# ISACA MÁSODIK SZERDAI ELŐADÁS


## Kollár Róbert CIA, Pintér Szabolcs


### Belső ellenőrzés és ISO tanúsítás – hasonlóságok és eltérések

2025 március 12.



ISACA®
Budapest Chapter

# FELELŐSSÉG KIZÁRÁSA

Az elhangzott prezentációk tartalmát illetően az ISACA Magyarországi Egyesület nem vállal felelősséget az abban nyújtott információk aktualitásáért, helyességéért és teljességéért.

Az itt elhangzott információk nem feltétlenül egyeznek meg az ISACA Magyarországi Egyesület álláspontjával.



ISACA®
Budapest Chapter

# ISACA, IIA, ISO

- **ISACA** (Information Systems Audit and Control Association), 1969
- **IIA** (Institute of Internal Auditors), 1941
- **ISO** (International Organization for Standardization) 1947, jogelődje: ISA (International Federation of the National Standardizing Associations), 1926



ISACA Budapest Chapter

# ISO szabványok



ISACA®
Budapest Chapter

# Az ISO szabványokról

MSZ EN ISO 9001:2015; MSZ ISO/IEC 27001:2023

- MSZ: Ez a jelzés a Magyar Szabványügyi Testület (MSZT) által kiadott szabványt jelöli.
- EN: Ez a jelzés az Európai Szabványt (European Norm) jelöli, ami azt jelenti,

hogy az adott szabvány az Európai Unió szabványosítási testületeinek(CEN,CENELEC, ETSI) közös munkájának eredménye.

- ISO: Ez a jelzés a Nemzetközi Szabványügyi Szervezetet jelöli (International Organization for Standardizationt).
- IEC:  A jelzés a Nemzetközi Elektrotechnikai Bizottságot jelöli (International Electrotechnical Commission ).

# A szabványok alkalmazása

- A szabványok alkalmazása önkéntes
- Bizonyos ágazatokban kötelezővé tehetik a jogszabályok vagy a szerződéses feltételek, hogy biztosítsák a termékek és szolgáltatások biztonságát és megbízhatóságát.

Példa: 2015. évi LVII. törvény az energiahatékonyságról

- 22. § (2) Mentesül a kötelező energetikai auditálás alól az a nagyvállalat, amely az EN ISO 50001 szabványnak megfelelő, akkreditált tanúsító szervezet által tanúsított energiagazdálkodási rendszert működtet.



ISACA Budapest Chapter

# ISO irányítási rendszerszabványok

MSZ EN ISO 9001:2015
MSZ EN ISO 14001:2015
MSZ ISO/IEC 27001:2023
MSZ EN ISO/IEC 27701:2021
MSZ EN ISO 22301:2025 EV
MSZ ISO 45001:2018
MSZ EN ISO 50001:2019




ISACA®
Budapest Chapter

# Az irányítási rendszerszabványok közös jellemzői

- Folyamat alapú megközelítés
- Kockázat alapú megközelítés
- PDCA-ciklus
- Vezetőség elköteleződése
- Érdekeltek bevonása
- Dokumentálás és nyomon követés (dokumentált információ)
- Képzés és tudatosság
- Egységes keretrendszer (High-Level Structure)




ISACA®
Budapest Chapter

# • Egységes keretrendszer (High-Level Structure)

## ISO 27001, 6. Tervezés

**6.1 A kockázatokkal és lehetőségekkel kapcsolatos tevékenységek**

**6.1.1 Általános követelmények**

Amikor az információbiztonság-irányítási rendszert tervezik, a szervezetnek figyelembe kell vennie a

4.1. szakaszban hivatkozott tényezőket és a 4.2. szakaszban hivatkozott követelményeket, és meg kell határoznia azokat a kockázatokat és lehetőségeket, melyekkel foglalkozni kell ahhoz, hogy:

a) biztosítsák az információbiztonság-irányítási rendszertől elvárt eredmény(ek) elérhetőségét;

b) megelőzzék vagy csökkentsék a nem kívánt hatásokat; és

c) elérjék a folyamatos fejlesztést. A szervezetnek meg kell terveznie:

d) az ezen kockázatokkal és lehetőségekkel kapcsolatos tevékenységeket; és

e) azt, hogy hogyan

1) építi be és valósítja meg ezeket a tevékenységeket az információbiztonság- irányítási rendszerének folyamataiba; és

2) értékeli ezen tevékenységek eredményességét.

## ISO 9001, 6. Tervezés

**6.1 A kockázatokkal és lehetőségekkel kapcsolatos tevékenységek**

**6.1.1.** A szervezetnek a minőségirányítási rendszer tervezése során át kell gondolnia a 4.1. szakaszban hivatkozott tényezőket és a 4.2. szakaszban hivatkozott követelményeket, valamint meg kell határoznia azokat a kockázatokat és lehetőségeket, amelyekkel foglalkozni kell ahhoz, hogy:

a) biztosítsák, hogy a minőségirányítási rendszer el tudja érni az elvárt eredmény(eke)t;

b) növeljék a kívánt hatásokat;

c) megelőzzék vagy csökkentsék a nem kívánt hatásokat;

d) fejlesztést érjenek el.

**6.1.2.** A szervezetnek meg kell terveznie:

a) az ezen kockázatokkal és lehetőségekkel foglalkozó tevékenységeket;

b) azt, hogy hogyan:

1) integrálja és vezeti be minőségirányítási rendszerének folyamataiba (lásd a 4.4. szakaszt) ezeket a tevékenységeket;

2) értékeli ezeknek a tevékenységeknek az eredményességét.



ISACA Budapest Chapter

# Az ISO 27000 szabványcsalád néhány eleme

ISO/IEC 27000 :
áttekintést nyújt az információbiztonsági rendszerek (ISMS) fogalmáról, valamint azokban használt szakmai kifejezések és meghatározásokról

**ISO/IEC 27001:**
Ez a legismertebb szabvány a családból, amely részletesen leírja az ISMS követelményeit

ISO/IEC 27002:
Az ISO 27001 az „A”-mellékletében szereplő követelmények részletezése

ISO/IEC 27003:
Az ISMS bevezetésének irányelveit tartalmazza

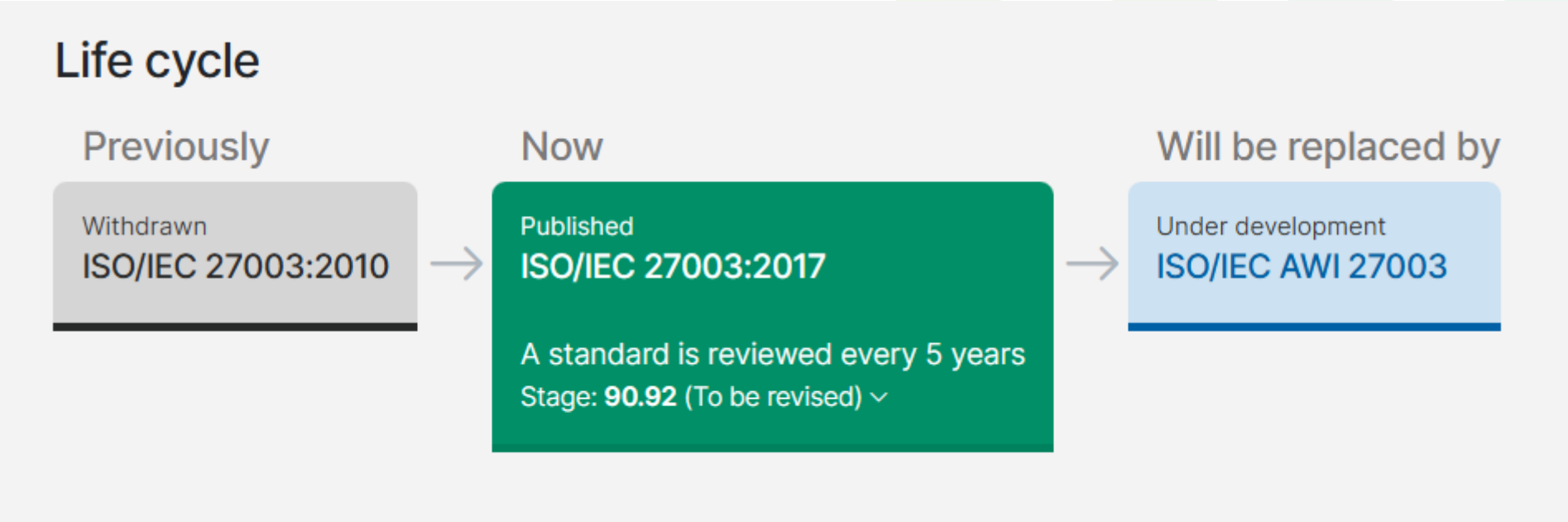
ISO/IEC 27004:
Az információbiztonsági teljesítmény mérésének irányelveit és módszereit részletezi

