Ernst & Young Kft.
Ernst & Young Ltd.
H-1132 Budapest Váci út 20.
1399 Budapest 62. Pf.632, Hungary

Tel: +36 1 451 8100
Fax: +36 1 451 8199
www.ey.com/hu
Cg. 01-09-267553

dr. Farkas Ádám – Szügyi Dániel – Schrettner Attila

ISO 37301 Compliance Management Systems szabvány

* Integritás és sikeres compliance működés a szabványosításon keresztül*

Bevezetés

A visszaélésmegelőzés és az integritás megőrzése több szempontból is fontos lehet egy szervezet számára. Erősíti a szervezet hírnevét **(50%), elősegíti az új tehetségek bevonzását és megtartást (41% és 40%), az ügyfelek megtartását (37%) és a pénzügyi teljesítmény fokozását (35%)**[1].

A felelős vállalati működés biztosítása azonban egyre nehezebb, amelyet a COVID-19 világjárvány hatása is fokoz. Ezt mutatja, hogy az elmúlt hónapokban felmerülő etikai aggodalmak közt szerepel a hagyományos munkavégzési módok háttérbe szorulása (33%), az ellátási láncok nehezebb menedzselése (28%), és a munkavállók juttatási csomagjának csökkenése (24%) is. Az ACFE kutatása is jelentős visszaélési kockázatokra hívja fel a figyelmet. 2020 decemberében a válaszadók 44%-a várt jelentős emelkedést és 46%-a várt emelkedést a visszaélések általános szintjében[2]. Ezen belül is kiemelt figyelem hárul a cyber térben elkövetett és a fizetési tranzakciókhoz kötődő visszaélésekre.

Szabványosítási trend és előzmények

A compliance szakembereknek ezekre a kihívásokra kell megoldást találniuk. Az utóbbi időben egyre erősebben jelentkező trend, hogy ezeknek a kihívásoknak a kezelésére a **nemzetközi jó gyakorlatokat összefoglaló szabványokat vezetnek be a szervezetek**. A vonatkozó szabványokon közt található meg az ISO 37xxx szabvány család is, amely kifejezetten a vállaltirányítás és az etikus vállalati működés területére vonatkozó szabványokat tartalmaz. A szabványcsaládnak eddig három tagja elérhető, az ISO 37001 Antikorrupciós irányítási rendszerek, az ISO 37002 Visszaélésbejelentéssel kapcsolatos rendszerek (*Whistleblowing management systems*) és az ISO 37301 Compliance irányítási rendszerek (*Compliance management systems*).

Az ISO 37001 - amely a szabványcsalád legelső tagja volt - már **Magyarországon is megjelent**, létezik nemzeti szabvány formájában, az MSZ ISO 37001:2019, és **a magyar kormány is jó gyakorlatként ismeri el**. A szabvány követendő példaként szerepel a kormány antikorrupciós stratégiájában[3], és a Gtbkr. Irányelvhez kapcsolódó Kézikönyvben is.[4]

Az ISO 37002 pedig a bejelentő rendszerek kiépítését vagy továbbfejlesztését támogatja. Segíti továbbá a bevezető szervezetet az EU whistleblowing irányelvnek[5] (és értelemszerűen majd az arra épülő magyar szabályozásnak való megfelelésben).

Az ISO 37301 pedig az ISO19600-at[6] váltja, egészíti ki és aktualizálja, hogy megfeleljen a jelen kor compliance kihívásainak. Már az ISO 19600 szabvány célja is az volt, hogy útmutatást nyújtson egy egyszerű, költséghatékony, átlátható és effektív compliance irányítási rendszer kialakításához, a PDCA ciklus „tervezés-cselekvés-ellenőrzés-beavatkozás” ismétlődő

[1] EY Global Integrity Report, 2020
[2] ACFE Fraud in the Wake of Covid-19: Benchmarking Report, December 2020 Edition
[3] A 2020-2022. közötti időszakra szóló középtávú Nemzeti Korrupcióellenes Stratégia, Link: https://korrupciomegelozes.kormany.hu/download/f/ff/92000/STRAT%C3%89GIA%20k%C3%B6zz%C3%A9tett.pdf, Letöltve: 2021.05.18.
[4] KÉZIKÖNYV a köztulajdonban álló gazdasági társaságok részére a belső kontrollrendszer kialakításához és működtetéséhez, Link: https://allamhaztartas.kormany.hu/download/8/f9/b2000/Gtbkr_k%C3%A9zik%C3%B6nyv_2021.pdf, Letöltve: 2021.05.18.
[5] Az Európai Parlament és a Tanács (EU) 2019/1937 Irányelve (2019. október 23.) az uniós jog megsértését bejelentő személyek védelméről
[6] ISO 19600:2014 Compliance management systems

négylépéses módszert alkalmazva. Mivel az ISO 37301 az ISO19600 szabvány alapján lett kiépítve, ezért nincsnek alapvető különbségek a kettő között. Azonban érdemes kiemelni az ISO 37301 lényegesebb új elemeit, mint például a foglalkoztatási folyamat során megkövetelt átvilágítást, a munkavállalói jelentéstételt (*whistleblowing*) és a munkavállalói védelem további erősítését, valamint a kivizsgálási (*investigation*) folyamatok erősítését. A tartalmi módosítások mellett a legnagyobb újdonság, hogy az ISO 37001 **már nem csupán irányelv, hanem tanúsítható szabvány**.

