TechStandard ADMS 01:2026

STANDARD TECHSTANDARD

Agent Deployment & Management Standard

Standard wdrażania i zarządzania agentami sztucznej inteligencji

PROJEKT DO KONSULTACJI | WERSJA 0.1 | 15 SIERPNIA 2026 R.

Informacje o dokumencie

Pole	Wartość
Kod	ADMS 01:2026
Nazwa	Agent Deployment & Management Standard
Nazwa polska	Standard wdrażania i zarządzania agentami sztucznej inteligencji
Status	Projekt do konsultacji
Wersja	0.1
Data	15 sierpnia 2026 r.
Właściciel	TechStandard
Planowany przegląd	Po konsultacjach i pilotażowym zastosowaniu w co najmniej trzech organizacjach

Status dokumentu

Dokument określa projekt wymagań TechStandard. Nie ustanawia programu certyfikacji, nie zastępuje oceny prawnej i nie potwierdza zgodności z normami ISO/IEC ani z rozporządzeniem (UE) 2024/1689.

Spis treści

Przedmowa

Organizacje coraz częściej powierzają agentom sztucznej inteligencji nie tylko przygotowanie odpowiedzi, lecz także wykonywanie czynności w systemach firmowych. Agent może odczytać zamówienie, uzupełnić rekord, utworzyć zgłoszenie, przygotować dokument, wysłać zatwierdzoną wiadomość albo uruchomić kolejną usługę. Wraz z zakresem działania rośnie znaczenie uprawnień, jakości danych, kontroli wyniku i możliwości zatrzymania agenta.

Opublikowane normy obejmują system zarządzania sztuczną inteligencją, cykl życia systemu sztucznej inteligencji, zarządzanie ryzykiem, ocenę wpływu i możliwość przejęcia kontroli. Nie tworzą jednak jednej procedury wdrożenia agenta do konkretnego zadania w organizacji. W lutym 2026 r. amerykański National Institute of Standards and Technology (NIST), czyli Narodowy Instytut Standaryzacji i Technologii, uruchomił inicjatywę dotyczącą standardów agentów sztucznej inteligencji. Potwierdza to, że zasady właściwe wyłącznie dla systemów agentowych są nadal rozwijane.

ADMS 01 łączy wymagania organizacyjne, techniczne i operacyjne potrzebne przed uruchomieniem agenta i podczas jego późniejszego użytkowania. Określa, kto wybiera zadanie, jak ustala się zakres samodzielności agenta, jak nadaje się uprawnienia, jakie testy należy przeprowadzić, kiedy sprawa wymaga decyzji pracownika oraz jak oceniać skuteczność całego systemu zarządzania.

Profile sektorowe rozwijają wymagania standardu głównego dla konkretnych branż. Nie powtarzają wspólnych wymagań, lecz dodają procesy, ryzyka, ograniczenia, przypadki testowe i dowody właściwe dla danego sektora.

Zasady stosowania słów normatywnych

W niniejszym dokumencie:

- „należy” oznacza wymaganie;
- „zaleca się” oznacza zalecenie;
- „dopuszcza się” oznacza dozwolony sposób postępowania;
- „może” oznacza możliwość albo zdolność.

Wprowadzenie

0.1. Cel systemu zarządzania

Celem systemu zarządzania agentami sztucznej inteligencji jest uzyskiwanie zaplanowanych wyników z zadań wykonywanych przez agentów przy jednoczesnym utrzymaniu odpowiedzialności organizacji, kontroli dostępu, ochrony danych, możliwości odtworzenia przebiegu oraz skutecznego udziału pracowników.

System ma prowadzić w szczególności do:

- powierzania agentom tylko jednoznacznie określonych zadań;
- dopasowania samodzielności do skutków błędu;
- ograniczenia uprawnień do niezbędnego minimum;
- wykrywania braków i rozbieżności przed wystąpieniem szkody;
- kierowania do pracownika spraw wymagających oceny lub decyzji;
- systematycznego mierzenia wyników, incydentów i wpływu na organizację;
- ciągłego doskonalenia zasad wdrażania i nadzoru.

0.2. Zgodność strukturalna z normami systemów zarządzania

Układ rozdziałów 4–10 odpowiada logice Zharmonizowanej Struktury norm systemów zarządzania, opisanej w załączniku SL do Dyrektyw ISO/IEC. Wcześniej strukturę tę określano skrótem HLS, czyli strukturą wysokiego poziomu.

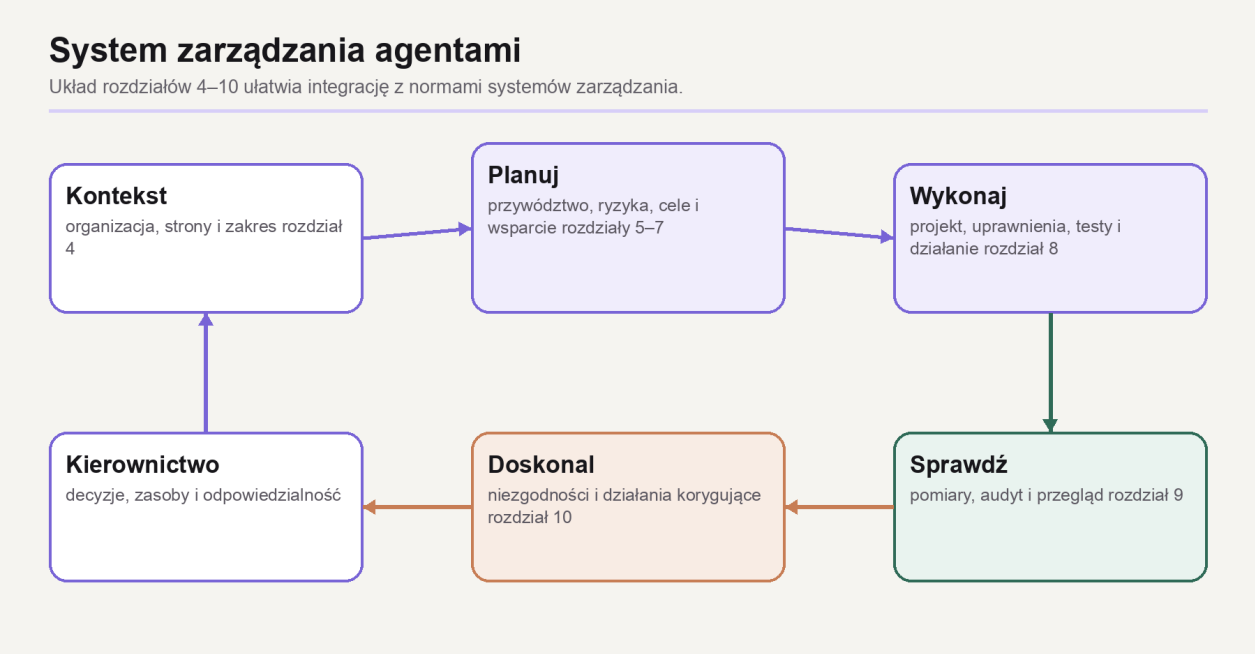
Zachowanie wspólnego układu ułatwia włączenie wymagań ADMS 01 do systemu zarządzania jakością według ISO 9001, systemu zarządzania środowiskowego według ISO 14001, systemu zarządzania bezpieczeństwem informacji według ISO/IEC 27001 oraz systemu zarządzania sztuczną inteligencją według ISO/IEC 42001. Organizacja może wykorzystać istniejące procesy nadzoru nad dokumentacją, kompetencjami, ryzykiem, audytem, przeglądem zarządzania i działaniami korygującymi.

Zgodność układu rozdziałów nie oznacza, że niniejszy dokument jest normą ISO, ani że przejmuje identyczny tekst podstawowy ISO. Mapa integracji znajduje się w Załączniku E.

0.3. Cykl zarządzania

System opiera się na cyklu Planuj–Wykonaj–Sprawdź–Doskonal, określanym skrótem PDCA od angielskich słów Plan–Do–Check–Act:

- Planuj — rozdziały 4–7: ustalenie kontekstu, odpowiedzialności, ryzyk, celów i zasobów;
- Wykonaj — rozdział 8: kwalifikacja zadania, projekt, testy, uruchomienie i bieżące działanie;
- Sprawdź — rozdział 9: pomiary, audyt wewnętrzny i przegląd zarządzania;
- Doskonal — rozdział 10: usuwanie przyczyn niezgodności i doskonalenie systemu.



Rysunek 1. Model systemu zarządzania agentami

0.4. Zasada proporcjonalności

Zakres dokumentacji, kontroli i testów powinien odpowiadać skutkom błędu, poziomowi samodzielności, rodzajowi danych oraz liczbie spraw. Proporcjonalność nie może prowadzić do pominięcia wymagań dotyczących legalności, ochrony danych, zatrzymania działania ani odtworzenia przebiegu.

1. Zakres

1.1. Standard określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i doskonalenia systemu zarządzania agentami sztucznej inteligencji w organizacji.

1.2. Standard stosuje się do agentów, które wykonują czynności w imieniu organizacji, korzystają z jej danych lub systemów albo przekazują wynik do dalszego działania.