ISO/IEC 27005:
Az információbiztonsági kockázatkezelés irányelveit és módszereit ismerteti



ISACA Budapest Chapter

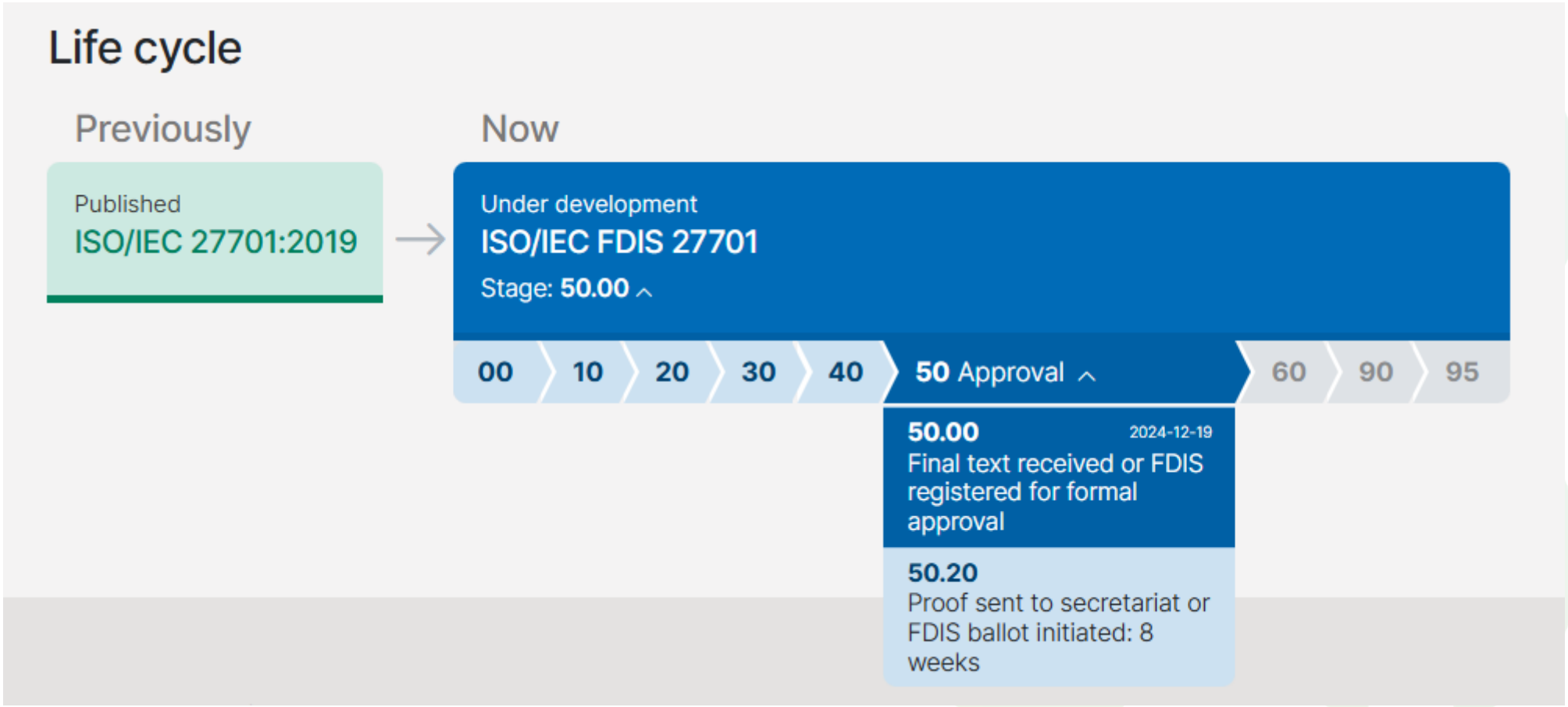
# Az ISO 27000 szabványcsalád néhány eleme






ISACA® Budapest Chapter

# Az ISO 27000 szabványcsalád néhány eleme






ISACA®
Budapest Chapter

# Az ISO 27000 szabványcsalád néhány eleme

| STAGE | SUBSTAGE | | | 90 Decision | | | |
|---|---|---|---|---|---|---|---|
| | 00 Registration | 20 Start of main action | 60 Completion of main action | 92 Repeat an earlier phase | 93 Repeat current phase | 98 Abandon | 99 Proceed |
| 00 Preliminary | 00.00 Proposal for new project received | 00.20 Proposal for new project under review | 00.60 Close of review | | | 00.98 Proposal for new project abandoned | 00.99 Approval to ballot proposal for new project |
| 10 Proposal | 10.00 Proposal for new project registered | 10.20 New project ballot initiated | 10.60 Close of voting | 10.92 Proposal returned to submitter for further definition | | 10.98 New project rejected | 10.99 New project approved |
| 20 Preparatory | 20.00 New project registered in TC/SC work programme | 20.20 Working draft (WD) study initiated | 20.60 Close of comment period | | | 20.98 Project deleted | 20.99 WD approved for registration as CD |
| 30 Committee | 30.00 Committee draft (CD) registered | 30.20 CD consultation initiated | 30.60 Close of comment period | 30.92 CD referred back to Working Group | | 30.98 Project cancelled | 30.99 CD approved for registration as DIS |
| 40 Enquiry | 40.00 DIS registered | 40.20 DIS ballot initiated: 12 weeks | 40.60 Close of voting | 40.92 Full report circulated: DIS referred back to TC or SC | 40.93 Full report circulated: decision for new DIS ballot | 40.98 Project cancelled | 40.99 Full report circulated: DIS approved for registration as FDIS |
| 50 Approval | 50.00 Final text received or FDIS registered for formal approval | 50.20 Proof sent to secretariat or FDIS ballot initiated: 8 weeks | 50.60 Close of voting. Proof returned by secretariat | 50.92 FDIS or proof referred back to TC or SC | | 50.98 Project cancelled | 50.99 FDIS or proof approved for publication |
| 60 Publication | 60.00 International Standard under publication | | 60.60 International Standard published | | | | |
| 90 Review | | 90.20 International Standard under systematic review | 90.60 Close of review | 90.92 International Standard to be revised | 90.93 International Standard confirmed | | 90.99 Withdrawal of International Standard proposed by TC or SC |
| 95 Withdrawal | | 95.20 Withdrawal ballot initiated | 95.60 Close of voting | 95.92 Decision not to withdraw International Standard | | | 95.99 Withdrawal of International Standard |



