

ISO/IEC 42001:2023

A Mesterséges Intelligencia Menedzsment Rendszerek Új Szabványja

1134 Budapest, Váci út 49, 6.em.

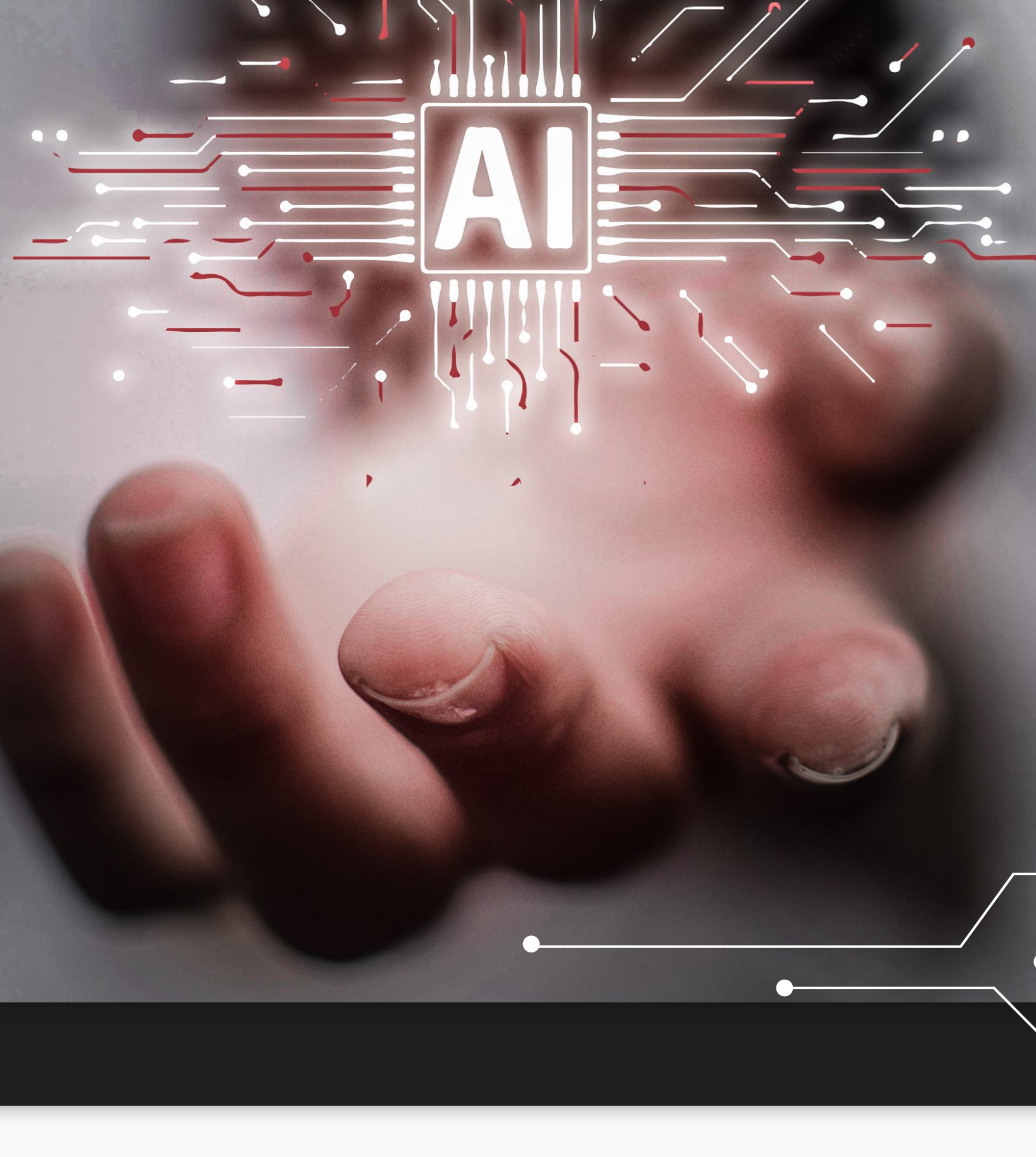
+36 1 278 2295

info@tamcert.hu

www.tamcert.hu



Az ISO/IEC 42001 szabványt 2023. decemberében tették közzé az AI üzleti célú növekedésének kezelésére, és olyan irányelveket, szabványokat, valamint követelményeket tartalmaz, amelyek az AI technológiák fejlesztésére, alkalmazására és szabályozására vonatkoznak.



