_

Trzy warianty z arkusza. Kwoty zaokrąglone do tysięcy złotych.

Wariant w arkuszu	Rok 1	Kolejne lata / rok
Minimum: firma ma już wiele rozwiązań	784 tys. zł	432 tys. zł
Realistyczny: wariant bazowy	1 121 tys. zł	617 tys. zł
Konserwatywny: więcej pracy	1 681 tys. zł	926 tys. zł

„Rok 1” w arkuszu: przygotowanie do wejścia na rynek i pierwsze 12 miesięcy. Opcje poza sumą.

Największym kosztem jest praca ludzi_

Wariant bazowy dostawcy systemu wysokiego ryzyka, rok 1.

94%

kosztu to praca własnego zespołu
i zewnętrznych specjalistów

752 tys. zł

Własny zespół

302,5 tys. zł

Zewnętrzni specjaliści

66 tys. zł

Licencje, opłaty, usługi
i infrastruktura

Kwoty z arkusza uwzględniają wartość czasu ludzi. Nie są wyłącznie nowymi fakturami.

Przykładowe koszty prac przy narzędziach_

Wariant bazowy dostawcy systemu wysokiego ryzyka. To koszt zadania, nie cena programu.

Zadanie i przykładowe narzędzia	Rok 1	Kolejne lata / rok
Historia działania, np. Langfuse i zapis logów	20 500 zł	16 100 zł
Wersje modeli, np. MLflow z dodatkami	16 600 zł	10 000 zł
Testy jakości i nadużyć, m.in. promptfoo	25 400 zł	11 200 zł

Wybrane pozycje T-37, T-38 i T-40 z arkusza. Już wchodzi do sum na poprzednich slajdach.

Jak czytać ten kosztorys?_

Cztery zasady, które chronią przed błędnym budżetem.

Praca też kosztuje	Czas własnego zespołu ma wartość, nawet bez nowej faktury.
Sum nie dodajemy drugi raz	206,4 tys. zł części technicznej już mieści się w 1,12 mln zł.
Opcje liczymy osobno	Opcjonalna certyfikacja i dodatkowa ocena są poza sumą.
Zakres jest różny	Mały pilotaż i dostawca produktu to inne zadania.

Cztery pytania przed zakupem narzędzia_

Po przykładzie dużego budżetu wracamy do wyboru narzędzia dla naszej firmy.

Połączenie

Czy działa z programami, których już używamy?

Praca ludzi

Kto je uruchomi i ile czasu zajmie późniejsza obsługa?

Dane

Co zapisuje, kto to zobaczy i jak usuniemy dane?

Wyjście

Czy pobierzemy nasze informacje, gdy zmienimy narzędzie?

Plan na 90 dni_

Najpierw jeden przykład z firmy. Rozszerzenie po ocenie wyników.

Dni 1-30

Lista zastosowań
i osoby odpowiedzialne.

Wybór jednej próby
i limit wydatków.

Dni 31-60

Ustawienie dostępu
i testy na przykładach.

Próba na małej grupie
po sprawdzeniu zabezpieczeń.

Dni 61-90

Ocena błędów, czasu
i kosztów.

Decyzja: rozwijamy,
poprawiamy lub kończymy.

Co zrobić w poniedziałek?_

Cztery ustalenia na pierwszą rozmowę z zespołem.

Jedno zastosowanie	Do jakiego konkretnego zadania użyjemy AI?
Jedna osoba	Kto odpowiada za wynik i może wstrzymać użycie?
Jedna lista prób	Jak sprawdzimy, czy AI pomaga i nie przekracza granic?
Jeden budżet	Ile czasu i pieniędzy przeznaczamy na próbę?

Pytania_

Narzędzia, koszty i przykłady z Państwa firm



AI I PRAWO

legalarchitect.pl

CYBERBEZPIECZEŃSTWO

cyberszlif.pl

KONTAKT

michal@nowakowski.ai · <https://www.linkedin.com/in/mjnowakowski/>

Dodatkowo: część techniczna kosztorysu_

Wariant bazowy. Grupy poniżej sumują się do całej części technicznej.

