



Sudhara International

+48 32 724 35 86



info@sudharapolska.com

www.sudharapolska.com

SYSTEM ZARZĄDZANIA SZTUCZNĄ INTELIGENCJĄ AI. WYMAGANIA NORMY ISO 42001:2026 PROGRAM SZKOLENIA

Cel szkolenia

Celem szkolenia jest kompleksowe przygotowanie uczestników do zrozumienia, interpretowania oraz praktycznego stosowania wymagań normy ISO/IEC 42001 w organizacji wykorzystującej lub rozwijającej systemy sztucznej inteligencji. Szkolenie porządkuje wymagania dotyczące budowy i utrzymania AIMS, pokazuje zależności pomiędzy łańcem organizacyjnym, ryzykiem, odpowiedzialnością, nadzorem człowieka oraz cyklem życia systemów AI, a także wspiera uczestników w przełożeniu zapisów normy na realia operacyjne, compliance i audytowe przedsiębiorstwa. Istotnym celem jest również przygotowanie organizacji do świadomego wdrożenia wymagań normy, identyfikacji luk oraz budowania spójnego podejścia do bezpiecznego, odpowiedzialnego i zgodnego z wymaganiami regulacyjnymi zarządzania AI.

Program szkolenia:

PRE-TEST

1. Wprowadzenie do ISO/IEC 42001

- Dlaczego powstała norma ISO 42001 – kontekst rozwoju AI i regulacji.
- Zakres i cel normy – do jakich organizacji ma zastosowanie.
- AI jako system socjotechniczny – ryzyka, odpowiedzialność, zaufanie.
- Powiązania z:
 - ISO 9001 (jakość).
 - ISO/IEC 27001 (bezpieczeństwo informacji).
 - ISO/IEC 27701 (ochrona danych).
 - EU AI Act.
- Struktura normy.

2. Kontekst organizacji i zakres AIMS

- Punkt 4 normy:
 - Zrozumienie organizacji i jej kontekstu.
 - Strony zainteresowane i ich wymagania.
- Określenie zakresu systemu AIMS:
 - produkty AI.
 - usługi AI.
 - systemy wspierające decyzje.
- Definicja ról: dostawca AI, użytkownik AI, integrator.



Park Technologiczny Woda Energia Bezpieczeństwo, Żeliwna 38A, 40-599 Katowice



Sudhara International

+48 32 724 35 86



info@sudharapolska.com



www.sudharapolska.com

- **Ćwiczenie:**

- identyfikacja systemów AI w organizacji
- określenie granic AIMS.

3. Przywództwo i odpowiedzialność (Leadership).

- Punkt 5 normy:
 - Zaangażowanie najwyższego kierownictwa.
 - Polityka AI.
 - Role, odpowiedzialności i uprawnienia.
- Odpowiedzialność zarządcza za decyzje podejmowane przez AI.
- Rola etyki, nadzoru człowieka (human oversight).
- Studium przypadku:
 - brak nadzoru nad modelem ML – skutki biznesowe i prawne.

4. Planowanie – ryzyka i cele AI.

- Punkt 6 normy:
 - Identyfikacja ryzyk i szans związanych z AI.
 - Ryzyka:
 - Techniczne.
 - Prawne.
 - Etyczne.
 - Reputacyjne.
 - Ocena wpływu AI (AI Impact Assessment).
- Cele AIMS i plan ich realizacji.
- **Warsztat:**
 - budowa prostej **macierzy ryzyk AI**.
 - przypisanie działań kontrolnych.

5. Zasoby, kompetencje i świadomość

- Punkt 7 normy:
 - Kompetencje zespołów AI.
 - Szkolenia i świadomość pracowników.
 - Komunikacja wewnętrzna i zewnętrzna.
- Zarządzanie wiedzą o systemach AI.
- Dokumentowanie procesów AIMS.
- **Ćwiczenie:**
 - mapa kompetencji dla zespołu AI.