Az **AI standardok célja**, hogy biztosítsák az AI rendszerek megbízhatóságát, biztonságát, etikus használatát és átláthatóságát, továbbá az AI standardok meghatározásában nemzetközi szervezetek, kormányok, és szakmai testületek is részt vettek annak érdekében, hogy globálisan elfogadott irányelvek és szabványok születhessenek.

Az AI standardok például előírnak **etikai irányelveket**, miszerint az AI fejlesztésében és használatában tiszteletben kell tartani az emberi jogokat, biztosítani kell az igazságosságot, átláthatóságot, és az adatvédelmet. Tartalmaznak továbbá **technikai előírásokat** is, mely követelmények az AI modellek pontosságára, robusztusságára és megbízhatóságára vonatkoznak. Az **adatkezelési standardok** alapján az adatok gyűjtése, tárolása és feldolgozása során kell betartani a titoktartási és biztonsági irányelveket. A **tesztelési és validálási eljárások** biztosítják, hogy az AI rendszerek helyesen működjenek a tervezett környezetben, és képesek legyenek kezelni a váratlan helyzeteket is.

Az AI rendszereknek továbbá meg kell felelniük a **vonatkozó jogszabályoknak** és előírásoknak, mint például:

- az **EU AI Act** (az első átfogó Európai Uniói AI törvény, mely eltérő szabványokat fogalmaz meg a különböző AI kockázati szintekhez)
- a **GDPR** (az Európai Unió adatvédelmi előírásokat tartalmazza)
- a **NIS2** (az Európai Unió kibebiztonsági előírásokat tartalmazza)



Az ISO/IEC 42001:2023 szabvány támogatja a NIS2 irányelvvel való összehangolást, amely a hálózati és információs rendszerek biztonságának megerősítését célozza meg, különös tekintettel az AI-alapú rendszerek sérülékenységeire. Ez különösen fontos a kritikus infrastruktúrák és szolgáltatások esetében, amelyek AI-rendszereket használnak.

A GDPR tekintetében az ISO/IEC 42001:2023 segíthet az AI rendszerek adatvédelmi megfelelőségének biztosításában, mivel előírja az AI átláthatóságát és az adatkezelési folyamatok dokumentálását. Ez lehetővé teszi a felhasználók adatainak biztonságos kezelését, a jogszertű adatfeldolgozást, és az egyének jogainak tiszteletben tartását.

Az NCSS (Nemzeti Kiberbiztonsági Stratégia) vonatkozásában az ISO/IEC 42001:2023 alkalmazása elősegíti a nemzeti és ipari kiberbiztonsági célok elérését, különösen az AI-rendszerek biztonságának és megbízhatóságának növelésével.

Az ISO/IEC 42001:2023 szabványt a fentiek alapján tehát mindazon szervezetek számára fejlesztették ki, amelyek AI-alapú szolgáltatásokat használnak, nyújtanak vagy fejlesztenek, akár a pénzügyi szektorban, akár az egészségügyben, akár a gyártásban, avagy minden olyan ágazatban, ahol AI-t használnak akár a döntéshozatalban, vagy az automatizálásban.

Az ISO/IEC 42001:2023 szabvány segít kezelni az AI-kompatibilis rendszerek fő adatvédelmi és biztonsági kockázatait iránymutatásokat adva a mesterséges intelligencia rendszerek tervezéséhez, bevezetéséhez, működtetéséhez és fenntartásához. A szabvány ennek megfelelően különös hangsúlyt fektet a biztonságra és az átláthatóságra.

Kinek van szüksége az ISO/IEC 42001:2023 szabvány által biztosított megfelelőségre?

Az AI-technológián alapuló szolgáltatásokat használó, fejlesztő vagy nyújtó vállalatok számára elengedhetetlen az ISO/IEC 42001:2023 szabványnak való megfelelés, de minden vállalat profitálhat a szabványban leírt mesterséges intelligencia-kezelési rendszer bevezetéséből, hiszen az AI számos különböző iparágban képes javítani az üzleti folyamatokat.

Az ISO/IEC 42001:2023 szabvány olyan AI rendszer megfelelőséget biztosít a szervezet számára, amely segít kiszűrni a jelentős potenciális kockázatokat, támogatja az AI használatát és innovációját, miközben biztosítja a biztonságos és felelősségteljes használatot abszolút versenylőnyt biztosítva ezzel a gyorsan változó technológiai környezetben.

Az ISO/IEC 42001:2023 szabvány kulcsfontosságú komponensei

1. A menedzsment rendszer

A szabvány részletes követelményeket határoz meg a mesterséges intelligencia rendszerek menedzseléséhez, beleértve a folyamatok dokumentálását, a kockázatterkékelést, és a folyamatos fejlesztést.