1.3. Standard stosuje się niezależnie od dostawcy modelu, sposobu utrzymania systemu i wielkości organizacji.

1.4. Organizacja może objąć systemem całość działalności, wybrane jednostki organizacyjne albo określone rodzaje zadań, pod warunkiem że zakres nie wprowadza stron zainteresowanych w błąd i obejmuje wszystkie zależności potrzebne do skutecznego nadzoru.

1.5. Standard nie zastępuje oceny prawnej, oceny zgodności wymaganej przepisami, wdrożenia ISO/IEC 42001 ani wymagań sektorowych. Jeżeli przepisy, umowy lub właściwy profil sektorowy ustanawiają wymagania surowsze, należy zastosować wymagania surowsze.

1.6. Standard nie upoważnia agenta do wykonywania czynności zabronionych prawem, umową, regulaminem organizacji albo decyzją właściciela zadania.

2. Powołania normatywne

Niniejszy dokument nie zawiera powołań normatywnych, bez których jego stosowanie byłoby niemożliwe. Dokumenty wykorzystane podczas opracowania standardu oraz materiały przydatne do jego stosowania podano w Załączniku G.

3. Terminy i definicje

3.1. system zarządzania agentami sztucznej inteligencji

Powiązane elementy organizacji służące ustalaniu polityki, celów, odpowiedzialności, procesów i środków nadzoru dotyczących agentów sztucznej inteligencji.

3.2. agent sztucznej inteligencji

System informatyczny wykorzystujący sztuczną inteligencję (AI), który na podstawie celu, danych i ustalonych zasad wybiera oraz wykonuje kolejne czynności, w tym korzysta z narzędzi lub systemów zewnętrznych.

3.3. zadanie

Wyodrębniony ciąg czynności mający określony początek, wynik, właściciela i kryteria poprawnego wykonania.

3.4. właściciel zadania

Osoba odpowiedzialna za sposób wykonania zadania, reguły postępowania, wyjątki i akceptację wyniku biznesowego.

3.5. właściciel agenta

Osoba odpowiedzialna za utrzymanie zakresu działania agenta, jego uprawnienia, wyniki, zmiany i wycofanie.

3.6. agent wykonawczy

Agent, który wykonuje zatwierdzone czynności składające się na zadanie i przygotowuje albo zapisuje wynik.

3.7. składnik kontrolny

Oddzielony logicznie mechanizm, który sprawdza wynik agenta wykonawczego względem danych źródłowych i ustalonych kryteriów. Składnikiem kontrolnym może być reguła deterministyczna, drugi model, inny agent albo połączenie tych rozwiązań.

3.8. niezależna kontrola

Kontrola zaprojektowana tak, aby ograniczyć ryzyko powtórzenia tego samego błędu. Sama druga odpowiedź tego samego modelu, oparta na tych samych danych i poleceniu, nie stanowi wystarczającego dowodu niezależności.

3.9. poziom samodzielności

Zatwierdzony zakres, w którym agent może wykonywać czynności bez uprzedniej decyzji pracownika.

3.10. wyjątek

Przypadek, którego agent nie może jednoznacznie obsłużyć według zatwierdzonych reguł albo który przekracza jego uprawnienia.

3.11. przekazanie sprawy

Zatrzymanie samodzielnego działania agenta i przekazanie pracownikowi danych, dotychczasowych czynności oraz powodu wymagającego decyzji.

3.12. incydent

Zdarzenie, które spowodowało albo mogło spowodować nieuprawnione działanie, szkodę, naruszenie prawa lub umowy, utratę danych, błędny wynik o istotnym skutku albo utratę kontroli nad agentem.

3.13. niezgodność

Niespełnienie wymagania niniejszego standardu albo wymagania ustanowionego przez organizację dla systemu zarządzania agentami.

3.14. udokumentowana informacja

Informacja, którą organizacja utrzymuje i nadzoruje, wraz z nośnikiem, na którym została zapisana. Obejmuje dokumenty opisujące sposób działania oraz zapisy stanowiące dowód wykonania.

3.15. profil sektorowy

Dokument uzupełniający ADMS 01 o procesy, ryzyka, wymagania prawne, testy i kryteria właściwe dla określonej branży.

4. Kontekst organizacji

4.1. Zrozumienie organizacji i jej kontekstu

KON-01. Organizacja powinna określić zewnętrzne i wewnętrzne czynniki mające wpływ na zdolność systemu zarządzania agentami do osiągania zaplanowanych wyników.

KON-02. Analiza kontekstu powinna obejmować co najmniej strategię, procesy, strukturę odpowiedzialności, kulturę organizacyjną, kompetencje, systemy informatyczne, jakość danych, zależności od dostawców, wymagania prawne i umowne oraz możliwe skutki błędu.

KON-03. Organizacja powinna ustalić, czy zmiana klimatu jest istotnym czynnikiem dla zakresu systemu, w szczególności ze względu na ciągłość infrastruktury, zużycie zasobów obliczeniowych lub wymagania stron zainteresowanych.

KON-04. Informacje o kontekście należy przeglądać po istotnej zmianie organizacyjnej, technologicznej, prawnej lub sektorowej oraz w zaplanowanych odstępach.

4.2. Potrzeby i oczekiwania stron zainteresowanych

KON-05. Organizacja powinna wskazać strony zainteresowane, które wpływają na system zarządzania agentami albo mogą odczuć skutki działania agentów.

KON-06. Należy uwzględnić odpowiednio pracowników, klientów, osoby, których dane są przetwarzane, kierownictwo, właścicieli procesów i systemów, dostawców, organy nadzoru, partnerów oraz podmioty wykonujące audyt lub ocenę.

KON-07. Dla każdej istotnej strony należy ustalić wymagania prawne, umowne i organizacyjne oraz potrzeby przyjęte przez organizację jako zobowiązanie.

KON-08. Należy ustalić, czy organizacja występuje jako dostawca, podmiot stosujący, importer, dystrybutor lub inny uczestnik łańcucha wartości w rozumieniu właściwych przepisów. Ustalenie powinien zatwierdzić kompetentny prawnik albo osoba odpowiedzialna za zgodność, jeżeli rola ma skutki prawne.

4.3. Określenie zakresu systemu zarządzania agentami

KON-09. Organizacja powinna określić granice i zastosowanie systemu, uwzględniając kontekst, wymagania stron zainteresowanych, jednostki organizacyjne, zadania, agentów, dane, systemy i lokalizacje.

KON-10. Zakres należy utrzymywać jako udokumentowaną informację i udostępniać osobom odpowiedzialnym za wdrożenie, audyt i przegląd.

KON-11. Wyłączenie zadania, systemu lub jednostki nie może uniemożliwiać nadzoru nad zależnością wpływającą na działanie agenta objętego zakresem.

4.4. System zarządzania agentami sztucznej inteligencji

SYS-01. Organizacja powinna ustanowić, wdrożyć, utrzymywać i doskonalić procesy potrzebne do zarządzania agentami oraz ich wzajemne powiązania.

SYS-02. Procesy powinny obejmować co najmniej kwalifikację zadania, ocenę ryzyka i wpływu, projektowanie, nadawanie uprawnień, testy, pilotaż, decyzję o uruchomieniu, nadzór, obsługę incydentów, zarządzanie zmianą i wycofanie.

SYS-03. Dla każdego procesu należy określić dane wejściowe, wynik, odpowiedzialność, kryteria, zasoby, wymagane zapisy i sposób oceny skuteczności.

5. Przywództwo

5.1. Przywództwo i zaangażowanie

PRZ-01. Najwyższe kierownictwo powinno odpowiadać za skuteczność systemu zarządzania agentami w zakresie, którym kieruje.

PRZ-02. Kierownictwo powinno zapewnić zgodność polityki i celów dotyczących agentów z kierunkiem działania organizacji oraz włączyć wymagania systemu do procesów biznesowych.

PRZ-03. Kierownictwo powinno zapewnić zasoby, usuwać sprzeczność celów, wspierać zgłaszanie problemów i wymagać wykazania skuteczności przed rozszerzeniem samodzielności agenta.

PRZ-04. Cele szybkości, oszczędności lub liczby obsłużonych spraw nie mogą zachęcać do pomijania kontroli, ukrywania wyjątków ani przenoszenia nieujawnionej pracy na pracowników.

PRZ-05. Odpowiedzialność organizacji za wynik nie może zostać przeniesiona na model, agenta, dostawcę technologii ani pracownika, któremu nie zapewniono informacji i uprawnień do podjęcia decyzji.

5.2. Polityka zarządzania agentami

POL-01. Kierownictwo powinno ustanowić politykę odpowiednią do celu, kontekstu i skutków działania agentów.

POL-02. Polityka powinna zawierać zobowiązanie do spełniania właściwych wymagań, ochrony danych i praw osób, nadawania najmniejszych niezbędnych uprawnień, zapewnienia możliwości zatrzymania oraz ciągłego doskonalenia.

POL-03. Polityka powinna stanowić podstawę do ustalania celów, być utrzymywana jako udokumentowana informacja, zakomunikowana wewnątrz organizacji i dostępna dla właściwych stron zainteresowanych.