6. Operacyjne zarządzanie systemami AI.

- Punkt 8 normy:
 - Planowanie i sterowanie operacyjne.
 - Cykl życia systemu AI:
 - Projektowanie.
 - Rozwój.
 - Testowanie.
 - Wdrożenie.
 - Eksploatacja.
 - Wycofanie.
- Dane treningowe – jakość, bias, zgodność prawna.
- Zarządzanie zmianą modelu (model drift).
- Podwykonawcy i modele zewnętrzne (third-party AI).





Sudhara International

+48 32 724 35 86



info@sudharapolska.com

www.sudharapolska.com

- **Warsztat:**

- analiza przykładowego procesu wdrażania modelu AI.

7. Monitorowanie, audit i zgodność.

- Punkt 9 normy:
 - Monitorowanie skuteczności AI.
 - KPI dla systemów AI.
 - Audyty wewnętrzne AIMS.
 - Przegląd zarządzania.
- Powiązanie z wymaganiami regulatorów.

- **Ćwiczenie:**

- lista kontrolna audytu ISO 42001.

8. Niezgodności, incydenty i doskonalenie.

- Punkt 10 normy:
 - Reagowanie na incydenty AI.
 - Zarządzanie niezgodnościami.
 - Działania korygujące.
 - Ciągłe doskonalenie AIMS.
- Incydenty:
 - Błędne decyzje AI.
 - Naruszenia praw człowieka.
 - Naruszenia danych.

- **Warsztat:**

- analiza incydentu AI i opracowanie CAPA.

9. Załącznik A normy ISO/IEC 42001 – środki zarządzania AI (Annex A).

- Rola Załącznika A w normie ISO/IEC 42001:
 - Katalog referencyjnych środków zarządzania (controls).
 - Wsparcie realizacji wymagań normy głównej (pkt 4-10).
 - Podejście oparte na ryzyku.
 - Analogia do Załącznika A normy ISO/IEC 27001.
- Struktura Załącznika A:
 - Pogrupowanie środków według obszarów zarządzania AI.
 - Powiązanie środków z cyklem życia systemu AI
 - Relacja Annex A ↔ ryzyka AI.
- Obszary Załącznika A:
 - Zarządzanie polityką i odpowiedzialnością za AI:
 - ustanowienie zasad odpowiedzialnego stosowania AI,
 - przypisanie odpowiedzialności właścicielskiej,
 - nadzór zarządczy nad systemami AI.
 - Zarządzanie ryzykiem AI:
 - identyfikacja i ocena ryzyk AI,
 - monitorowanie ryzyk w czasie,
 - aktualizacja środków kontrolnych.
 - Zarządzanie danymi i modelami AI:
 - jakość i integralność danych,
 - zapobieganie stronniczości (bias),
 - walidacja i testowanie modeli.





Sudhara International

+48 32 724 35 86



info@sudharapolska.com

www.sudharapolska.com

- Nadzór nad cyklem życia systemu AI:
 - projektowanie i rozwój,
 - wdrażanie i eksploatacja,
 - wycofanie i archiwizacja.
- Transparentność i wyjaśnialność AI:
 - dokumentowanie działania systemów AI,
 - informowanie użytkowników o użyciu AI,
 - możliwość wyjaśnienia decyzji algorytmicznych.
- Nadzór człowieka (Human Oversight):
 - mechanizmy ingerencji człowieka,
 - eskalacja decyzji,
 - zapobieganie niekontrolowanej automatyzacji.
- Bezpieczeństwo, odporność i ciągłość działania:
 - odporność modeli na błędy i manipulacje,
 - bezpieczeństwo infrastruktury AI,
 - ciągłość działania systemów AI.
- Zarządzanie podwykonawcami i rozwiązaniami zewnętrznymi:
 - third-party AI,
 - wymagania umowne,
 - ocena ryzyk dostawców.
- Zarządzanie incydentami AI:
 - wykrywanie i zgłaszanie incydentów,
 - analiza przyczyn źródłowych,
 - działania korygujące.
- Dobór i stosowanie środków z Załącznika A:
 - adekwatność do ryzyk AI,
 - uzasadnienie zastosowania lub wyłączenia środka,
 - spójność z celami AIMS.
- Statement of Applicability (SoA):
 - dokumentowanie decyzji dotyczących Annex A,
 - powiązanie ryzyk z kontrolami,
 - wykorzystanie SoA podczas auditów.
- Zastosowanie Załącznika A w praktyce:
 - wsparcie audytów wewnętrznych,
 - przygotowanie do audytu certyfikującego,
 - zgodność z EU AI Act.
- **Warsztat praktyczny:**
 - mapowanie systemu AI do wybranych środków Załącznika A,
 - ocena skuteczności zastosowanych kontroli,
 - identyfikacja luk i działań doskonalących.