2. Az etikai irányelvek

Az ISO/IEC 42001:2023 hangsúlyozza az AI rendszerek etikus működésének biztosítását, beleértve a diszkriminációmentességet, az átláthatóságot, és a felelősségvállalást.

3. Az audit és megfelelés

A szabvány meghatározza az auditálás és a megfelelés ellenőrzésének módszereit, amelyek segítenek biztosítani, hogy a szervezetek betartsák az előírásokat és folyamatosan megfeleljenek a legújabb követelményeknek.

Kihívások és megoldások a szervezetek számára

Adatszívárgás esete:

A szervezet alkalmazottai érzékeny információkat vihetnek be az AI-kompatibilis megoldásokba, vagy egy termék mesterséges intelligencia segítségével elemzi a már rendelkezésre álló adatokat. Ezek a rendszerek ezeket az információkat képzési célokra is felhasználhatják, ami azt eredményezheti, hogy más felhasználók számára is hozzáférhetővé válnak. Tekintettel arra, hogy az AI-rendszerek nagy mennyiségű adatot kezelnek, ez különleges adatvédelmi és biztonsági kihívásokat jelent. A szabvány előírja az adatkezelési gyakorlatok dokumentálását, a hozzáférés-szabályozás és titkosítási technikák alkalmazását.

Téves diagnosztikák:

Az AI-rendszereket olyan belső modell felépítésére képezték ki, amely lehetővé teszi számukra az adatok osztályozását, döntések meghozatalát vagy kérdések megválaszolását. Ez azonban nem jelenti azt, hogy az AI-rendszer mindig helyes lesz. A mesterséges intelligencia rendszer helytelen válasza azt eredményezheti, hogy egy vállalkozás rossz üzleti döntéseket hoz, vagy elmulasztja egy olyan kibertámadást, amellyel kapcsolatban az AI-re támaszkodott, hogy az észlelje és blokkolja azt. A transzparencia és a felelősség elengedhetetlen, a szabvány segít kialakítani azokat az irányelveket és folyamatokat, amelyek az AI rendszerek működésének átláthatóságának biztosításához, valamint a felelősségi lánc tisztázásához szükségesek.

Szabályozási megfelelés:

A vállalatokra különféle adatvédelmi törvények vonatkoznak, amelyek korlátozzák az ügyfelek személyes adatainak gyűjtését és felhasználását. Ezeknek az adatoknak a mesterséges intelligencia rendszerekben való felhasználása vagy bizonyos üzleti döntések meghozatalához az AI használata sértheti a szabályozási követelményeket. Az ISO/IEC 42001:2023 szabvány gyakorlati útmutatást ad arra vonatkozóan, hogy a szervezetek hogyan tudják hatékonyan kezelni ezeket a kockázatokat.

Az ISO/IEC 42001:2023 tanúsítás előnyei

Az ISO/IEC 42001:2023 tanúsítással cégszerezheti az irányítást a mesterséges intelligencia használata felett, fokozva a vállalati kibebiztonságot és biztosítva a technológia felelősségteljes használatát.

Az ISO/IEC 42001:2023 szabvány alapján, a megfelelési tanúsítási eljárás során feltárásra kerülnek az AI rendszerek, így ezen ismeretek birtokában a szervezet

- meghatározhat irányelveket és biztonsági ellenőrzéseket az adatszívárgás elleni védelem érdekében,
- mélyreható védelmet nyújthat meg az AI hibák kockázatának kezelése érdekében,
- biztosíthatja, hogy az AI használat minden esetben megfeleljen a vonatkozó előírásoknak,
- az AI-t a saját üzleti céljaihoz igazíthatja.

További előnyök

a. Az emberek többsége jobban aggódik az AI használat miatt, mint izgatott lenne felőle, az ISO/IEC 42001:2023-nak való megfeleléssel javíthatja a cége/márkaja imázsát azáltal, hogy bizonyítja a cég elkötelezettségét a felelősségteljes AI fejlesztések iránt.

b. Az ISO/IEC 42001:2023 segít a mesterséges intelligencia kockázatainak kezelésében azáltal, hogy az AI használatára vonatkozóan teljes rálátást és ellenőrzést biztosít a szervezet számára.

c. Lehetőséget biztosít az AI általi termékfejlesztésre, vagy az AI által továbbfejlesztett termékek integrációjára.