ISACA® Budapest Chapter

# Az ISO 27000 szabványcsalád

| | |
|---|---|
| ISO/IEC 27000: Információbiztonsági irányítási rendszerek – Áttekintés és szójegyzék Meghatározza az alapfogalmakat és terminológiát az információbiztonsági irányítási rendszerekhez (ISMS). | ISO/IEC 27032: Kiberbiztonsági irányelvek Fókuszál a kiberbiztonsági kérdésekre és az online fenyegetések kezelésére. |
| ISO/IEC 27001: Információbiztonsági irányítási rendszerek – Követelmények Az ISMS létrehozásának, bevezetésének, fenntartásának és folyamatos fejlesztésének követelményeit tartalmazza. | ISO/IEC 27033: Hálózatbiztonság Többrészes szabvány a hálózatbiztonság részletes útmutatásával. |
| ISO/IEC 27002: Információbiztonsági ellenőrzések gyakorlati szabályzata Útmutatást ad az információbiztonsági kontrollok kiválasztásához és bevezetéséhez. | 27033-1: Áttekintés és koncepciók. |
| ISO/IEC 27003: ISMS bevezetésének útmutatója Segítséget nyújt az ISMS megtervezéséhez és megvalósításához. | 27033-2: Hálózatbiztonság tervezése és megvalósítása. |
| ISO/IEC 27004: Információbiztonsági irányítás – Monitoring, mérés, elemzés és értékelés Útmutatást ad az információbiztonsági teljesítmény méréséhez és értékeléséhez. | 27033-3: Hálózatbiztonsági forgatókönyvek. |
| ISO/IEC 27005: Információbiztonsági kockázatkezelés Részletes útmutatást nyújt a kockázatkezelési folyamatokhoz. | ISO/IEC 27034: Alkalmazásbiztonság Útmutatást ad a biztonság beépítéséhez az alkalmazásfejlesztésbe. |
| ISO/IEC 27006: Követelmények az ISMS tanúsítást végző szervezetek számára Meghatározza a tanúsító szervezetekre vonatkozó követelményeket. | ISO/IEC 27035: Információbiztonsági incidenskezelés Többrészes szabvány az incidenskezelési folyamatokhoz. |
| ISO/IEC 27007: Irányelvek az ISMS auditálásához Útmutatást nyújt az ISMS belső és külső auditjainak végrehajtásához. | ISO/IEC 27036: Információbiztonság beszállítói kapcsolatokban Segít a beszállítókkal kapcsolatos biztonsági kockázatok kezelésében. |
| ISO/IEC 27008: Irányelvek az információbiztonsági kontrollok értékeléséhez Segítséget nyújt az auditoroknak a kontrollok hatékonyságának értékelésében. | ISO/IEC 27037: Digitális bizonyítékok kezelése Útmutató a digitális bizonyítékok gyűjtéséhez és megőrzéséhez. |
| ISO/IEC 27009: Az ISO/IEC 27001 ágazatspecifikus alkalmazása Útmutatást ad az ISO/IEC 27001 követelményeinek ágazatspecifikus alkalmazásához. | ISO/IEC 27038: Specifikáció digitális törléshez (redaction) Meghatározza a digitális dokumentumok érzékeny adatainak biztonságos eltávolítását. |
| ISO/IEC 27010: Információbiztonsági irányítás szervezetek közötti kommunikációhoz Fókuszál a szervezetek közötti információmegosztás biztonságára. | ISO/IEC 27039: Betörés-észlelő és megelőző rendszerek (IDPS) Útmutató az IDPS rendszerek kiválasztásához és működtetéséhez. |
| ISO/IEC 27011: Információbiztonsági irányítási irányelvek távközlési szervezetek számára Specifikus útmutatás a távközlési ágazatnak. | ISO/IEC 27040: Tárolási biztonság Részletes útmutatás az adattárolás biztonságához. |
| ISO/IEC 27013: Az ISO/IEC 27001 és az ISO/IEC 20000-1 integrált megvalósításának útmutatója Segít az információbiztonsági és az IT szolgáltatásmenedzsment rendszerek összehangolásában. | ISO/IEC 27041: Incidensvizsgálati módszerek biztosítása Segít az incidensvizsgálati módszerek megfelelőségének értékelésében. |
| ISO/IEC 27014: Információbiztonsági irányítás Útmutatást ad az információbiztonság irányításához a szervezet felső vezetése számára. | ISO/IEC 27042: Digitális bizonyítékok elemzése és értelmezése Útmutató az incidensvizsgálatokhoz. |
| ISO/IEC 27015: Információbiztonsági irányítási irányelvek pénzügyi szolgáltatásokhoz Specifikus útmutatás a pénzügyi szektor számára. | ISO/IEC 27043: Incidensvizsgálat elvei és folyamatai Átfogó megközelítés az incidensvizsgálatokhoz. |
| ISO/IEC 27016: Információbiztonság-gazdaságtan szervezeti szinten Segít megérteni az információbiztonság gazdasági vonatkozásait. | ISO/IEC 27050: Elektronikus adatfeltárás (eDiscovery) Többrészes szabvány az elektronikus adatok jogi célú feltárásához. |
| ISO/IEC 27017: Információbiztonsági kontrollok felhőszolgáltatásokhoz Kiegészíti az ISO/IEC 27002-t felhőspecifikus kontrollokkal. | ISO/IEC 27100: Kiberbiztonság – Áttekintés és fogalmak Meghatározza a kiberbiztonság alapfogalmait és keretrendszerét. |
| ISO/IEC 27018: Azonosítható személyes adatok védelme nyilvános felhőben Útmutatás a személyes adatok kezeléséhez felhőalapú környezetben. | ISO/IEC 27701: Adatvédelmi információkezelési rendszer (PIMS) Kiterjesztés az ISO/IEC 27001 és 27002 szabványokhoz a személyes adatok védelmére. |
| ISO/IEC 27019: Információbiztonsági irányítás az energiaközmű ágazat számára Specifikus követelményeket határoz meg az energiaszektor számára. | ISO/IEC 27799: Egészségügy – Információbiztonsági irányítás Útmutatás az egészségügyi információk védelméhez. |
| ISO/IEC 27031: ICT készenlét az üzletmenet-folytonossághoz Útmutatást ad az informatikai rendszerek folyamatos működésének biztosításához. | ISO/IEC 27018: Személyes adatok védelme felhőben (Ismétlés, de fontos kiemelni a PII védelmét felhőszolgáltatásokban.) |

# A kockázatkezelés szabványai

Az ISO 31000 és az EN IEC 31010 szabványok fókuszában a kockázatkezelés áll, de különböző aspektusokra fókuszálnak

ISO 31000: ez a szabvány általános irányelveket és keretrendszert biztosít a kockázatkezelés számára. Leírja a kockázatkezelési folyamatokat, segít a kockázatkezelési stratégiájuk kidolgozásában és végrehajtásában. Az ISO 31000 főként a kockázatkezelési kultúra, politika, program és folyamatokra összpontosít.

EN IEC 31010: konkrét módszereket és technikákat biztosít a kockázatok azonosítására és értékelésére.




ISACA Budapest Chapter

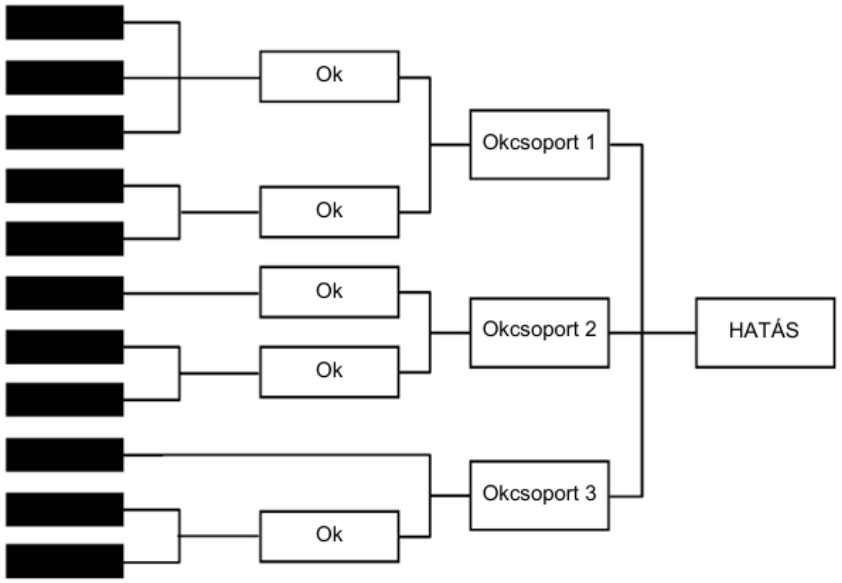
# A kockázatkezelés ISO szabványai

| Eszközök és eljárások | Kockázatfelmérési folyamat | | | | | Lásd a mellék-letet |
|---|---|---|---|---|---|---|
| | Kockázat-azonosítás | Kockázatelemzés | | | Kockázat-értékelés | |
| | | Követ-kezmény | Valószí-nűség | Kockázati szint | | |
| Ötletbörze | SA[1] | NA[2] | NA | NA | NA | B 01 |
| Strukturált vagy félig strukturált interjúk | SA | NA | NA | NA | NA | B 02 |
| Delphi | SA | NA | NA | NA | NA | B 03 |
| Ellenőrző listák | SA | NA | NA | NA | NA | B 04 |
| Előzetes veszélyelemzés | SA | NA | NA | NA | NA | B 05 |
| Veszély- és működőképesség-tanulmányok (HAZOP) | SA | SA | A[3] | A | A | B 06 |
| Veszélyelemzés és kritikus szabályozási pontok (HACCP) | SA | SA | NA | NA | SA | B 07 |
| Környezeti kockázatfelmérés | SA | SA | SA | SA | SA | B 08 |
| Strukturált «Mi van, ha?» (SWIFT) | SA | SA | SA | SA | SA | B 09 |
| Szcenárióelemzés | SA | SA | A | A | A | B 10 |
| Üzleti hatáselemzés | A | SA | A | A | A | B 11 |
| Eredendőok-elemzés | NA | SA | SA | SA | SA | B 12 |
| Hibamód- és hatáselemzés | SA | SA | SA | SA | SA | B 13 |
| Hibafaelemzés | A | NA | SA | A | A | B 14 |
| Eseményfa-elemzés | A | SA | A | A | NA | B 15 |
| Ok- és következmény-elemzés | A | SA | SA | A | A | B 16 |
| Ok- és hatáselemzés | SA | SA | NA | NA | NA | B 17 |
| Védelmiszint-elemzés (LOPA) | A | SA | A | A | NA | B 18 |
| Döntésfa | NA | SA | SA | A | A | B 19 |
| Emberimegbízhatóság-elemzés | SA | SA | SA | SA | A | B 20 |
| „Bow tie"-elemzés | NA | A | SA | SA | A | B 21 |
| Megbízhatóság-központú karbantartás | SA | SA | SA | SA | SA | B 22 |
| Kúszókör-elemzés | A | NA | NA | NA | NA | B 23 |
| Markov-elemzés | A | SA | NA | NA | NA | B 24 |
| Monte-Carlo-szimuláció | NA | NA | NA | NA | SA | B 25 |
| Bayes-statisztikák és Bayes-hálók | NA | SA | NA | NA | SA | B 26 |
| FN-görbék | A | SA | SA | A | SA | B 27 |