Az ISO 37301 szabvány alapelvei és a szabvány által elvárt tevékenységek

Az ISO 37301 szabvány működése elméleti síkon három alapelvre épül, a **kockázat alapú megközelítésre** (*risk-based approach*), a **folyamatos fejlesztésre**[7] (*contious impovement*) és a **vezetői elköteleződésre** (*tone-at-the-top*).

A kockázat alapú megközelítés garantálja, hogy a szabvány elvárásai találkozzanak a bevezető szervezet elvárásaival, így minden szervezet személyre szabott irányítási rendszert vezethet be[8]. A bevezető szervezet saját, méretének, stratégiájának, földrajzi elhelyezkedésének, iparági sajátosságainak, termékportfóliójának, üzleti modelljének és szabályozási környezetének figyelembevételével alakítja ki kockázati univerzumát. A kockázati univerzum segít a szervezet **visszaélési és integritási profiljának 360°-os feltérképezésében** és az egyes kockázati területek priorizálásába.

A folyamatos fejlesztés biztosítja, hogy a compliance irányítási rendszer ne legyen statikus és ne csak a dokumentáció szintű megfelelést szolgálja. A folyamatos fejlesztés jegyében a kockázatok felmérését, az átvilágítási feladatokat és az auditokat rendszeres időközönként, egy előre felállított terv szerint kell elvégezni. Az ezen tevékenységek során feltárt új kockázatok vagy nemmegfelelőségek kezelésére pedig helyesbítő intézkedéseket kell megfogalmazni és megvalósítani. Így **a compliance irányítási rendszer organikusan fejlődik és igazodik** a szervezet és a környezete elvárásaihoz.

A vezetői elköteleződés abban jelenik meg, hogy a szervezet nem csupán operatív szinten foglalkozik a compliance kérdéseivel, hanem **stratégiai prioritássá teszi a felelős működés és az integritás elérését**. A vezetők pedig ennek megfelelően maguk is tudatosan és tervezetten kommunikálják ezeket az üzeneteket és üzeneteiket saját példamutatásukkal erősítik meg.

A fent említett három alapelvet követve az ISO 37301 szabvány egymásra épülő tevékenységeket határoz meg egy hatásos és hatékony compliance irányítási rendszer létrehozása és működtetése érdekében: a szervezet környezetének megértését, a vezetői szerepvállalást, a compliance irányítási rendszer tervezését és támogatását, a rendszer működésével, valamint a compliance rendszer teljesítményértékelésével és folyamatos fejlesztésével kapcsolatos tevékenységeket. Ezekkel a tevékenységekkel kapcsolatos elvárásokat a szabvány részletesen tartalmazza.[9]

ISO 37301 szabvány bevezetése és előnyök

A fenti elvárások teljesítése kihívást jelenthet a szervezetek számára és speciális szaktudás bevonását is igényelheti. A bevezetési folyamat magában foglal egy **érintett elemzést (*stakeholder analysis*), kockázatértékelést, célkijelölést, eltéréselemzést (*gap assessment*), fejlesztési terv összeállítását, az egyes fejlesztések megvalósítást a szabályzatok, folyamatok és informatikai rendszerek szintjén, képzési és kommunikációs terv meghatározását.** Ezek után pedig egy tanúsító audit keretében a szervezet megszerezheti az ISO 37301 tanúsítványt, amelyet éves ellenőrző audit (*surveillance audit*) erősít meg.

---

[7] PDCA (*Plan-Do-Check-Act*) ciklus alapján
[8] Ambrus István, Farkas Ádám (2019): A compliance alapkérdései – a szabályszerű vállalati működés elmélete és gyakorlata
[9] ISO 37301 Compliance management systems — Requirements with guidance for use

A szabvány bevezetésének és a tanúsítvány megszerzésének előnyei közé sorolható:

- Egységes keretbe foglalja a szerte ágazó compliance tevékenységeket (antikorrupció, adatvédelem, visszaélés-megelőzés, pénzmosás ellenes stb.)
- A bevezető szervezet elkötelezettséget mutatja az etikus működés iránt
- Nemmegfelelőségek és hatósági, bírósági eljárások kockázatának csökkentését szolgálja
- Növeli a munkavállalói elkötelezettséget
- Erősíti az üzleti partnerkapcsolatokat, versenyelőnyként szolgálhat

Ezen előnyök miatt a szabvány széles körű elterjedése várható. Az ISO 37301 esetén az ISO várakozása az, hogy a nagyságrendileg ~18.000 tanúsítás várható globálisan[10].

Kapcsolat a belső ellenőrzéshez

A várható elterjedés és a visszaélésmegelőzésmegelőzési, integritási aspektus miatt a belső ellenőröknek is érdemes lehet megismerkedni a szabvánnyal.

Ennek fő oka, hogy a szabvány - más ISO szabványokhoz hasonlóan - maga is elvár bizonyos audit tevékenységeket a compliance irányítási rendszer vonatkozásában. Ezeket érdemes a belső ellenőrzés tevékenységével összhangba állítani, esetleg bevonni a belső ellenőrzést is már a tervezés fázisában. Ez erősítheti a compliance és a belső ellenőrzés közti együttműködést és tudás megosztást, valamint elkerülhető a duplikációk a szabvány szerinti és az általános audit tervben.

[10] Ethics Intelligence: What to expect from the eagerly anticipated ISO 37301?, Link: https://ethic-intelligence.com/blogs/certified-for-compliance/what-to-expect-from-the-eagerly-anticipated-iso-37301, Letöltve: 2021.05.18.