d. Az AI számos iparágban képes átalakítani a vállalkozásokat és növelni azok termelékenységét, versenylőnyt biztosítva ezzel a gyorsan változó technológiai környezetben.

e. Az ISO/IEC 42001:2023 támogatja az AI használatát és innovációját, miközben biztosítja a biztonságos és etikus használatot.

f. Az ISO/IEC 42001:2023 segít abban, hogy a mesterséges intelligencia szabályozása világszerte harmonizálásra kerüljön, megkönnyítve ezzel a nemzetközi együttműködést és az innovációt.

g. A gyorsan változó technológiai környezetben a szervezeteknek folyamatosan frissíteniük kell az AI rendszereiket és a kapcsolódó szabályozási megfelelést. Az ISO/IEC 42001:2023 biztosítja az ehhez szükséges keretrendszert.

Kapcsolódás más szabványokhoz és a jövőbeli kilátások

Az ISO/IEC 42001:2023 jól integrálható más ipari szabványokkal, mint például az ISO/IEC 9001 a minőségirányítás, az ISO/IEC 27001 az információbiztonság vagy az ISO/IEC 27701 az adatvédelem terén, lehetővé téve egy átfogó menedzsment rendszer kialakítását.

Ahogy a kifejezetten ajánlott azon szervezetek számára, amelyek mesterséges intelligenciát használó termékeket vagy szolgáltatásokat használnak, fejlesztenek vagy nyújtanak.

A vállalatok világszerte törekednek az ISO/IEC 27001 megfelelésre annak bizonyítására, hogy megvédik ügyfeleik adatait és vállalati rendszereit a potenciális kiberfenyegetésekkel szemben.

Az ISO/IEC 42001 és 27001 végrehajtása során a szervezeteknek figyelembe venniük a kettő közötti átfedéseket, és integrált megközelítést kell kidolgozniuk mind az információbiztonság, mind az AI-kezelés terén. Például az ISO/IEC 27001 szabványnak való megfelelés kockázatelemzésében kiemelt helyen kell szerepelnie a használt mesterséges intelligencia-kompatibilis rendszerek, azok alkalmazásai és a lehetséges kapcsolódó kockázatok teljes jegyzékének.

Az ISO/IEC 42001:2023 jövőbeli változatai várhatóan kiterjednek majd a mesterséges intelligencia új alkalmazásaihoz, mint például az autonóm rendszerek, a mélytanulás, vagy a kvantum számítástechnika.

Mennyi ideig tart az ISO/IEC 42001:2023 tanúsítás?

Az ISO/IEC 42001:2023 tanúsítási folyamat időtartama kis- és középvállalkozások esetében 6-10 hónapig terjedhet, nagyobb szervezetek esetében ez hosszabb is lehet. Néhány tényező, amely befolyásolja a tanúsítási folyamat időtartamát:

- A szervezet mérete és összetettsége
- Az iparág
- A meglévő AI használat

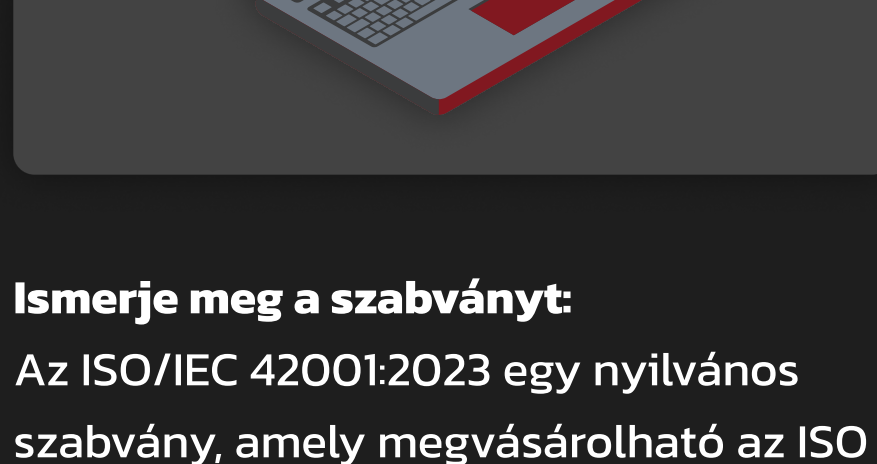
Mivel ennek a folyamatnak a többsége a szervezet felelőssége, a megvalósításra szükséges idő attól függ, hogy a szervezet mennyi ideig tart a céljainak megtervezése, azok megvalósítása és dokumentálása. Ha ez megtörtén, maga az audit néhány hetet vesz igénybe.