ISACA Budapest Chapter

# A kockázatkezelés ISO szabványai



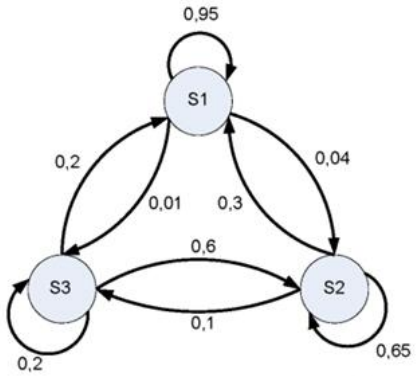

**B6. ábra: Példa ok- és hatáselemzés fájának megformázására**

Az ok- és hatásdiagram általában minőségileg használatos. Lehet azt feltételezni, hogy a probléma valószínűsége 1, és valószínűségeket rendelni az általános okokhoz, és egymást követően a közreható okokhoz, az azok jelentősége miatti bizalom foka alapján. Azonban a közreható okok gyakran kölcsönhatásba lépnek, és komplex módon járulnak hozzá a hatáshoz, ami érvénytelenné teszi a számítást.




ISACA Budapest Chapter

# A kockázatkezelés ISO szabványai




**B9. ábra: Példa a Markov-féle rendszerdiagramra**

Az állapotból induló, önmagához mutató nyilat rendszerint nem mutatják, de ezen a példán belül mutatjuk a teljesség miatt.

Képviselje $P_i$ azt a valószínűséget, hogy a rendszer $i$ állapotban van $i$ = 1, 2, 3 esetén, akkor az egyidejűleg megoldandó egyenletek:

$$P1 = 0{,}95\ P1 + 0{,}30\ P2 + 0{,}20\ P3 \quad \text{(B1.)}$$

$$P2 = 0{,}04\ P1 + 0{,}65\ P2 + 0{,}60\ P3 \quad \text{(B2.)}$$

$$P3 = 0{,}01\ P1 + 0{,}05\ P2 + 0{,}20\ P3 \quad \text{(B3.)}$$




ISACA® Budapest Chapter

# Akkreditáció, tanúsítás



ISACA®
Budapest Chapter

# Akkreditáció

**Akkreditálás:** harmadik fél által kiadott igazolás megfelelőségértékelést végző szervezetről, amely szerint az hivatalosan igazolja annak felkészültségét (kompetenciáját) konkrét megfelelőségértékelési feladatok elvégzésére.

A NAH által a Nemzeti Akkreditálási Rendszer keretében (MSZ EN ISO/IEC 17011:2018 - Megfelelőségértékelés. Megfelelőségértékelést végző szervezeteket akkreditáló testületekre vonatkozó követelmények)

az akkreditálásról szóló jogszabályok, nemzeti szabványként közzétett európai és nemzetközi szabványok figyelembevételével szervezetek, illetve természetes személyek akkreditálhatók.

Pl.:

- terméktanúsító szervezet,
- irányítási rendszereket tanúsító szervezet,
- vizsgálólaboratórium, stb…



ISACA Budapest Chapter

# A NAH nyilvántartásában IBIR tanúsítására jogosult szervezetek

## IBIR tanúsítás / ISMS certification

CertUnion Hungary Tanúsító Kft.
**NAH-4-0118/2021**

CERTOP Termék- és Rendszertanúsító Kft.
**NAH-4-0137/2022**

EUROCERT Minősítő és Tanúsító Kft.
**NAH-4-0119/2022**

IWS Solutions Kft.
**NAH-4-0152/2022**

Magyar Szabványügyi Testület
**NAH-4-0127/2023**

MARTON Szakértő Iroda Kft.
**NAH-4-0047/2023**

ÉMI-TÜV SÜD Minőségügyi és Biztonságtechnikai Kft.
**NAH-4-0041/2023**

TAM CERT Magyarország Vizsgáló és Tanúsító Kft. TAM CERT Rendszertanúsító hely
**NAH-4-0157/2023**



ISACA® Budapest Chapter

# Az MVM Informatika Zrt. ISO 27001 tanúsítványa

Certificate of Registration

nqa

Tanúsítjuk, hogy az alábbi szervezet irányítási rendszere megfelel az említett szabvány követelményeinek a lenti alkalmazási területen.

Tanúsított szervezet neve:
**MVMI Zrt.**

Címe:
**7030 Paks, Vasút utca 1. Magyarország**
**7030 Paks, 8803/15 hrsz. Magyarország**
**1031 Budapest, Szentendrei út 207-209. Magyarország**
**1139 Budapest, Béke tér 9. Magyarország**
**6726 Szeged, Temesvári körút 27-29. Magyarország**

Alkalmazott szabvány:
**MSZ ISO/IEC 27001:2023**

Alkalmazási terület:
**IT Infrastruktúra – UNIX, WINDOWS szerverek, DESKTOP és HÁLÓZAT – üzemeltetése és fejlesztése, alkalmazási rendszerek üzemeltetése és fejlesztése, valamint az ezekhez kapcsolódó ügyfélszolgálat (Help Desk) és szolgáltatásmenedzsment funkciók során kezelt szervezeti- és ügyfél információk védelme**

**Összhangban a MVMI Zrt. Alkalmazhatósági Nyilatkozatával (verziószám: 14, kiadás 2024. március 21.)**

A nyilvántartásba vétel feltétele, hogy a Szervezet a fenti szabványnak megfelelő irányítási rendszert tartson fenn, amelyet az NQA figyelemmel kísér.
Vitás esetekben ezen oklevél angol nyelvű változata az irányadó.

Ügyvezető igazgató

| | |
|---|---|
| Tanúsítvány száma: | 69354 |
| Kiadás: | 2016. szeptember 28. |
| Újra kiadás: | 2024. május 17. |
| Érvényes: | 2027. szeptember 03. |
| EA kód: | 33 |

UKAS



ISACA Budapest Chapter

# Az ISO 27001 tanúsítókra vonatkozó követelmények

- **ISO/IEC 27001:2022**: Ez a szabvány az információbiztonsági irányítási rendszerek (ISMS) követelményeit határozza meg.
- **ISO/IEC 17021-1:2016**: Ez a szabvány a menedzsment rendszerek auditálását és tanúsítását végző szervezetek követelményeit írja le.
- **ISO/IEC 27006-1:2024**: Ez a szabvány az információbiztonsági irányítási rendszerek auditálását és tanúsítását végző szervezetek követelményeit határozza meg.




ISACA Budapest Chapter

# ISO tanúsítás

## Az ISO tanúsítás célja

- Biztosítja a szervezet megfelelését a nemzetközi szabványoknak
- Javítja a folyamatok hatékonyságát és minőségét

## A tanúsítási folyamat lépései

- Részletes dokumentáció és bizonyítékok gyűjtése
- Auditálás és értékelés a szabványoknak való megfelelés érdekében

## Független szervezetek szerepe

- Az ISO tanúsítást független, akkreditált szervezetek végzik



ISACA Budapest Chapter

# ISO 19011, az irányítási rendszerek auditálása

Az ISO 19011 egy nemzetközi szabvány, amely a belső és külső auditok végrehajtására vonatkozó útmutatásokat tartalmazza.

- **Auditálási alapelvek:** Az auditálás alapelvei, amelyek biztosítják az auditok következetességét és hatékonyságát.
- **Auditprogram irányítása:** Az auditprogramok tervezése, végrehajtása és nyomon követése.
- **Auditok végrehajtása:** Az auditok végrehajtásának folyamata, beleértve az audit tervezését, végrehajtását és jelentéskészítését.
- **Auditorok kompetenciája:** Az auditorok képzettsége és értékelése, valamint a folyamatos fejlesztésük.




ISACA Budapest Chapter

# ISO auditorok, szakmai követelmények

**Ismeretekkel kell rendelkezniük** az ISO szabványokról és azok alkalmazásáról. Ez magában foglalja az ISO 9001, ISO 14001, ISO 27001 és más releváns szabványok ismeretét (belső auditori, illetve vezető auditori tanúsítvány, amelyeket irányítási szabványonként külön-külön kell megszerezni)

Az auditoroknak **részt kell venniük** az ISO szabványokkal kapcsolatos képzéseken és továbbképzéseken. Ez biztosítja, hogy naprakészek legyenek a legújabb szabványokkal és auditálási technikákkal kapcsolatban.