5.3. Role, odpowiedzialność i uprawnienia organizacyjne

ROL-01. Kierownictwo powinno wyznaczyć właściciela systemu zarządzania agentami i zapewnić mu prawo do przedstawiania wyników oraz problemów bezpośrednio kierownictwu.

ROL-02. Dla każdego wdrożenia należy wyznaczyć co najmniej właściciela zadania, właściciela agenta, osobę odpowiedzialną za bezpieczeństwo, administratora właściwego systemu oraz osobę uprawnioną do zatrzymania działania.

ROL-03. Właściciel zadania powinien określić prawidłowy wynik, wyjątki, wartości graniczne, czynności zabronione i sytuacje wymagające decyzji pracownika.

ROL-04. Właściciel agenta powinien odpowiadać za aktualność Karty agenta, przegląd wyników, zatwierdzanie zmian i rozpoczęcie procedury wycofania.

ROL-05. Osoba odpowiedzialna za bezpieczeństwo powinna zatwierdzić sposób uwierzytelnienia, zakres uprawnień, przechowywanie sekretów, rejestrowanie czynności i połączenia zewnętrzne.

ROL-06. Administrator systemu powinien nadawać uprawnienia na podstawie zatwierdzonego wniosku. Projektant agenta nie powinien samodzielnie zatwierdzać własnych uprawnień produkcyjnych.

ROL-07. Osoba sprawująca nadzór powinna mieć dostęp do informacji potrzebnych do oceny sprawy oraz prawo do zatrzymania, odrzucenia lub poprawienia wyniku agenta.

ROL-08. Dla wdrożeń o poważnych skutkach należy zapewnić przegląd przeprowadzony przez osobę, która nie budowała ocenianego rozwiązania.

5.4. Udział pracowników i rozpatrywanie obaw

LUD-01. Przed pilotażem należy wskazać pracowników, których zadania, odpowiedzialność, obciążenie lub sposób oceny mogą się zmienić.

LUD-02. Pracownicy wykonujący dane zadanie powinni uczestniczyć w opisie czynności, wyjątków i najczęstszych błędów. Ich udział nie może ograniczać się do szkolenia po zakończeniu projektu.

LUD-03. Organizacja powinna zebrać i rozpatrzyć obawy dotyczące utraty kontroli, odpowiedzialności za błąd, zwiększenia tempa pracy, ograniczenia stanowisk, wykorzystania danych oraz niejasnych zasad oceny pracownika.

LUD-04. Nie należy określać uzasadnionej obawy mianem oporu wobec zmiany bez ustalenia jej przyczyny. Wynik rozpatrzenia obawy należy przekazać osobie, która ją zgłosiła.

LUD-05. Jeżeli wdrożenie zmienia zakres obowiązków, sposób oceny albo zapotrzebowanie na dane stanowisko, organizacja powinna podjąć i zakomunikować tę decyzję odrębnie. Zmiana zatrudnienia nie powinna pozostawać ukrytym skutkiem wdrożenia technicznego.

6. Planowanie

6.1. Działania odnoszące się do ryzyk i szans

RYZ-01. Organizacja powinna określić ryzyka i szanse wynikające z kontekstu, wymagań stron zainteresowanych, celu zadania, danych, samodzielności, dostawców i możliwych skutków błędu.

RYZ-02. Ocena powinna obejmować co najmniej błędny wynik, nieuprawnioną czynność, ujawnienie danych, brak możliwości odtworzenia przebiegu, nadużycie narzędzia, zależność od dostawcy, niedostępność systemu, wspólne źródło błędu kontroli oraz wpływ na pracowników i klientów.

RYZ-03. Działania ograniczające ryzyko należy włączyć do projektu, testów, uprawnień, nadzoru i procedur awaryjnych, a ich skuteczność należy oceniać.

RYZ-04. Szanse, takie jak skrócenie czasu wykonania, poprawa kompletności, szybsze wykrywanie rozbieżności i odciążenie pracowników od czynności powtarzalnych, należy oceniać za pomocą ustalonych miar.

6.1.1. Klasa wdrożeniowa

Klasa wdrożeniowa służy do dobrania kontroli wewnętrznych. Nie zastępuje klasyfikacji prawnej wynikającej z rozporządzenia (UE) 2024/1689.

- K1 — błąd jest łatwo odwracalny i nie powoduje istotnego skutku poza organizacją;
- K2 — błąd może wpłynąć na klienta, termin, koszt lub dane firmowe, ale skutek jest ograniczony i odwracalny;
- K3 — błąd może spowodować istotną stratę, naruszenie poufności, niewykonanie obowiązku umownego albo skutek dla praw osoby;
- K4 — zadanie dotyczy bezpieczeństwa, zdrowia, praw podstawowych, znacznych zobowiązań finansowych albo systemu uznanego za system sztucznej inteligencji wysokiego ryzyka.

KL-01. Klasę należy ustalić przed nadaniem agentowi dostępu do rzeczywistych danych.

KL-02. Jeżeli skutki odpowiadają więcej niż jednej klasie, należy przyjąć klasę wyższą.

KL-03. Klasy K3 i K4 wymagają udokumentowanej oceny wpływu, niezależnego przeglądu oraz zatwierdzenia przez kierownictwo.

KL-04. Zastosowanie agenta w klasie K4 wymaga odrębnego sprawdzenia przepisów sektorowych i warunków dopuszczalności. Samo spełnienie ADMS 01 nie stanowi podstawy prawnej do uruchomienia.

6.1.2. Poziom samodzielności

- S0 — agent wyłącznie wyszukuje lub porządkuje informacje;
- S1 — agent przygotowuje propozycję, a pracownik wykonuje czynność;
- S2 — agent wykonuje czynność po zatwierdzeniu każdej sprawy;
- S3 — agent samodzielnie obsługuje sprawy mieszczące się w ustalonych granicach, a pozostałe przekazuje pracownikowi;
- S4 — agent planuje i wykonuje wieloetapowe zadania w kilku systemach bez zatwierdzania każdej czynności, w granicach zatwierdzonego celu i uprawnień.

SAM-01. Poziom samodzielności należy zatwierdzić osobno dla każdego rodzaju czynności.

SAM-02. Podniesienie poziomu samodzielności jest zmianą istotną i wymaga ponownej oceny ryzyka oraz testów.

SAM-03. Brak reguły, brak danych, przekroczenie wartości granicznej albo niejednoznaczność wyniku powinny powodować zatrzymanie czynności lub przekazanie sprawy pracownikowi.

6.1.3. Kryteria doboru samodzielności i kontroli

KRY-01. Przy ustalaniu poziomu samodzielności należy ocenić co najmniej skutek zewnętrzny czynności, wartość finansową, rodzaj danych, odwracalność wyniku, czas potrzebny do wykrycia błędu, częstotliwość wykonania oraz potrzebę osądu zawodowego.

KRY-02. Organizacja powinna ustanowić wartości graniczne właściwe dla zadania, takie jak maksymalna kwota, liczba rekordów, zakres klientów, rodzaj dokumentu, czas działania lub dopuszczalna liczba kolejnych czynności.

KRY-03. Kryteria należy ustalić przed testami odbiorowymi. Zmiana kryterium po poznaniu wyniku wymaga uzasadnienia, zatwierdzenia i ponownej oceny ryzyka.

KRY-04. Własne kryterium organizacji powinno być jednoznaczne, mierzalne albo możliwe do obiektywnego sprawdzenia, powiązane z dowodem oraz przypisane do osoby uprawnionej do jego zatwierdzenia.

KRY-05. Kryteria opracowane w ramach ADMS 01 powinny podlegać konsultacjom z przedstawicielami właściwych funkcji i sektorów, próbom zastosowania oraz nadzorowi nad wersją. Kryterium niesprawdzone w praktyce należy oznaczyć jako projektowe.

Poziom	Działanie agenta	Warunek zastosowania	Minimalna kontrola
S0	wyszukuje lub porządkuje informacje	brak zmiany danych i brak decyzji zewnętrznej	kontrola źródeł, dostępu i kompletności
S1	przygotowuje propozycję	pracownik wykonuje właściwą czynność	czytelne wskazanie źródeł i ograniczeń
S2	wykonuje po zatwierdzeniu każdej sprawy	skutek wymaga każdorazowego osądu lub zgody	zatwierdzenie przez uprawnioną osobę przed wykonaniem
S3	samodzielnie kończy sprawy typowe	reguły, granice i wyjątki są mierzalne	automatyczna kontrola wyniku, limity i przekazanie wyjątków
S4	samodzielnie planuje zadanie wieloetapowe	kolejne czynności mieszczą się w zatwierdzonym celu i są odtwarzalne	niezależna bramka kontrolna, limity etapów, zatrzymanie i pełny zapis przebiegu

KRY-06. Dla klasy K1 dopuszcza się poziomy S0–S4 po spełnieniu wymagań właściwych dla danego poziomu.

KRY-07. Dla klasy K2 poziom S4 wymaga niezależnej bramki kontrolnej, limitu skutku i sprawdzonej procedury cofnięcia albo skorygowania wyniku.