POST-TEST

Grupa odbiorcza

Szkolenie jest skierowane do osób odpowiedzialnych za projektowanie, wdrażanie, nadzorowanie, utrzymanie oraz auditowanie systemów AI w organizacji. W szczególności rekomendowane jest dla:

- Kadry managerskiej i właścicieli procesów odpowiedzialnych za nadzór nad wykorzystaniem AI.



Park Technologiczny Woda Energia Bezpieczeństwo, Żeliwna 38A, 40-599 Katowice



Sudhara International

+48 32 724 35 86



info@sudharapolska.com

www.sudharapolska.com

- Specjalistów i inżynierów z obszarów IT, cyberbezpieczeństwa, danych, rozwoju systemów i transformacji cyfrowej.
- Osób odpowiedzialnych za compliance, zarządzanie ryzykiem, ochronę danych osobowych oraz governance.
- Pełnomocników systemów zarządzania oraz osób wdrażających i utrzymujących SZAI/AIMS.
- Auditorów wewnętrznych oraz osób przygotowujących organizację do audytów klientów, wewnętrznych i certyfikacyjnych.
- Wszystkich interesariuszy, którzy chcą zrozumieć wymagania ISO/IEC 42001 i ich praktyczne zastosowanie w działalności operacyjnej.



Korzyści po szkoleniu

- Rozumieją strukturę i wymagania normy ISO/IEC 42001 oraz potrafią odnieść je do realiów swojej organizacji,
- Potrafią identyfikować systemy AI, określać granice AIMS oraz przypisywać role i odpowiedzialności związane z zarządzaniem AI.
- Zdobywają praktyczne podejście do identyfikacji ryzyk technicznych, prawnych, etycznych i reputacyjnych związanych z AI.
- Potrafią powiązać wymagania normy z cyklem życia systemu AI: od projektowania i wdrożenia po monitorowanie, nadzór i doskonalenie.
- Lepiej przygotowują organizację do audytów wewnętrznych, działań zgodnościowych oraz wdrażania środków z Załącznika A.
- Zyskują większą pewność w zakresie interpretacji wymagań dotyczących transparentności, nadzoru człowieka, incydentów AI, dostawców zewnętrznych i dokumentowania decyzji.
- Otrzymują praktyczne podstawy do udziału we wdrożeniu, utrzymaniu i doskonaleniu systemu zarządzania sztuczną inteligencją.



Metodyka szkolenia

Szkolenie prowadzone jest w formule praktyczno-warsztatowej, z naciskiem na użyteczność biznesową i możliwość bezpośredniego zastosowania wymagań normy w organizacji. Metodyka obejmuje:

- eksperckie omówienie wymagań normy w powiązaniu z praktyką organizacyjną,
- warsztaty umożliwiające przećwiczenie identyfikacji systemów AI, granic AIMS, ryzyk i działań kontrolnych,
- analizę studiów przypadków pokazujących konsekwencje braku nadzoru, nieprawidłowego wdrożenia lub niewłaściwego zarządzania AI,
- pracę na przykładach dokumentów, list kontrolnych i podejściu audytowym,
- dyskusje moderowane, które pozwalają odnieść wymagania normy do specyfiki branży i dojrzałości organizacji,
- elementy weryfikacji wiedzy przed i po szkoleniu wspierające ocenę przyrostu kompetencji uczestników.

To kompleksowe szkolenie pozwoli uczestnikom skutecznie stosować wymagania ISO 42001:2026 w swojej codziennej pracy.

Czas trwania szkolenia – 2 dni



Park Technologiczny Woda Energia Bezpieczeństwo, Żeliwna 38A, 40-599 Katowice