ISACA® Budapest Chapter

# ISO auditorok, szakmai követelmények

**Szakmai ismeretek:** Az auditoroknak alapos ismeretekkel kell rendelkezniük az auditált szakterülettel kapcsolatosan (szakirányú képesítés).

**Tapasztalat:** Az auditoroknak gyakorlati tapasztalattal kell rendelkezniük az auditálás területén. Ez magában foglalja a belső és külső auditok végrehajtását, valamint a különböző iparágakban szerzett tapasztalatokat.

**Etikai normák:** Az auditoroknak magas etikai normákat kell követniük, beleértve a függetlenséget, pártatlanságot és a bizalmas információk kezelését.




ISACA®
Budapest Chapter

# IRCA (International Register of Certificated Auditors)

Az IRCA (International Register of Certificated Auditors) egy nemzetközi szervezet, amely az auditorok és vezető auditorok képzését és tanúsítását végzi. Az IRCA célja, hogy biztosítsa az auditorok magas szintű szakmai tudását és kompetenciáját, valamint hogy elősegítse a minőségirányítási rendszerek hatékony működését világszerte.



ISACA®
Budapest Chapter

# Az IRCA tanúsítvány előnyei az auditorok számára

## Globális elismertség

Az IRCA globális elismertsége biztosítja az auditorok számára a nemzetközi tapasztalatszerzés lehetőségét, amely elősegíti szakmai fejlődésüket.

## Nemzetközi partnerségek

Az IRCA nemzetközi partnerekkel együttműködve támogatja az auditorok fejlődését, lehetővé téve számukra a tudásmegosztást és a legjobb gyakorlatok alkalmazását.

## Minőségellenőrzés

A nemzetközi partnerségek javítják a minőségellenőrzési folyamatokat, biztosítva a legmagasabb szintű szakmai követelményeknek való megfelelést.



ISACA Budapest Chapter

# Auditok ISO környezetben

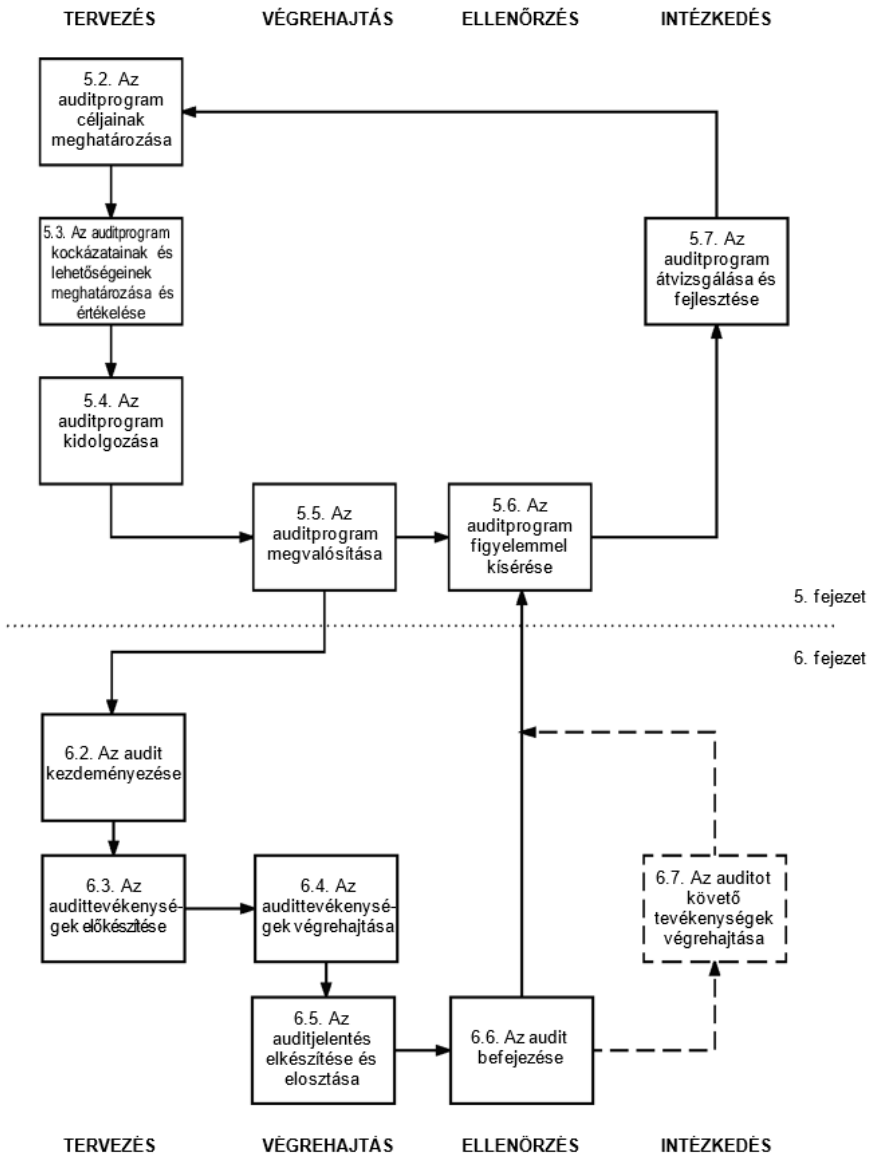
| Első fél általi audit | Második fél általi audit | Harmadik fél általi audit |
|---|---|---|
| Belső audit | Külső szolgáltató auditja | Tanúsítási és/vagy akkreditálási audit |
| | Egyéb külső érdekelt fél auditja | Jogszabályi, egyéb szabályozói audit |

Forrás: MSZ EN ISO 19011:2018



ISACA Budapest Chapter

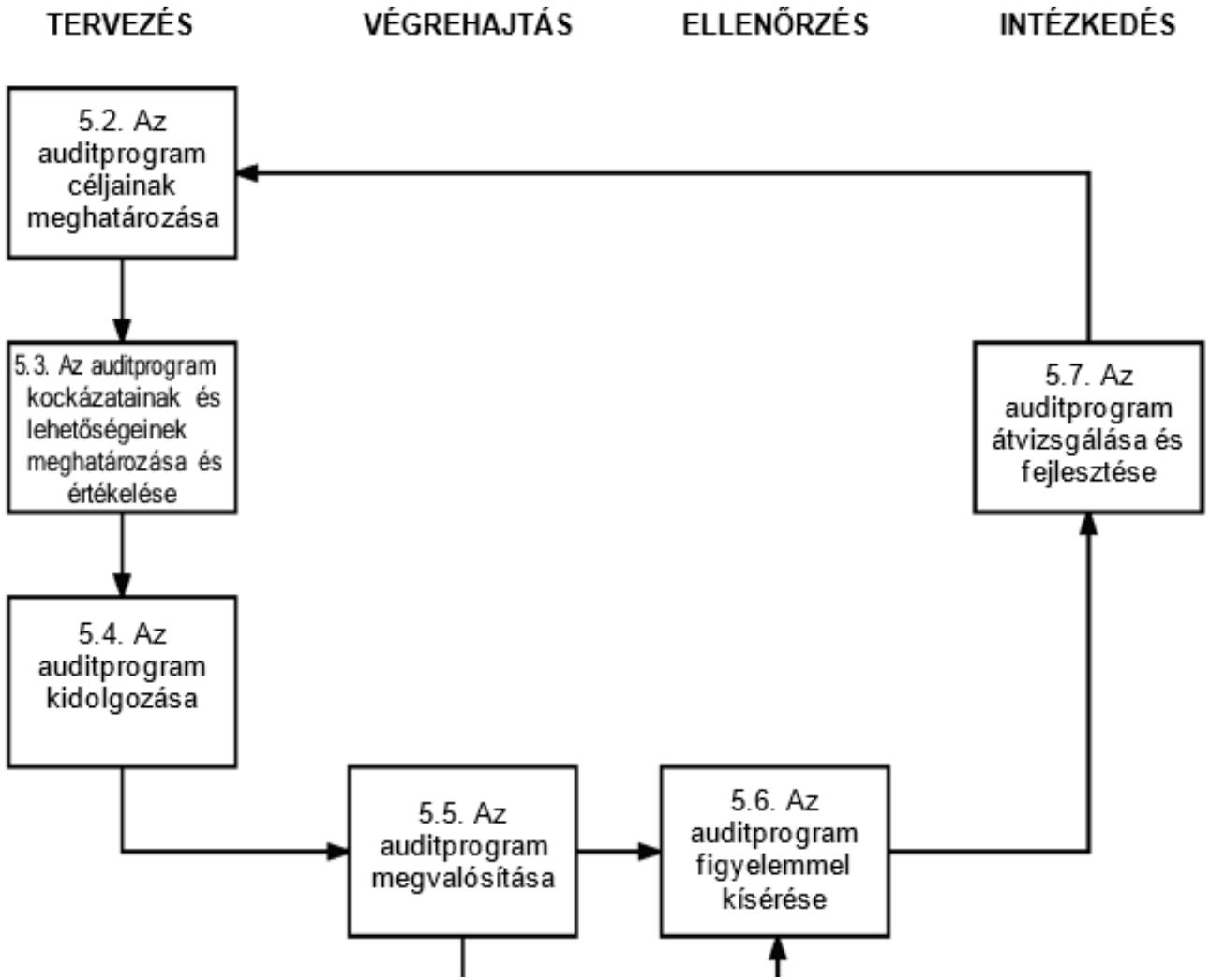
# Az audit folyamat (ISO 19011)