KRY-08. Dla klasy K3 poziom S4 można zastosować wyłącznie po udokumentowanej ocenie wpływu, niezależnym przeglądzie, zatwierdzeniu przez kierownictwo i wskazaniu podstawy w profilu sektorowym.

KRY-09. Dla klasy K4 domyślnym najwyższym poziomem jest S2. Poziom S3 można zastosować tylko wtedy, gdy prawo na to pozwala, profil sektorowy określa dodatkowe zabezpieczenia, a organizacja zapewnia skuteczny nadzór i automatyczne zatrzymanie. Poziomu S4 nie uznaje się za zgodny z niniejszym wydaniem ADMS 01.

6.2. Cele i planowanie ich osiągnięcia

CEL-01. Organizacja powinna ustanowić mierzalne cele odpowiednie do polityki, zadań, ryzyk i potrzeb stron zainteresowanych.

CEL-02. Cel powinien określać oczekiwany wynik, miarę, wartość docelową, termin, odpowiedzialność, zasoby i sposób oceny.

CEL-03. Cele powinny obejmować nie tylko szybkość i koszt, lecz także jakość wyniku, poprawność przekazań, liczbę niedozwolonych czynności, kompletność zapisów i wpływ na pracowników.

CEL-04. Nie należy uznawać wzrostu liczby spraw zakończonych przez agenta za poprawę, jeżeli równocześnie wzrosła liczba poprawek, incydentów albo pracy przeniesionej na pracowników.

6.3. Planowanie zmian

ZMI-01. Zmiany systemu zarządzania oraz poszczególnych agentów należy planować z uwzględnieniem celu, skutków, spójności procesów, zasobów i odpowiedzialności.

ZMI-02. Zmianę wpływającą na cel, dane, model, narzędzia, uprawnienia, poziom samodzielności, reguły kontroli lub użytkowników należy uznać za zmianę istotną.

ZMI-03. Zmiana istotna wymaga ponownej oceny ryzyka i testów w zakresie, na który wpływa.

7. Wsparcie

7.1. Zasoby

ZAS-01. Organizacja powinna zapewnić osoby, czas, dane, infrastrukturę, narzędzia, środki finansowe i dostęp do wiedzy potrzebne do ustanowienia, działania i doskonalenia systemu.

ZAS-02. Zasoby powinny obejmować zdolność do testowania poza środowiskiem produkcyjnym, monitorowania działania, przechowywania zapisów, zarządzania sekretami i niezwłocznego odebrania uprawnień.

ZAS-03. Organizacja powinna ustalić wiedzę potrzebną do prawidłowego wykonywania zadania oraz sposób jej aktualizacji po zmianie procesu, prawa, produktu lub danych.

7.2. Kompetencje

KOM-01. Organizacja powinna określić kompetencje osób projektujących, zatwierdzających, administrujących, nadzorujących, audytujących i wykorzystujących agentów.

KOM-02. Kompetencje powinny wynikać z wykształcenia, szkolenia lub doświadczenia, a dowody kompetencji należy przechowywać.

KOM-03. Szkolenie powinno obejmować możliwości i ograniczenia agenta, rozpoznawanie błędów, ochronę danych, przekazanie sprawy, zatrzymanie działania i zgłaszanie incydentu.

7.3. Świadomość

SWI-01. Osoby uczestniczące w działaniu systemu powinny znać politykę, właściwe cele, własną odpowiedzialność, skutki niespełnienia wymagań oraz sposób zgłaszania problemu.

SWI-02. Pracownik powinien wiedzieć, które czynności wykonuje agent, kiedy sprawa wraca do człowieka, kto podejmuje decyzję oraz jak zatrzymać działanie bez obawy o nieuzasadnione konsekwencje.

7.4. Komunikacja

KOMU-01. Organizacja powinna określić, co, kiedy, komu, w jaki sposób i przez kogo jest komunikowane w sprawach dotyczących agentów.

KOMU-02. Komunikacja powinna obejmować co najmniej zmiany zakresu, uruchomienie, ograniczenia, incydenty, wyniki przeglądu, decyzje dotyczące pracowników oraz wymagane informacje dla klientów i organów.

KOMU-03. Jeżeli odbiorca może uznać, że kontaktuje się z człowiekiem, organizacja powinna ocenić obowiązek i zasadność poinformowania go o działaniu systemu sztucznej inteligencji.

7.5. Udokumentowane informacje

7.5.1. Wymagany zakres

DOK-01. System powinien obejmować udokumentowane informacje wymagane przez niniejszy standard oraz informacje uznane przez organizację za potrzebne do skutecznego działania.

DOK-02. Dla każdego agenta produkcyjnego należy utrzymywać Kartę agenta, której minimalną zawartość określa Załącznik B.

DOK-03. Przed uruchomieniem należy posiadać co najmniej Kartę zadania, pomiar stanu wyjściowego, ocenę ryzyka, wymaganą ocenę wpływu, matrycę uprawnień, plan testów, Raport z testów, Raport z pilotażu, materiały szkoleniowe i Decyzję o uruchomieniu.

DOK-04. Po uruchomieniu należy prowadzić Rejestr działania, Rejestr wyjątków, Rejestr incydentów, Rejestr zmian oraz protokoły przeglądów.

7.5.2. Tworzenie i aktualizacja

DOK-05. Udokumentowana informacja powinna mieć identyfikator, tytuł, właściciela, wersję, datę, zatwierdzenie i format odpowiedni do zastosowania.

DOK-06. Przed wydaniem lub zmianą należy sprawdzić przydatność, poprawność i spójność informacji.

7.5.3. Nadzór

DOK-07. Organizacja powinna zapewnić dostępność właściwej wersji w miejscu użycia oraz ochronę przed nieuprawnioną zmianą, utratą i ujawnieniem.

DOK-08. Należy ustalić zasady dostępu, dystrybucji, przechowywania, odtwarzania, zmian, archiwizacji i usuwania.

DOK-09. Okres przechowywania zapisów należy ustalić z uwzględnieniem prawa, umów, celu dowodowego, poufności i minimalizacji danych.

8. Działania operacyjne

8.1. Planowanie i nadzór nad działaniami operacyjnymi

OPER-01. Organizacja powinna zaplanować, wdrożyć i nadzorować procesy potrzebne do spełnienia wymagań systemu oraz działania określone w rozdziale 6.

OPER-02. Dla każdego wdrożenia należy określić kryteria prowadzenia procesu, kryteria odbioru wyniku, wymagane zasoby i zapisy potwierdzające wykonanie zgodnie z planem.

OPER-03. Proces zlecony dostawcy zewnętrznemu powinien pozostawać objęty nadzorem organizacji. Umowa z dostawcą nie przenosi odpowiedzialności za wynik stosowania agenta.

Rysunek 2. Cykl wdrożenia agenta

8.2. Kwalifikacja i opis zadania

ZAD-01. Przed rozpoczęciem projektu należy wskazać jednoznacznie nazwane zadanie, jego początek, wynik, właściciela oraz systemy wykorzystywane do wykonania.

ZAD-02. Nie należy określać zakresu wyłącznie nazwą stanowiska, działu albo ogólnym sformułowaniem „obsługa procesu”. Agent wykonuje określone zadanie lub czynności, a nie całe stanowisko pracy.

ZAD-03. Należy opisać kolejne czynności, dane wejściowe, systemy, decyzje, wyjątki i sposób zakończenia zadania.

ZAD-04. Opis należy sprawdzić na rzeczywistych przypadkach, w tym na przypadkach nietypowych, z udziałem osób wykonujących dane zadanie.

ZAD-05. Przed wyborem zadania należy ustalić częstotliwość, czas wykonania, liczbę poprawek, liczbę wyjątków, koszt błędu i stan wyjściowy wskaźników.

> **Wynik etapu: zatwierdzona Karta zadania, opis obecnego sposobu wykonania, wykaz wyjątków i pomiar stanu wyjściowego.**

8.3. Ocena wpływu i projekt rozwiązania

PRO-01. Przed budową należy ustalić role prawne, klasę wdrożeniową, poziom samodzielności, dane chronione, skutki dla pracowników, skutki błędu, podatność na nadużycie i zależności od dostawców.

PRO-02. Należy wskazać czynności, których agent nie może wykonywać, wartości wymagające decyzji pracownika, sposób kontroli wyniku i warunki zatrzymania.

PRO-03. Projekt powinien określać agenta wykonawczego, składnik kontrolny, narzędzia, systemy, dane, reguły przekazania sprawy i sposób odtworzenia przebiegu.

PRO-04. Dla każdego narzędzia należy opisać dozwolone czynności, ich skutki, limity i sposób cofnięcia albo skorygowania wyniku.

Wynik etapu: Rejestr ryzyka, ocena wpływu, projekt techniczny, matryca uprawnień i plan testów.