Grupa prac z arkusza	Rok 1	Kolejne lata / rok
Historia, wersje i dane / T-37 do T-39	57 300 zł	40 800 zł
Testy i monitoring / T-40 do T-41	42 000 zł	24 700 zł
Nadzór i bezpieczeństwo / T-42 do T-43	56 300 zł	21 600 zł
Zmiany, dokumenty, zgłoszenia i serwery / T-44 do T-47	50 800 zł	58 100 zł

Razem: 206 400 zł w roku 1 i 145 200 zł rocznie w kolejnych latach.

Dodatkowo: proste znaczenie pojęć_

Nazwy spotykane w narzędziach i rozmowach z IT.

Model	Element AI, który tworzy odpowiedź lub przewiduje wynik.
Agent	AI, które może wykonywać czynności w innych programach.
Test	Próba z ustaleniem, jakiego wyniku oczekujemy.
Historia działania	Zapis zdarzeń pozwalający odtworzyć konkretną sprawę.

Dodatkowo: inny wariant kosztorysu

Zrzut pokazuje osobny wariant: 1 106 300 zł. Główne slajdy opierają się na kwocie 1 120 500 zł.

Ile kosztuje zgodność jednego systemu wysokiego ryzyka - dostawca							
PLN. Budżet bazowy AI Act bez RODO i opcji. Rok 1 = wdrożenie + 12 miesięcy przy ustawieniu domyślnym. Mnożniki są testem wrażliwości, nie cenami rynkowymi.							
Obszar	Rok 1 – 0,7x	Rok 1 – bazowy	Rok 1 – 1,5x	Rok 2+ – 0,7x	Rok 2+ – bazowy	Rok 2+ – 1,5x	Udział roku 1
Normatywny	271 320 zł	387 600 zł	581 400 zł	87 220 zł	124 600 zł	186 900 zł	35
Operacyjny	294 700 zł	421 000 zł	631 500 zł	200 830 zł	286 900 zł	430 350 zł	38
Techniczny	208 390 zł	297 700 zł	446 550 zł	79 590 zł	113 700 zł	170 550 zł	27
RAZEM	774 410 zł	1 106 300 zł	1 659 450 zł	367 640 zł	525 200 zł	787 800 zł	100
Dodatki i koszty powiązane — poza bazą							
Certyfikacja ISO/IEC 42001	48 300 zł	69 000 zł	103 500 zł	19 320 zł	27 600 zł	41 400 zł	
Dodatkowy przegląd zewnętrzny (opcja)	22 400 zł	32 000 zł	48 000 zł	0 zł	0 zł	0 zł	
Rodzaje nakładu — rok 1, bazowy							
Rodzaj nakładu	Ilość	Koszt (zł)	Udział				
Inżynierowie / ML (osobodni)	341	443 300 zł	40%				
Compliance i koordynacja (osobodni)	284	284 000 zł	26%				
Prawnik zewnętrzny (godziny)	174	95 700 zł	9%				
Konsultant / audytor (godziny)	406	142 100 zł	13%				
Ekspert domenowy / tester (godziny)	128	38 400 zł	3%				
Licencje, opłaty, usługi, infrastruktura (zł)	102 800	102 800 zł	9%				
RAZEM rok 1 — bazowy		1 106 300 zł					
Nakład roczny w ekwiwalencie etatów (220 dni)							
Inżynierowie / ML (FTE)	0,61						
Compliance i koordynacja (FTE)	0,70						
Sankcje — kontekst, poza budżetem (nie prognoza kary)							
Art. 16: limit kwotowy 15 mln EUR (por. 3% obrotu)	64 500 000 zł						
Art. 5: limit kwotowy 35 mln EUR (por. 7% obrotu)	150 500 000 zł						
Informacje dla organów: 7,5 mln EUR (por. 1% obrotu)	32 250 000 zł						
Kwoty PLN to przeliczenie limitów kwotowych. Dla MŚP niższy limit; poza MŚP zasadniczo wyższy. Szczegóły art. 99, także SMC.							

Źródła i założenia_

Pełne odsyłacze i adresy komórek znajdują się w notatkach prowadzącego.

Program	PFR, moduł 2: technologia, 13 października 2026.
Koszty	Przekazany arkusz dostawcy systemu wysokiego ryzyka.
Narzędzia	Dokumentacja VerifyWise, promptfoo, Langfuse i MLflow. Projekt ENISA v0.4.
Przykłady	Firma Kowalskiego i mały pilotaż są przykładami szkoleniowymi.

Kwoty z arkusza to szacunki. Zrzuty pokazują przykładowe interfejsy, a nie wdrożenie w firmie.