ISACA® Budapest Chapter

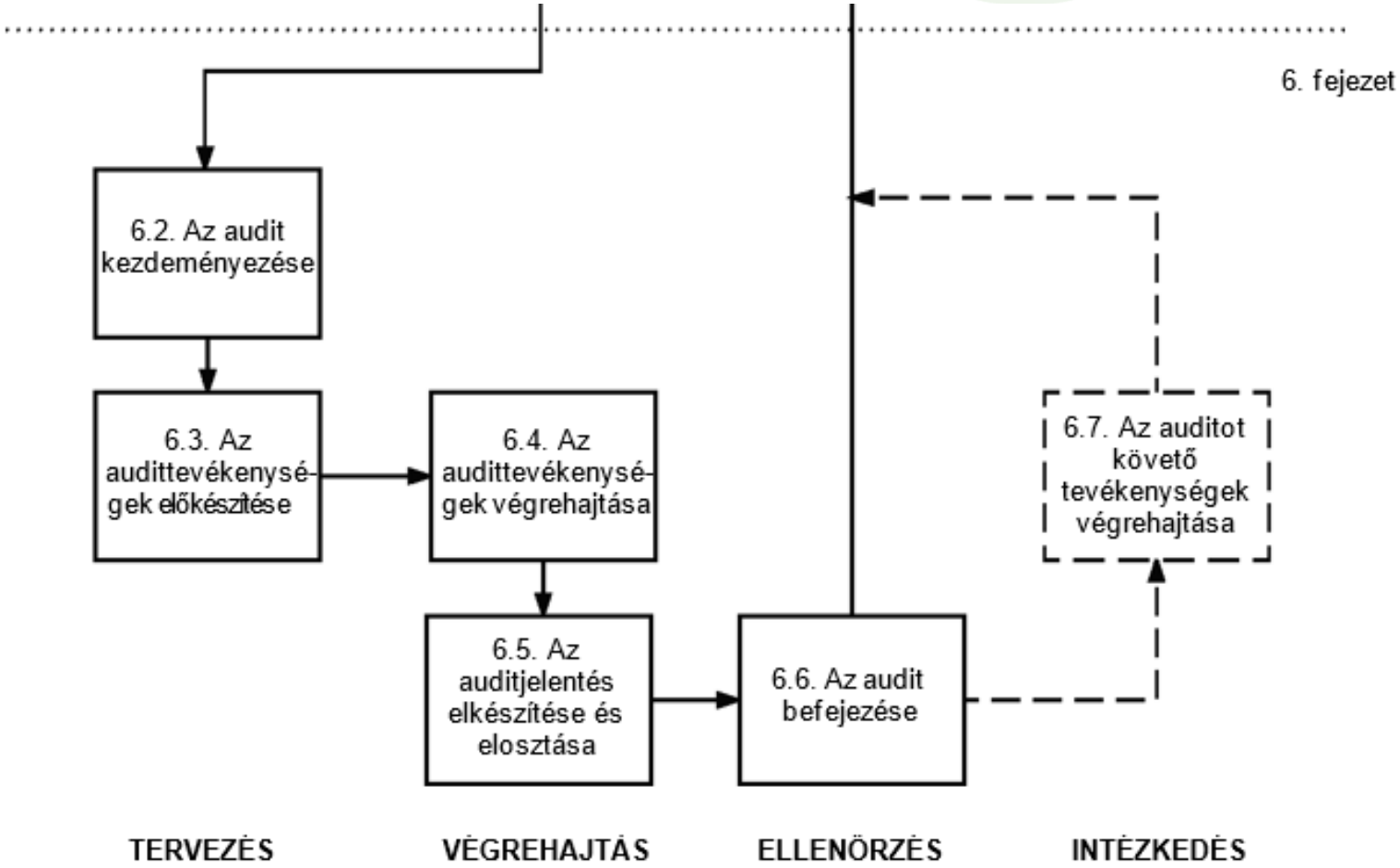
# Az audit folyamat (ISO 19011)






ISACA Budapest Chapter

# Az audit folyamat (ISO 19011)






ISACA Budapest Chapter

# Feladatok tanúsítási ciklusban

- Folyamatos felügyelet és értékelés
- Kockázatkezelés: A szervezetnek folyamatosan azonosítania és értékelnie kell az új kockázatokat, és megfelelő intézkedéseket kell hoznia azok kezelésére.
- Belső auditok
- Vezetőségi átvizsgálás
- Dokumentáció frissítése
- Folyamatos fejlesztés



ISACA Budapest Chapter

# Vezetőségi átvizsgálás

- **9.3.2. A vezetőségi átvizsgálás bemenetei**

A vezetőségi átvizsgálásnak figyelembe kell vennie az alábbiakat:

a) a korábbi vezetőségi átvizsgálásokból származó intézkedések állapota;

b) azon külső és belső tényezők változásai, amelyek az információbiztonság-irányítási rendszer szempontjából lényegesek;

c) az érdekelt felek azon elvárásainak változásai, amelyek az információbiztonság-irányítási rendszer szempontjából lényegesek;

d) az információbiztonság teljesítményére vonatkozó visszajelzések, beleértve a trendeket:

   1) a nemmegfelelőségekről és a helyesbítő tevékenységekről;
   2) a figyelemmel kísérés és mérés eredményeiről;
   3) az audit eredményeiről;
   4) az információbiztonsági célok teljesüléséről;

e) az érdekelt felek visszajelzései;

f) a kockázatfelmérés eredményei és a kockázatkezelési terv állapota;



ISACA Budapest Chapter

# Vezetőségi átvizsgálás

- **9.3.3. A vezetőségi átvizsgálás kimenetei**

A vezetőségi átvizsgálás kimeneteinek döntéseket és intézkedéseket kell tartalmazniuk a folyamatos fejlesztési lehetőségekre és az információbiztonság irányítási rendszer változtatásaira vonatkozó igényre.

A vezetőségi átvizsgálások eredményeiről bizonyítékként dokumentált információkat kell megőrizni.



ISACA Budapest Chapter

# Belső ellenőrzés

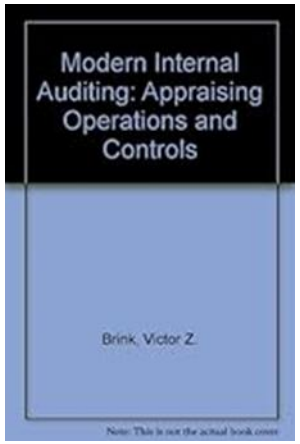


ISACA®
Budapest Chapter

# Amit tudni akartál a belső ellenőrzésről……

**(de sosem merted megkérdezni)**

Victor Z. Brink
A belső ellenőrzés szülőatyja




The Institute of Internal Auditors

Az IIA 1941 november 17-én alakult New Yorkban 24 taggal.