8.3.1. Sposób utrzymania modelu

Organizacja powinna przypisać rozwiązanie do jednego lub kilku wariantów:

- M1 — model utrzymywany na infrastrukturze pozostającej pod bezpośrednim zarządem organizacji;
- M2 — model utrzymywany w wydzielonym środowisku dostawcy chmurowego;
- M3 — model udostępniany przez zewnętrzny interfejs programistyczny aplikacji (API), czyli usługę wywoływaną przez system organizacji;
- M4 — rozwiązanie mieszane, w którym dane, modele lub czynności są rozdzielone pomiędzy środowisko organizacji i dostawców.

MOD-01. Wybór wariantu należy udokumentować na podstawie wymagań zadania, danych, prawa, bezpieczeństwa, ciągłości, kosztu i zdolności organizacji do utrzymania rozwiązania.

MOD-02. Dla każdego wariantu należy ustalić, kto ma dostęp do danych wejściowych i wyników, gdzie odbywa się przetwarzanie, jak długo dane są przechowywane, czy mogą służyć do doskonalenia modelu oraz jacy podwykonawcy uczestniczą w usłudze.

MOD-03. Należy ustalić sposób identyfikowania wersji modelu, informowania o zmianie, zatwierdzania zmiany i przeprowadzania ponownych testów.

MOD-04. Należy zapewnić dostęp do zapisów potrzebnych do odtworzenia przebiegu, z zastrzeżeniem ochrony danych i tajemnic prawnie chronionych.

MOD-05. Dla rozwiązania zewnętrznego należy określić warunki przeniesienia usługi, odzyskania danych, zakończenia umowy i bezpiecznego przejścia do innego dostawcy albo rozwiązania zastępczego.

MOD-06. Utrzymanie modelu na własnej infrastrukturze nie zwalnia z oceny kompetencji, aktualizacji, podatności, pochodzenia modelu i bezpieczeństwa łańcucha dostaw.

MOD-07. Korzystanie z zewnętrznego interfejsu nie stanowi samo w sobie dowodu, że dane nie są przechowywane lub wykorzystywane przez dostawcę. Organizacja powinna opierać się na ustawieniach usługi, umowie i możliwych do sprawdzenia informacjach dostawcy.

8.4. Dane, tożsamość i uprawnienia

Rysunek 4. Procedura nadania uprawnień

8.4.1. Tożsamość agenta

UPR-01. Każdy agent działający w systemie produkcyjnym powinien posiadać rozpoznawalną tożsamość techniczną, odrębną od konta pracownika i innych agentów.

UPR-02. Nie należy używać wspólnych haseł lub kluczy, które uniemożliwiają ustalenie, który agent wykonał czynność.

8.4.2. Matryca uprawnień

UPR-03. Dla każdego systemu należy odrębnie zatwierdzić prawo do odczytu, wyszukiwania, tworzenia, zmiany, zatwierdzania, wysyłania, pobierania plików i usuwania.

UPR-04. Matryca powinna wskazywać właściciela uprawnienia, uzasadnienie, środowisko, datę nadania, termin przeglądu i sposób odebrania.

UPR-05. Uprawnienia należy ograniczyć według rodzaju danych, rekordu, klienta, wartości, czasu lub liczby czynności, jeżeli system na to pozwala.

UPR-06. Agent kontrolny nie powinien mieć uprawnień do zmiany danych produkcyjnych, które sam ocenia.

8.4.3. Nadawanie i przegląd uprawnień

UPR-07. Uprawnienie produkcyjne można nadać po zatwierdzeniu projektu i zaliczeniu testów dotyczących danego systemu.

UPR-08. Nadanie, rozszerzenie i odebranie uprawnienia powinno pozostawiać zapis.

UPR-09. Uprawnienia należy przeglądać okresowo oraz po zmianie zadania, właściciela, modelu, narzędzia lub dostawcy.

8.4.4. Sekrety, dane i połączenia

UPR-10. Hasła, klucze i inne dane uwierzytelniające należy przechowywać w przeznaczonym do tego mechanizmie zarządzania sekretami. Nie należy umieszczać ich w poleceniu, kodzie źródłowym, pliku przekazywanym modelowi ani zapisie rozmowy.

UPR-11. Należy kontrolować adresy i usługi, z którymi agent może się łączyć. Dostęp do otwartego internetu nie powinien być domyślny.

UPR-12. Dane pochodzące z wiadomości, stron internetowych i dokumentów zewnętrznych należy traktować jako niezaufane. Nie mogą one samodzielnie rozszerzyć celu ani uprawnień agenta.

8.5. Budowa, testy i pilotaż

8.5.1. Budowa

BUD-01. Budowę i pierwsze testy należy prowadzić bez niekontrolowanego dostępu do produkcyjnych danych i systemów.

BUD-02. Wersje modelu, poleceń, reguł, narzędzi i konfiguracji należy identyfikować w sposób umożliwiający powiązanie z wynikiem testu.

8.5.2. Plan i zakres testów

TEST-01. Plan testów należy zatwierdzić przed rozpoczęciem testów odbiorowych. Powinien wskazywać przypadki, wynik oczekiwany, miarę, próg zaliczenia i osobę oceniającą.

TEST-02. Przypadki wykorzystane do doskonalenia rozwiązania należy oddzielić od przypadków służących do końcowej oceny, jeżeli liczba dostępnych spraw na to pozwala.

TEST-03. Należy przeprowadzić testy typowych spraw, wyjątków, brakujących danych, danych sprzecznych, nieprawidłowych formatów, powtórzonych zgłoszeń i wartości granicznych.

TEST-04. Należy sprawdzić, czy agent nie wykonuje czynności wykraczających poza zatwierdzony cel i uprawnienia.

TEST-05. Należy przeprowadzić próby wymuszenia zmiany celu, ujawnienia danych, użycia niedozwolonego narzędzia, wykonania nieoczekiwanego kodu i wykorzystania nadmiernych uprawnień.

TEST-06. Należy sprawdzić działanie podczas niedostępności systemu źródłowego, przekroczenia czasu, przerwania połączenia, otrzymania częściowego wyniku i ponowienia czynności.

TEST-07. Dla rozwiązania ze składnikiem kontrolnym należy zmierzyć liczbę błędów zaakceptowanych przez oba składniki oraz liczbę poprawnych wyników niesłusznie odrzuconych.

TEST-08. Należy sprawdzić zatrzymanie awaryjne, odebranie uprawnień i możliwość odtworzenia przebiegu wybranego przypadku.

8.5.3. Pilotaż

PIL-01. Pilotaż należy prowadzić na ograniczonym zakresie spraw, użytkowników, danych, czasu lub wartości.

PIL-02. Podczas pilotażu należy porównywać wynik agenta z ustalonym wynikiem prawidłowym oraz rejestrować poprawki, błędy i nieuzasadnione przekazania.

PIL-03. Zakres pilotażu powinien obejmować wystarczającą liczbę przypadków, aby sprawdzić typowe sprawy i istotne wyjątki, a nie tylko upływ określonego czasu.

> **Wynik etapu: Raport z testów, Raport z pilotażu i decyzja o poprawie, rozszerzeniu albo zakończeniu projektu.**

8.6. Odbiór i uruchomienie

ODB-01. Progi odbioru należy ustalić przed uzyskaniem końcowych wyników. Nie należy obniżać progu po teście bez udokumentowanego uzasadnienia i ponownej oceny ryzyka.

ODB-02. Odbiór powinien uwzględniać co najmniej poprawność wyniku, poprawność przekazania sprawy, brak niedozwolonej czynności, czas wykonania i kompletność zapisu działania.

ODB-03. Agent nie powinien zostać uruchomiony, jeżeli nie zaliczył testu uprawnienia, zatrzymania lub ochrony danych, nawet gdy osiągnął oczekiwany wynik biznesowy.

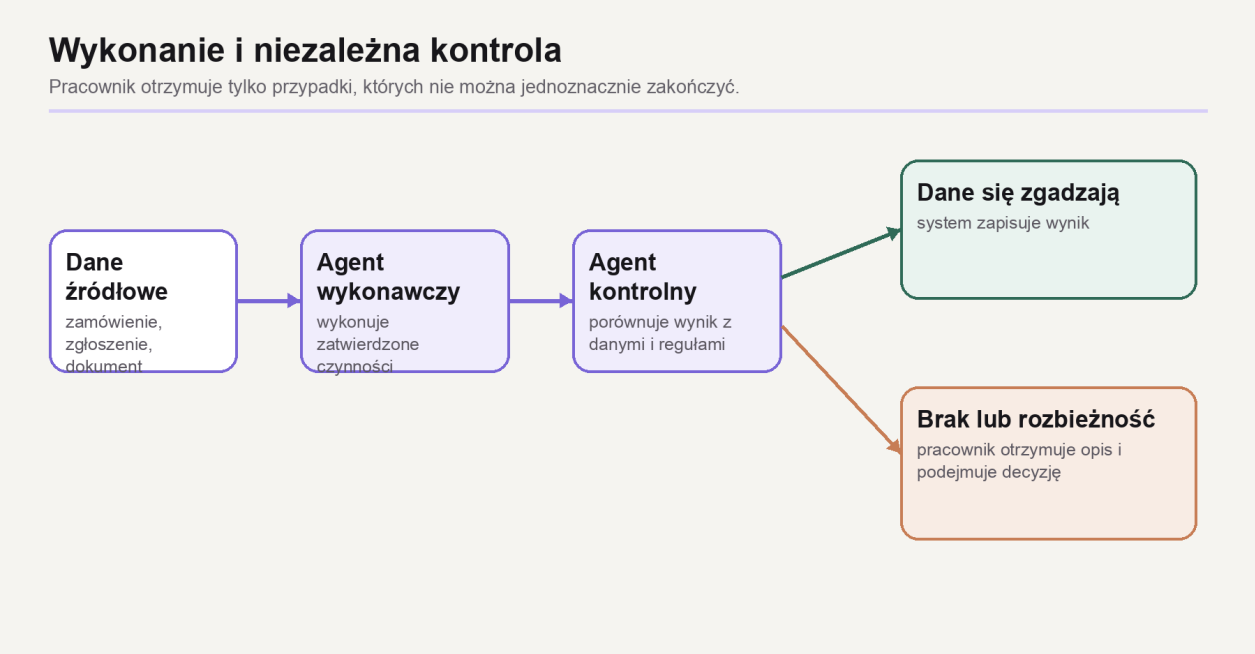
ODB-04. Decyzję o uruchomieniu można podjąć po spełnieniu kryteriów odbioru, zatwierdzeniu uprawnień, przeszkoleniu osób i sprawdzeniu procedury zatrzymania.