Mennyibe kerül az ISO/IEC 42001:2023 tanúsítvány?

Az audit ára az időtartamhoz hasonló okok miatt változhat.

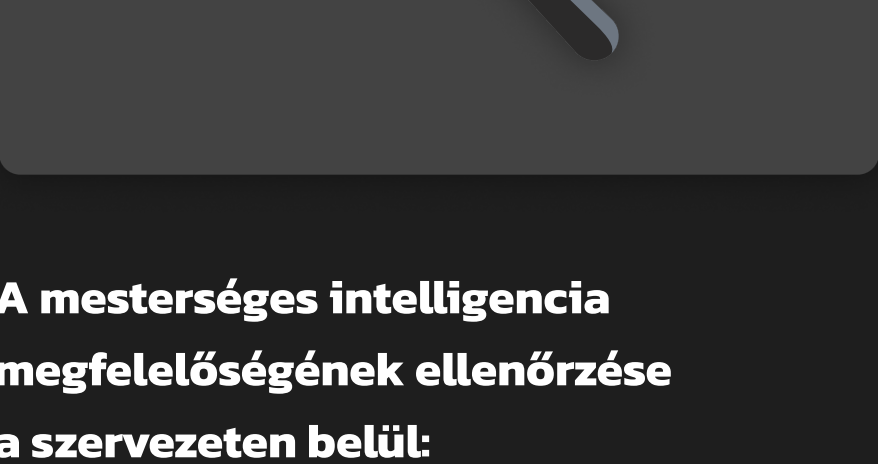
Gyakorlati előkészítési lépés az ISO/IEC 42001:2023 megfeleléshez

A mesterséges intelligencia fellendülésével az ISO/IEC 42001:2023-nak való megfelelés segíthet megkülönböztetni a szervezetet, és megmutatni elkötelezettségét a technológia felelősségteljes használatát iránt. Néhány fontos lépés az ISO/IEC 42001:2023 megfeleléshez:



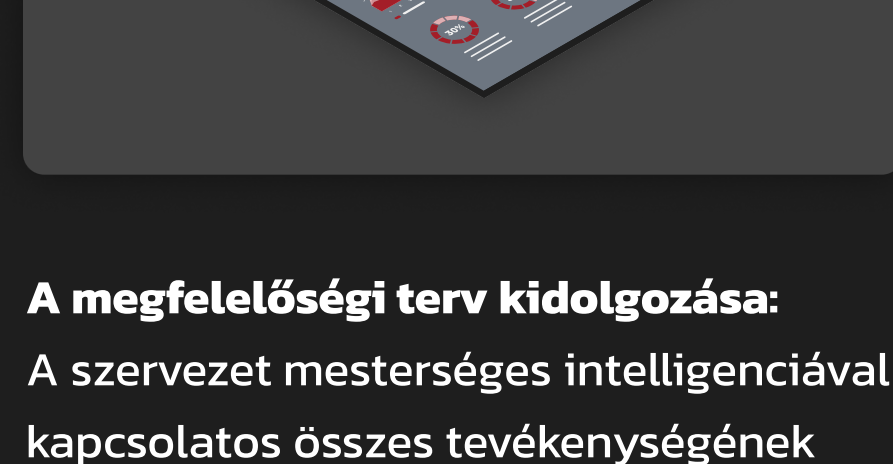
Ismerje meg a szabványt:

Az ISO/IEC 42001:2023 egy nyilvános szabvány, amely megvásárolható az ISO webhelyéről. Egy szabvány példány beszerezése és áttekintése betekintést nyújthat a mesterséges intelligencia kezelésének legjobb gyakorlataiba.



A mesterséges intelligencia megfelelőségének ellenőrzése a szervezetben belül:

A szervezet működhet mesterséges intelligencia-szolgáltatóként, – előállítóként, –vevőként vagy a három kombinációjaként, és a szabvány alkalmazásával, illetve a megfelelés előnyeirnek kiaknázásával feltérképezheti a szervezet jelenlegi és/vagy tervezett mesterséges intelligencia-kitettségét



A megfelelési terv kidolgozása:

A szervezet mesterséges intelligenciával kapcsolatos összes tevékenységének központi irányítás alá történő vonása összetett folyamat lehet, különösen akkor, ha egy szervezet több (termelési, szolgáltatói vagy fogyasztói) szerepet is betölt. A folyamatok és vezérlések fejlesztése, teste szabása ugyanakkor teljes mértékben a vállalat céljainak tükrében történhet meg