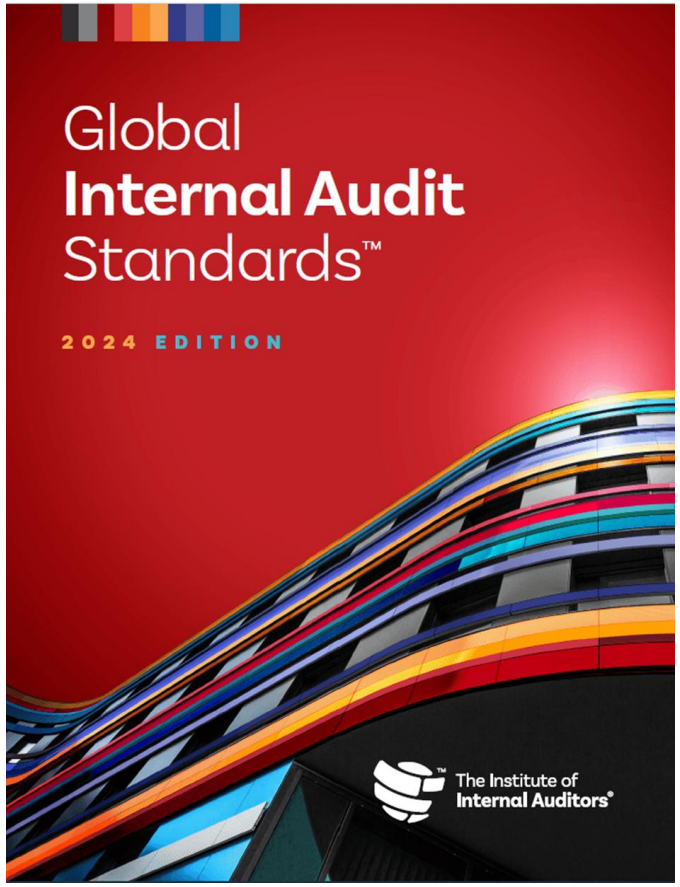
Mára 112 nemzeti képviselet és több mint 200.000 tag

A BEMSZ a magyar képviselet 1992-ben jött létre és jelenleg 620 tagot számlál



ISACA® Budapest Chapter

# A normák és a belső ellenőrzés célja




## A belső ellenőrzés célja

A belső ellenőrzés erősíti a szervezet értéket teremtő, védő és fenntartó képességét azáltal, hogy független, kockázatalapú és tárgyilagos bizonyosságot, tanácsot, mélyebb szakmai megértésre és az előretekintésre vonatkozó lehetőséget nyújt a vezető testület és a felsővezetés számára.

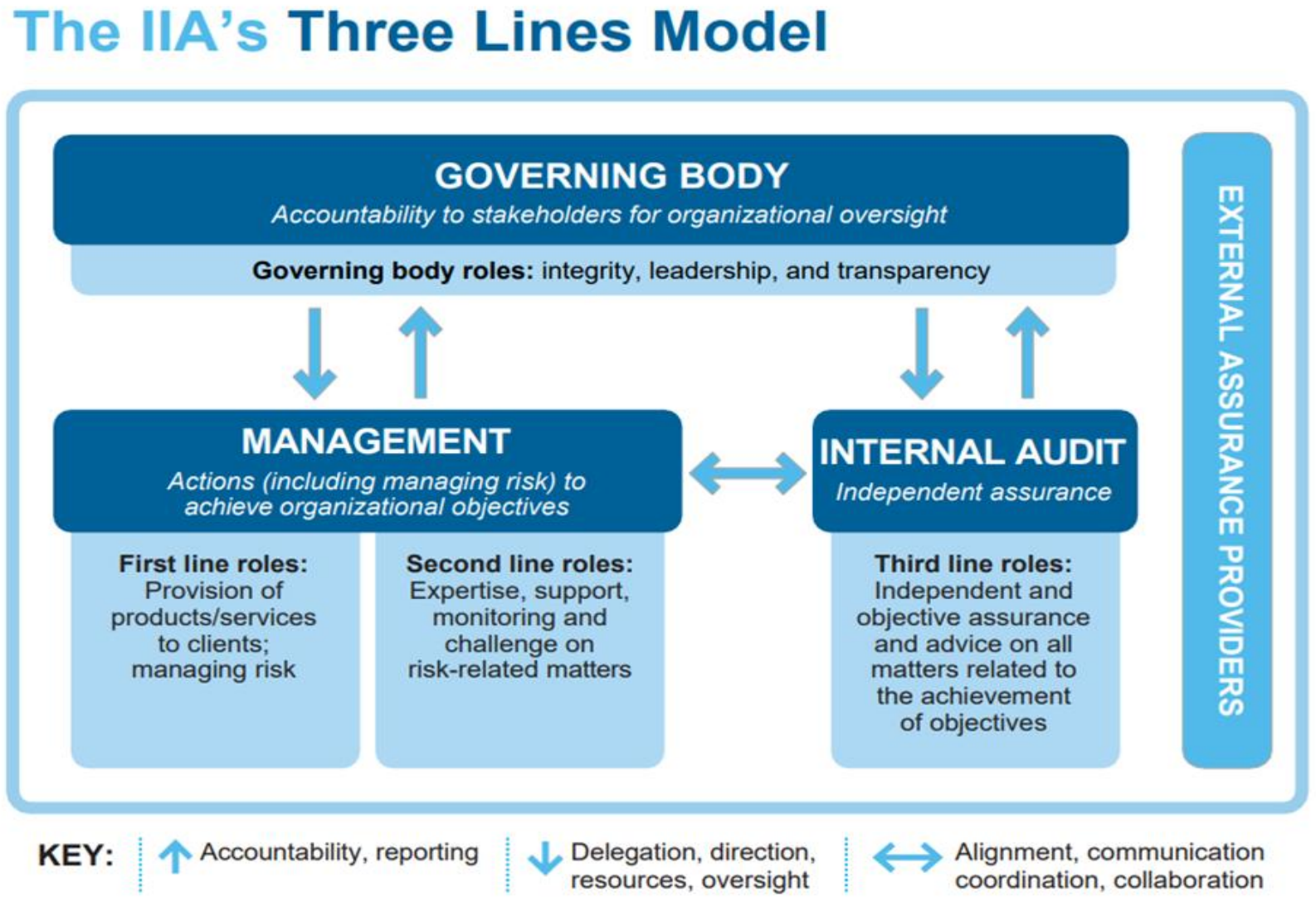
A belső ellenőrzés az alábbi területeken javítja a szervezet működését:

- A célkitűzések sikeres elérése.
- Irányítás, kockázatkezelés és kontrollfolyamatok.
- Döntéshozatal és felügyelet.
- A szervezet hírneve és hitelessége az érdekelt körében.
- Képesség a közérdek szolgálatára.