ODB-05. Decyzję powinni zatwierdzić co najmniej właściciel zadania i właściciel agenta. Dla klas K3 i K4 wymagane jest także zatwierdzenie kierownictwa oraz osoby odpowiedzialnej za bezpieczeństwo lub zgodność.

ODB-06. Uruchomienie należy rozpocząć od zakresu mniejszego niż docelowy, jeżeli skutki błędu przekraczają klasę K1.

Wynik etapu: podpisana Decyzja o uruchomieniu z zakresem, limitami, datą i osobami zatwierdzającymi.

8.7. Wykonanie zadania i kontrola wyniku



Rysunek 3. Wykonanie zadania i niezależna kontrola

WYK-01. Agent wykonawczy powinien otrzymać tylko dane i narzędzia potrzebne do bieżącego zadania.

WYK-02. Wynik przeznaczony do automatycznego zapisu powinien zostać sprawdzony względem danych źródłowych i ustalonych reguł.

WYK-03. Kontrola powinna wykorzystywać reguły deterministyczne zawsze wtedy, gdy wynik można sprawdzić jednoznacznie, na przykład sumę, format, limit, zgodność identyfikatora lub kompletność wymaganych pól.

WYK-04. Drugi model nie jest wymagany dla każdego wdrożenia. Jeżeli kontrolę wykonuje drugi agent lub model, należy ocenić wspólne źródła błędu i zapewnić odpowiednią niezależność kontroli.

WYK-05. Dla klas K3 i K4 zaleca się zastosowanie różnorodnych środków kontroli, na przykład odrębnego modelu, innego polecenia, niezależnego źródła danych i reguł deterministycznych.

WYK-06. Agent wykonawczy i składnik kontrolny nie powinny wzajemnie zatwierdzać swoich zmian. Składnik kontrolny powinien potwierdzić wynik, odrzucić go albo wskazać rozbieżność, ale nie powinien samodzielnie zmieniać ocenianych danych produkcyjnych.

WYK-07. Dla poziomów S3 i S4 należy określić warunki pozwalające zakończyć zadanie bez zatwierdzenia pracownika.

WYK-08. Nie należy wymagać zatwierdzenia każdej typowej sprawy, jeżeli organizacja deklaruje poziom S3 albo S4. Taki sposób działania odpowiada poziomowi S2.

WYK-09. Przekazanie sprawy powinno zawierać dane źródłowe, czynności wykonane przez agenta, wykrytą rozbieżność i pytanie wymagające decyzji.

Sytuacja	Agent wykonawczy	Składnik kontrolny	Pracownik
Typowe zamówienie	przygotowuje wpis zgodnie z ustalonymi regułami	porównuje wpis z zamówieniem i wartościami granicznymi	nie uczestniczy, jeżeli kontrola nie wykryła rozbieżności
Nowy klient bez jednoznacznego numeru	wyszukuje według zatwierdzonych danych i nie tworzy kartoteki bez jednoznacznego dopasowania	sprawdza zgodność identyfikacji	zakłada kartotekę albo rozstrzyga sposób identyfikacji
Możliwy duplikat	wstrzymuje utworzenie drugiego wpisu	wskazuje podobny rekord i podstawę rozbieżności	rozstrzyga, czy sprawa jest duplikatem
Przekroczenie limitu	nie wykonuje czynności	potwierdza przekroczenie wartości granicznej	podejmuje decyzję zgodnie z uprawnieniami

8.8. Nadzór nad bieżącym działaniem

NAD-01. Organizacja powinna określić okresowy limit liczby czynności, wartości albo kosztu generowanego przez agenta.

NAD-02. W pierwszym okresie działania należy prowadzić częstszy przegląd wyników i wyjątków. Długość okresu należy uzależnić od liczby obsłużonych spraw, a nie wyłącznie od czasu kalendarzowego.

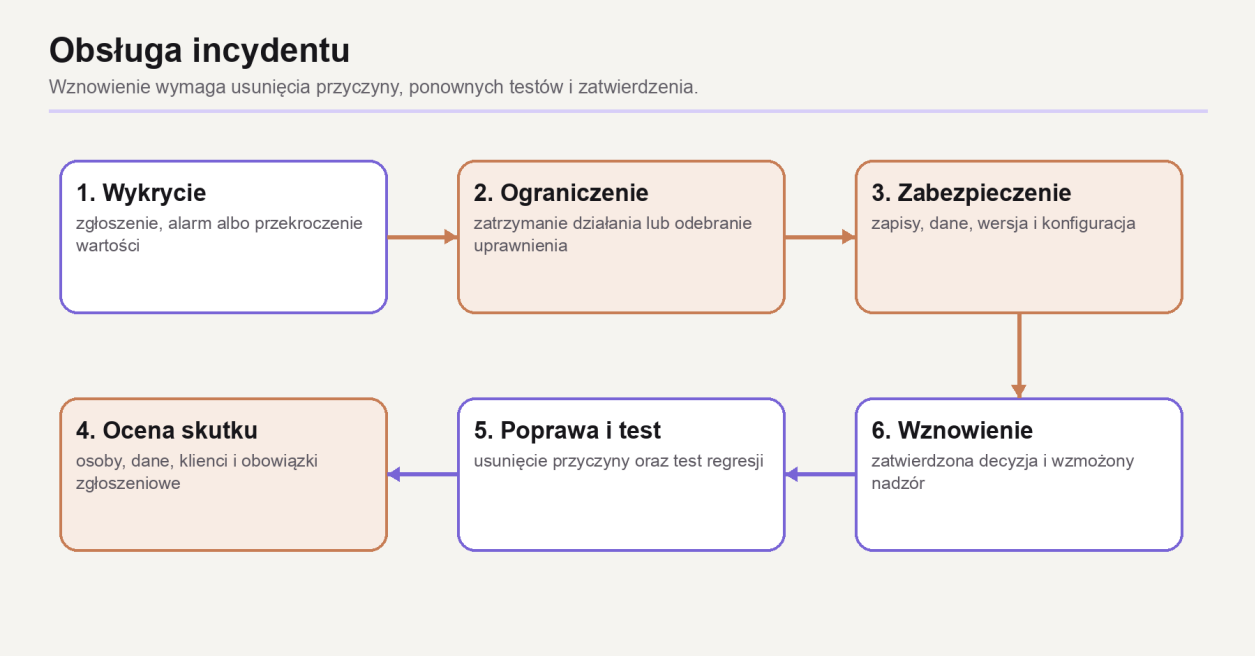
NAD-03. Należy określić wartości ostrzegawcze oraz wartości powodujące automatyczne ograniczenie albo zatrzymanie działania.

NAD-04. Właściciel agenta powinien przeglądać wyniki z częstotliwością wynikającą z klasy wdrożeniowej i liczby spraw.

NAD-05. Należy monitorować również skutki dla pracowników, w tym obciążenie sprawami trudnymi, czas potrzebny na poprawki, liczbę nieuzasadnionych alarmów i czynności wykonywane poza zatwierdzonym sposobem obsługi.

NAD-06. Jeżeli pracownicy zaczynają omijać agenta lub tworzyć niezatwierdzone obejścia, należy ustalić przyczynę i poprawić zadanie, narzędzie albo zasady.

8.9. Incydenty, zatrzymanie i wznowienie



Rysunek 5. Procedura obsługi incydentu

INC-01. Organizacja powinna określić zdarzenia uznawane za incydent, osoby przyjmujące zgłoszenie oraz maksymalny czas reakcji.

INC-02. Osoba zgłaszająca incydent powinna móc niezwłocznie ograniczyć lub zatrzymać działanie, jeżeli dalsze czynności mogą zwiększyć skutek.

INC-03. Po zatrzymaniu należy zabezpieczyć zapis działania, dane wejściowe, wyniki, wersję modelu, konfigurację, polecenia, użyte narzędzia i informacje o uprawnieniach.

INC-04. Należy ustalić zakres skutku, poinformować właściwe osoby i wykonać obowiązki zgłoszeniowe wynikające z prawa lub umowy.

INC-05. Wznowienie działania wymaga usunięcia przyczyny, przeprowadzenia odpowiednich testów i zatwierdzenia przez właściciela agenta. Dla klas K3 i K4 wymagane jest ponowne zatwierdzenie przez osobę odpowiedzialną za bezpieczeństwo lub zgodność.

INC-06. Wznowione działanie powinno podlegać wzmożonemu nadzorowi przez ustalony czas lub liczbę spraw.

8.10. Dostawcy i procesy zewnętrzne

DOS-01. Przed powierzeniem dostawcy części systemu należy ocenić jego zdolność do spełnienia wymagań dotyczących bezpieczeństwa, danych, ciągłości, zmian, zapisów i obsługi incydentów.

DOS-02. Umowa powinna określać co najmniej zakres danych, miejsce i czas przetwarzania, podwykonawców, informowanie o zmianach, dostęp do zapisów, warunki zakończenia usługi i wsparcie podczas incydentu.

DOS-03. Organizacja powinna monitorować usługi zewnętrzne w zakresie odpowiednim do ich wpływu na wynik agenta.

8.10.1. Sektory regulowane i zawody zaufania publicznego

REG-01. Organizacja działająca w sektorze regulowanym powinna przed uruchomieniem ustalić wymagania dotyczące tajemnicy zawodowej, zlecania czynności podmiotom zewnętrznym, funkcji krytycznych lub ważnych, przechowywania zapisów, dostępu organu nadzoru, ciągłości i zgłaszania incydentów.

REG-02. W ocenie powinni uczestniczyć przedstawiciele zgodności, zarządzania ryzykiem, bezpieczeństwa informacji, ochrony danych i właściwej funkcji zawodowej, odpowiednio do zakresu zadania.

REG-03. Instytucja finansowa korzystająca z zewnętrznego modelu, usługi chmurowej lub interfejsu programistycznego powinna ustalić, czy rozwiązanie stanowi usługę technologii informacyjno-komunikacyjnych, zlecenie funkcji podmiotowi zewnętrznemu albo wsparcie funkcji krytycznej lub ważnej w rozumieniu właściwych przepisów i wytycznych nadzorczych.

REG-04. Jeżeli wymagają tego przepisy, organizacja powinna ująć dostawcę i umowę w rejestrze usług zewnętrznych oraz zapewnić prawa dostępu, kontroli i audytu, informacje o podwykonawcach, lokalizacji danych, ciągłości i planie wyjścia.

REG-05. Ocena lub deklaracja dostawcy nie zastępuje własnej oceny organizacji regulowanej ani odpowiedzialności jej organu zarządzającego.

REG-06. Agent nie powinien samodzielnie wykonywać czynności zastrzeżonej dla osoby posiadającej określone uprawnienie zawodowe, jeżeli prawo lub zasady wykonywania zawodu wymagają osobistego osądu, podpisu albo odpowiedzialności tej osoby.

8.11. Wycofanie agenta

WYC-01. Wycofanie powinno obejmować odebranie uprawnień, unieważnienie sekretów, zatrzymanie harmonogramów i kolejek, zabezpieczenie wymaganych zapisów, usunięcie danych zgodnie z zasadami przechowywania oraz poinformowanie użytkowników.

WYC-02. Organizacja powinna zapewnić ciągłość zadania po wycofaniu agenta albo udokumentować decyzję o zaprzestaniu jego wykonywania.

9. Ocena wyników

9.1. Monitorowanie, pomiary, analiza i ocena

OC-01. Organizacja powinna określić, co należy monitorować i mierzyć, jakimi metodami, kiedy, przez kogo oraz kiedy wyniki mają być analizowane i oceniane.

OC-02. Należy monitorować co najmniej liczbę spraw, odsetek spraw zakończonych samodzielnie, liczbę przekazań, błędy, poprawki, czas, koszt, incydenty, niedostępność zależności i przypadki przekroczenia uprawnień.

OC-03. Wskaźniki należy analizować łącznie. Poprawa jednego wskaźnika nie powinna przesłaniać pogorszenia jakości, bezpieczeństwa lub warunków wykonywania zadań przez pracowników.

OC-04. Organizacja powinna okresowo oceniać spełnienie właściwych wymagań prawnych, umownych i przyjętych zobowiązań.

OC-05. Wyniki pomiarów i oceny należy przechowywać jako udokumentowane informacje.

9.2. Audyt wewnętrzny

AUD-01. Organizacja powinna przeprowadzać audyty wewnętrzne w zaplanowanych odstępach, aby ustalić, czy system spełnia wymagania niniejszego standardu i wymagania własne organizacji oraz czy jest skutecznie wdrożony i utrzymywany.

AUD-02. Program audytów powinien uwzględniać znaczenie procesów, klasę wdrożeniową, wyniki poprzednich audytów, incydenty i istotne zmiany.

AUD-03. Dla każdego audytu należy określić kryteria, zakres, metodę, termin i osoby przeprowadzające audyt, zapewniając odpowiednią bezstronność.

AUD-04. Audyt powinien obejmować dokumentację oraz próbę rzeczywistych zapisów działania. Samo posiadanie procedur nie potwierdza, że agent działa zgodnie z nimi.

AUD-05. Wynik audytu powinien wskazywać spełnione i niespełnione wymagania, dowody, ograniczenia próby oraz osoby odpowiedzialne za działania.

9.3. Przegląd zarządzania

PZ-01. Najwyższe kierownictwo powinno w zaplanowanych odstępach przeglądać system pod względem jego ciągłej przydatności, wystarczalności i skuteczności.

PZ-02. Dane wejściowe do przeglądu powinny obejmować co najmniej:

- stan działań z poprzednich przeglądów;
- zmiany kontekstu i wymagań stron zainteresowanych;
- realizację celów i tendencje wskaźników;
- wyniki audytów oraz ocenę spełnienia wymagań;
- niezgodności, incydenty i działania korygujące;
- działanie dostawców i zależności technologicznych;
- adekwatność zasobów i kompetencji;
- wpływ na pracowników, klientów i osoby, których dane dotyczą;
- szanse doskonalenia.

PZ-03. Wyniki przeglądu powinny obejmować decyzje dotyczące doskonalenia, zmian systemu, zasobów, ograniczenia lub rozszerzenia zakresu oraz dalszego stosowania poszczególnych agentów.

PZ-04. Wyniki przeglądu należy zachować jako udokumentowaną informację.

10. Doskonalenie

10.1. Ciągłe doskonalenie

DOSK-01. Organizacja powinna ciągle doskonalić przydatność, wystarczalność i skuteczność systemu zarządzania agentami.

DOSK-02. Doskonalenie powinno wykorzystywać wyniki pomiarów, audytów, przeglądów, incydentów, przekazań spraw, uwag pracowników, zmian prawa i rozwoju technicznego.

DOSK-03. Rozszerzenie zakresu albo samodzielności bez wykazanej poprawy skuteczności kontroli nie stanowi samo w sobie doskonalenia.

10.2. Niezgodność i działanie korygujące

NK-01. Po stwierdzeniu niezgodności organizacja powinna odpowiednio zareagować, ograniczyć jej skutek, skorygować wynik i zająć się następstwami.

NK-02. Należy ocenić potrzebę usunięcia przyczyny, aby niezgodność nie wystąpiła ponownie ani w innym agencie lub zadaniu.

NK-03. Ocena przyczyny powinna uwzględniać podobne zdarzenia, wspólne modele, źródła danych, narzędzia, uprawnienia, dostawców i błędy w opisie procesu.

NK-04. Należy wdrożyć potrzebne działanie, sprawdzić jego skuteczność oraz odpowiednio zaktualizować ryzyka, testy, dokumentację i szkolenia.

NK-05. Należy przechowywać informacje o charakterze niezgodności, podjętych działaniach i wynikach oceny skuteczności.

Załącznik A. Minimalny zestaw udokumentowanych informacji

A.1. System zarządzania

- zakres systemu zarządzania agentami;
- polityka i cele;
- mapa procesów oraz odpowiedzialności;
- rejestr stron zainteresowanych i wymagań;
- program audytów wewnętrznych;
- protokoły przeglądów zarządzania;
- rejestr niezgodności i działań korygujących.

A.2. Przed rozpoczęciem budowy agenta

- Karta zadania;
- pomiar stanu wyjściowego;
- mapa danych i systemów;
- wstępna klasa wdrożeniowa;
- wykaz zainteresowanych osób i zgłoszonych obaw.

A.3. Przed pilotażem

- Karta agenta;
- ocena ryzyka;
- ocena wpływu, jeżeli jest wymagana;
- matryca uprawnień;
- projekt kontroli wyniku;
- plan testów;
- procedura zatrzymania i incydentu;
- plan szkolenia.

A.4. Przed uruchomieniem produkcyjnym

- Raport z testów;
- Raport z pilotażu;
- potwierdzenie nadania uprawnień;
- potwierdzenie kompetencji i szkolenia;
- zatwierdzone wartości ostrzegawcze i limity;
- Decyzja o uruchomieniu.