ISACA Budapest Chapter

# És azok a bizonyos vonalak



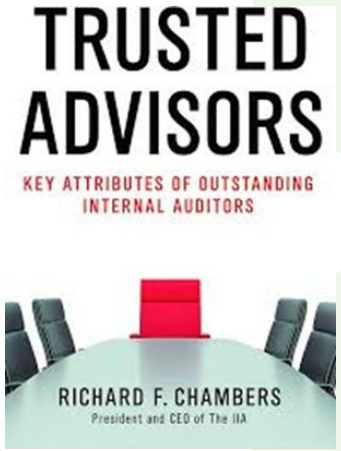


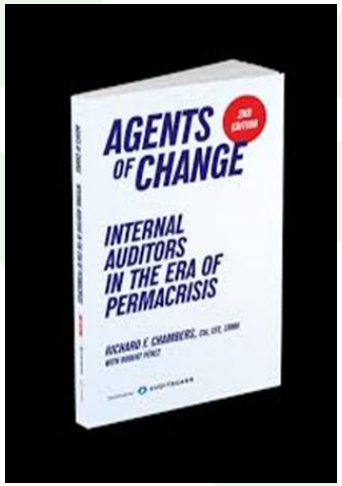

ISACA Budapest Chapter

# Belső rendőrség vs. Tanácsadói szerep

A szabályszerűségi /compliance és a teljesítmény-ellenőrzés már a múlt

A modern belső ellenőr

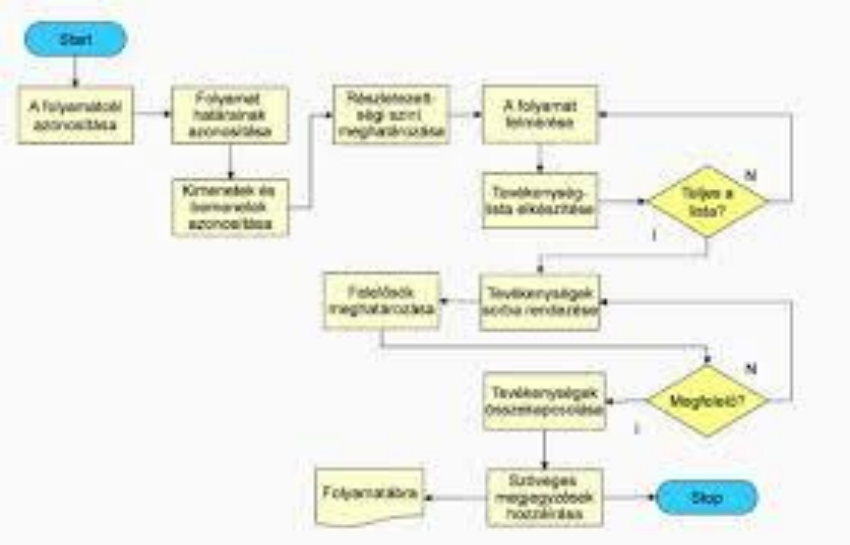


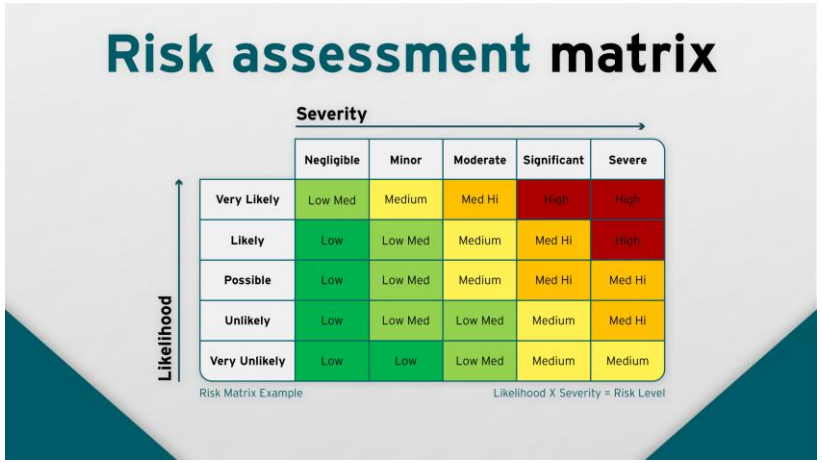






ISACA Budapest Chapter

# Folyamat – kockázatok - kontorollok




## Inherent Risk – Mitigation – Residual Risk

### Risk Control Matrix

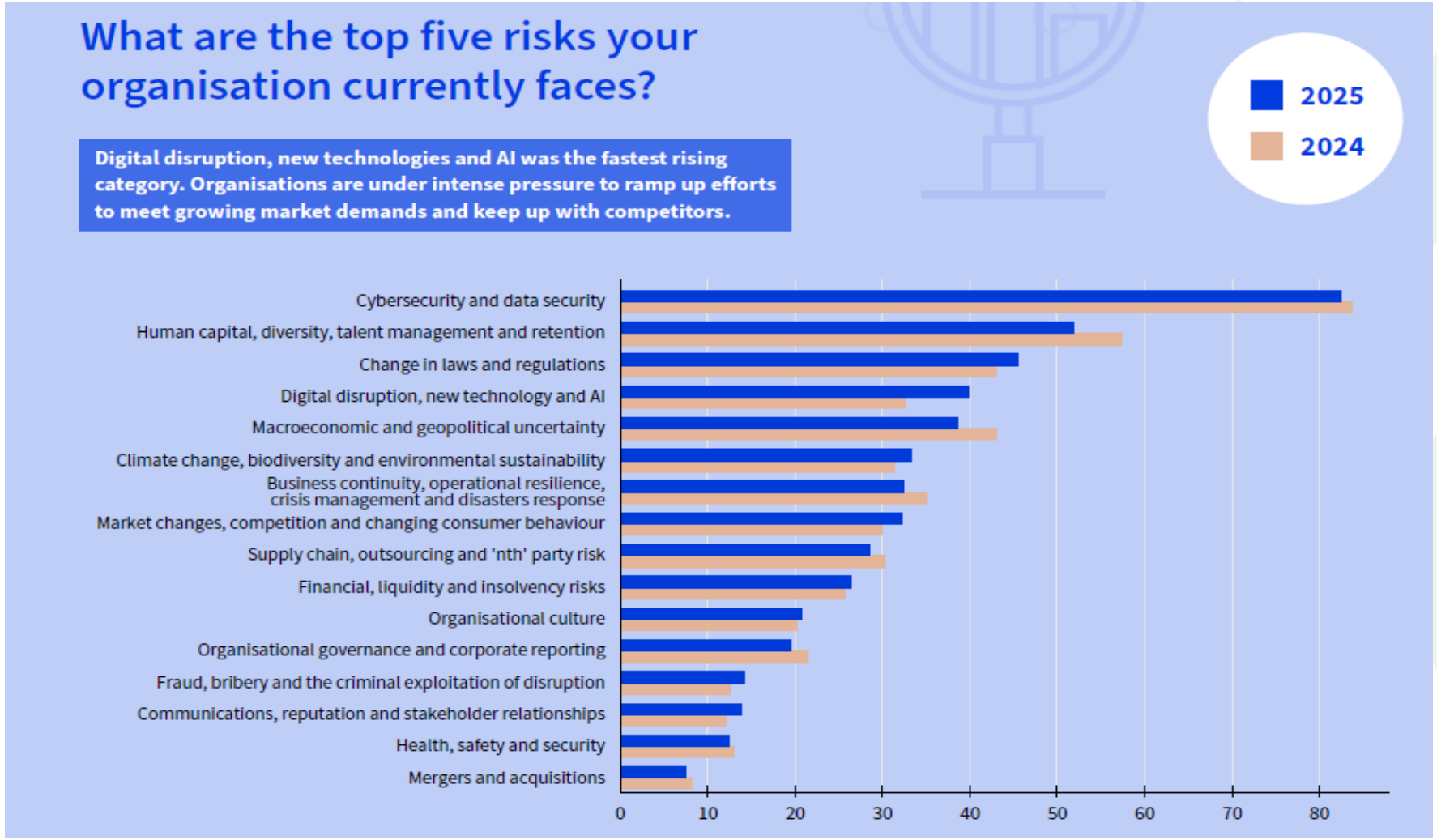
| Key Process Number | Process | Risk Number | Risk | Control Objective | Control Number | Control Description | Control Owner | Process Narrative | Control Category | Control Type | Primary Secondary | Control Frequency | Design Assessment |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| - | Text Here | - | Text Here | - | - | - | Text Here | - | - | - | - | - | Text Here |
| - | - | - | - | - | - | Text Here | - | - | - | Text Here | - | Text Here | - |
| - | Text Here | - | Text Here | - | - | Prepare a risk control matrix to have a close tap on the risk related measures you have intended to take. The below table helps you to keep a log of the control measures you have decided to take to manage the risk levels. | - | - | - | - | Text Here | - | Text Here |
| - | - | - | - | - | - | T | - | Text Here | - | Text Here | - | - | - |
| - | Text Here | - | Text Here | - | - | - | - | - | - | - | Text Here | - | - |
| Text Here | - | - | - | Text Here | - | - | - | Text Here | - | Text Here | - | - | - |

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.



ISACA® Budapest Chapter

# Mivel foglalkozunk manapság (ECIIA – RIF2025)






ISACA® Budapest Chapter

# ISO tanúsítás vs. IIA normák szerinti belső audit

| | ISO tanúsítási módszerek | IIA Normák szerinti belső audit |
|---|---|---|
| **Cél** | Az ISO tanúsítás célja, hogy biztosítsa a szervezet megfelelését a nemzetközi szabványoknak, és javítsa a folyamatok hatékonyságát és minőségét. | Az IIA normák szerinti belső audit célja, hogy értékelje és javítsa a szervezet kockázatkezelési, ellenőrzési és irányítási folyamatait. |
| **Fókusz** | A folyamatok és rendszerek megfelelőségének és hatékonyságának értékelése a szabványok szerint. | A külső és belső, pénzügyi és nem pénzügyi riportok megbízhatósága és megfelelősége, az üzleti folyamatok, projektek hatékonysága és eredményessége.<br>A vonatkozó jogszabályoknak, belső szabályozóknak, szerződéseknek való megfelelés |
| **Módszertan** | Részletes dokumentáció és bizonyítékok gyűjtése, auditálás és értékelés a szabványoknak való megfelelés érdekében. | Szisztematikus és független értékelés, amely magában foglalja a kockázatok azonosítását és a kontrollok hatékonyságának vizsgálatát. |
| **Audit típusok** | Első, második és harmadik fél általi auditok. (ISO 19011 szerint) | Bizonyosságot adó audit és tanácsadás |
| **Eredmény** | Tanúsítvány, belső audit jelentés, amely igazolja a szabványoknak való megfelelést. | Jelentés, amely javaslatokat, ajánlásokat tartalmaz a folyamatok javítására és a kockázatok kezelésére. |
| **Időzítés** | Az ISO tanúsítási folyamat előre meghatározott időközönként történik.<br>(3 évente tanúsítás, évente felügyeleti audit) | A belső auditok gyakorisága a szervezet igényeitől függően változhat, de általában rendszeres időközönként kerülnek végrehajtásra. |
| **Függetlenség** | Az ISO tanúsítást független, akkreditált szervezetek végzik. | A belső auditokat a szervezet belső audit csapata végzi (illetve megbízott külsős) |
| **Kockázatkezelés** | Az ISO tanúsítás során a kockázatkezelés a szabványoknak való megfelelés részeként kerül értékelésre. | Az IIA normák szerinti belső audit a kockázatkezelési folyamatok hatékonyságának értékelésére összpontosít. |

ISACA® Budapest Chapter


# KÖSZÖNJÜK A FIGYELMET!