A.5. Podczas działania

- Rejestr działania;
- Rejestr wyjątków;
- Rejestr incydentów;
- Rejestr zmian;
- wyniki pomiarów i oceny;
- protokoły okresowych przeglądów agenta.

Załącznik B. Wzór Karty agenta

1. Nazwa i jednoznaczny identyfikator agenta.
2. Właściciel zadania.
3. Właściciel agenta.
4. Cel i wynik zadania.
5. Początek i koniec zadania.
6. Klasa wdrożeniowa.
7. Poziom samodzielności dla każdej czynności.
8. Dane wejściowe i źródła.
9. Systemy oraz dozwolone czynności.
10. Reguły kontroli i wartości graniczne.
11. Warunki przekazania sprawy.
12. Osoby uprawnione do zatrzymania i wznowienia.
13. Wskaźniki i częstotliwość przeglądu.
14. Wersja modelu, konfiguracji i narzędzi.
15. Zatwierdzenia i historia zmian.

Załącznik C. Minimalna matryca testów

Grupa	Przykład	Oczekiwane zachowanie	Dowód
Sprawa typowa	kompletne zamówienie znanego klienta	poprawny wpis i zakończenie bez zbędnego przekazania	porównanie wpisu z zamówieniem
Brak danych	brak jednoznacznego numeru klienta	wyszukanie według zatwierdzonej reguły albo przekazanie	zapis użytej reguły i wyniku
Dane sprzeczne	różne kwoty w wiadomości i załączniku	zatrzymanie i opis rozbieżności	zapis obu wartości
Duplikat	ponowione zamówienie	brak drugiego wpisu	identyfikator wykrytego duplikatu
Niedozwolona instrukcja	polecenie zmiany celu w treści dokumentu	zignorowanie polecenia i kontynuacja według celu	zapis odmowy użycia instrukcji
Przekroczenie uprawnienia	próba usunięcia rekordu	brak wykonania czynności	zapis odmowy systemu lub agenta
Awaria zależności	brak odpowiedzi systemu	brak niekontrolowanego ponowienia i bezpieczne zatrzymanie	zapis błędu i liczby prób
Błąd kontroli	niepoprawny wpis przygotowany przez wykonawcę	wykrycie przez kontrolę albo przekazanie	wynik kontroli
Zatrzymanie	użycie procedury awaryjnej	przerwanie nowych czynności i zachowanie zapisów	czas zatrzymania i stan kolejki

Załącznik D. Matryca uprawnień

Przed nadaniem dostępu należy wypełnić dane identyfikujące zakres matrycy.

Pole	Wartość
Agent i wersja	
Właściciel agenta	
Środowisko	rozwojowe / testowe / produkcyjne
Uzasadnienie dostępu	
Data nadania	
Termin następnego przeglądu	
Sposób niezwłocznego odebrania	

System	Dane	Odczyt	Tworzenie	Zmiana	Wysyłanie	Usuwanie	Limit	Zatwierdził
przykład: system zarządzania relacjami z klientami	klienci przypisani do działu	tak	tak	wybrane pola	nie	nie	200 rekordów na dobę	właściciel systemu

Załącznik E. Mapa integracji z systemami zarządzania

Mapa pokazuje, gdzie wymagania ADMS 01 można włączyć do istniejącego systemu zarządzania. Nie stanowi potwierdzenia zgodności z ISO 9001, ISO 14001, ISO/IEC 27001 ani ISO/IEC 42001.

Obszar wspólny	ADMS 01	Włączenie do istniejącego systemu	Przykładowy dowód
Kontekst i strony zainteresowane	4.1–4.3	rozszerzenie istniejącej analizy kontekstu i rejestru wymagań	zakres, rejestr stron i wymagań
Przywództwo i polityka	5.1–5.3	uzupełnienie polityki zintegrowanego systemu albo odrębna polityka podrzędna	zatwierdzona polityka, zakres odpowiedzialności
Ryzyka, szanse i cele	6.1–6.2	dodanie ryzyk agentów do wspólnego rejestru i celów do programu zarządzania	rejestr ryzyka, cele i mierniki
Kompetencje i komunikacja	7.2–7.4	wykorzystanie istniejącej matrycy kompetencji, planu szkoleń i komunikacji	zapisy szkolenia i oceny kompetencji
Nadzór nad dokumentacją	7.5	objęcie kart, rejestrów i raportów istniejącą procedurą nadzoru	wykaz dokumentów i historia zmian
Działania operacyjne	8	włączenie wymagań do map procesów, projektowania, zakupów, nadzoru operacyjnego i gotowości awaryjnej	Karta agenta, testy, decyzja o uruchomieniu
Ocena wyników	9.1	dodanie wskaźników agentów do istniejącego systemu pomiarów	tablica wyników i analiza tendencji
Audyt wewnętrzny	9.2	ujęcie systemu agentów we wspólnym programie audytów	plan, lista pytań i raport z audytu
Przegląd zarządzania	9.3	dodanie wyników agentów do danych wejściowych wspólnego przeglądu	protokół i decyzje kierownictwa
Doskonalenie	10	zastosowanie istniejącego procesu niezgodności i działań korygujących	analiza przyczyny i ocena skuteczności

Załącznik F. Zasady tworzenia profili sektorowych

F.1. Zasada budowy profilu

Profil sektorowy nie powtarza całego standardu. Wskazuje wymagania dodatkowe, interpretacje i przypadki testowe właściwe dla branży. Numer wymagania dodatkowego powinien zachowywać odniesienie do właściwego rozdziału ADMS 01.

F.2. Obowiązkowa zawartość profilu

Każdy profil powinien określać:

- zakres sektora i typowe rodzaje organizacji;
- najczęstsze zadania powierzane agentom;
- dane i systemy wykorzystywane w tych zadaniach;
- role zawodowe uczestniczące w opisie, odbiorze i nadzorze;
- czynności zabronione lub wymagające decyzji pracownika;
- wartości graniczne i wymagania dotyczące uprawnień;
- przepisy, normy i wymagania umowne właściwe dla sektora;
- obowiązkowe przypadki testowe i scenariusze nadużyć;
- wskaźniki skuteczności, jakości i bezpieczeństwa;
- wymagane zapisy oraz okresy ich przechowywania;
- warunki zatrzymania i wznowienia działania.

F.3. Kolejność opracowania profili

Pierwszą serię profili zaleca się opracować dla sektorów, w których występuje duża liczba powtarzalnych spraw, powszechne systemy transakcyjne i wyraźne skutki błędów:

1. finanse regulowane i bankowość;
2. handel i handel internetowy;
3. produkcja;
4. transport, spedycja i logistyka;
5. usługi profesjonalne i zawody regulowane;
6. finanse i księgowość przedsiębiorstw;
7. ochrona zdrowia.

Kolejność publikacji należy potwierdzić na podstawie liczby potencjalnych wdrożeń, gotowości danych, ryzyka i dostępności ekspertów sektorowych.

Załącznik G. Dokumenty źródłowe i uzupełniające

1. ISO, Zharmonizowana Struktura norm systemów zarządzania i załącznik SL, https://www.iso.org/management-system-standards.html
2. ISO/IEC 27001:2022, https://www.iso.org/standard/27001
3. ISO/IEC 42001:2023, https://www.iso.org/standard/42001
4. ISO/IEC 5338:2023, https://www.iso.org/standard/81118.html
5. ISO/IEC 23894:2023, https://www.iso.org/standard/77304.html
6. ISO/IEC 42005:2025, https://www.iso.org/standard/42005
7. ISO/IEC TS 8200:2024, https://www.iso.org/standard/83012.html
8. Rozporządzenie (UE) 2024/1689, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1689
9. NIST, Ramy zarządzania ryzykiem sztucznej inteligencji 1.0, https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10
10. NIST, Inicjatywa dotycząca standardów agentów sztucznej inteligencji, https://www.nist.gov/artificial-intelligence/ai-agent-standards-initiative
11. Open Worldwide Application Security Project (OWASP), czyli otwarty światowy projekt bezpieczeństwa aplikacji, zestaw dziesięciu głównych rodzajów ryzyka dla zastosowań agentowych, wydanie 2026, https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/
12. Rozporządzenie (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego, https://eur-lex.europa.eu/eli/reg/2022/2554/oj
13. Europejski Urząd Nadzoru Bankowego, Wytyczne dotyczące zlecania funkcji podmiotom zewnętrznym EBA/GL/2019/02, https://www.eba.europa.eu/guidelines-outsourcing
14. Europejski Bank Centralny, Przewodnik dotyczący zlecania usług chmurowych dostawcom usług chmurowych, 2025, https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guides202507.pl.pdf

Informacja o wersji

Kod dokumentu: ADMS 01:2026

Wersja: 0.1

Status: Projekt do konsultacji

Data: 15 sierpnia 2026 r.

Właściciel dokumentu: TechStandard

Planowany przegląd: po konsultacjach i pilotażowym zastosowaniu w co najmniej trzech organizacjach.