AJÁNLÁS a COSO kockázatkezelési keretrendszer alkalmazására

2023. szeptember

Belső Ellenőrök Magyarországi Közhasznú Szervezete

30 BEMSZ ALAPÍTVA: 1992.

A BELSŐ ELLENŐRÖK MAGYARORSZÁGI KÖZHASZNÚ SZERVEZETE (BEMSZ) KOCKÁZATKEZELÉSI ÁLLANDÓ BIZOTTSÁGA:

Smohay Ferenc CIA, CISA	– ABT Hungária Tanácsadó Kft., partner, BEMSZ elnök
Doszpod Dénes MBA	– RiGoCon Kft., ügyvezető, BEMSZ elnökségi tag, a Bizottság vezetője
Baki László CIA, CCSA	– Magyar Nemzeti Bank, kiemelt vezető auditor
Bánhegyi Réka CIA	– Magyar Nemzeti Bank, vezető auditor
Demjénné Gyöngy Judit	– Generali Biztosító, adatirányítási vezető
Geiszlinger Árpád CIA, CMIIA, CRMA	– BEMSZ elnökségi tag
Simon-András Henrietta CIA	– MOL Nyrt. belső ellenőr

I. BEVEZETÉS, TÉMAFELVETÉS 2

II. A COSO ÁTFOGÓ KOCKÁZATMENEDZSMENT KERETRENDSZERÉNEK BEMUTATÁSA 3

III. AZ ALAPELVEK BEMUTATÁSA 8
III.1. Vállalatirányítás és kultúra 9
III.2. Stratégia és célkitűzések 10
III.3. Teljesítmény 11
III.4. Felülvizsgálat és módosítás 13
III.5. Információ, kommunikáció és jelentések 15

IV. A BELSŐ ELLENŐRZÉS HELYE ÉS SZEREPE 16

V. ÖSSZEFOGLALÓ 19

I. Bevezetés, témafelvetés

Az utóbbi években megélt globális és makroszintű események - legyenek azok egészségügyi, társadalmi vagy gazdasági indíttatásúak - rendkívüli módon alakították át (és alakítják ma is) a vállalatok kockázati profilját, egyben azok belső dinamikáját. A pandémia, a beszerzési láncok időszakos fennakadása, az energiaválság, az ukrajnai háború, a pénzpiaci likviditás kiszáradása, az állami beavatkozások, az infláció vagy a volatilis árfolyam, mind-mind velünk élő „élmények". Korábban az ún. Fekete hattyú (nem várt módon bekövetkező és drámai következményekkel járó) gazdasági jelenségekre úgy tekintettünk, mint rendkívül ritka eseményekre, viszont az elmúlt 3 évben ez a jelenség szinte a mindennapok részévé vált, de legalábbis sokkal gyakrabban üti fel a fejét. Mindeközben az előttünk álló fejlődés és kihívások – csak hogy néhányat említsünk: az ESG-szempontok, a munkahelyi kultúra, a digitalizáció, a robotika vagy a mesterséges intelligencia – napról napra kikényszerítik az előre gondolkodást és az innovatív fejlesztéseket az ellenálló képesség folyamatos fenntartása mellett.

Ennek eredményeként a kockázatok értelmezése és megközelítése még inkább stratégiai jelentőségre tesz szert. Mostantól már végképp nem tekinthetünk rá úgy, mint egyfajta delegált és silóban kezelt feladatra, ezzel szemben olyan integrált tevékenységként kell működtetni, ami egyszerre és láthatatlanul épül be a vállalatirányítás minden aspektusába, az operatív mindennapokba és a szervezeti kultúrákba. A különböző kockázati tényezők összefüggenek egymással, a külső és belső hatások át- és átjárják a folyamatokat, a rendszereket és a szervezeti egységeket.

Az említett tapasztalatok, kihívások és menedzsment-igények ugyanakkor jótékonyan hatnak vissza a kockázat-kontroll területek szakmai fejlődésére is. Jelen ajánlással az a célunk, hogy hozzájáruljunk ehhez a folyamathoz a *COSO ERM 2017 - Integrált*

Kockázatmenedzsment Keretrendszer[1] bemutatásán és értelmezésén keresztül. Tisztában vagyunk vele, hogy a Keretrendszer egy komplex iránymutatás, aminek teljeskörű implementációja méretgazdaságot feltételez, ugyanakkor elegendő rugalmassággal rendelkezik ahhoz, hogy bármely szervezet a saját képére formálja, a megfelelő pontokon és hangsúllyal. Teheti ezt akár egyes elemek kiemelésével más szempontok figyelmen kívül hagyása mellett, összességében mégis hozzáadott értéket teremtve a szemlélet és a gondolkodásmód szervezeten belüli elterjesztésével.

II. A COSO átfogó kockázatmenedzsment keretrendszerének bemutatása

ELŐZMÉNY

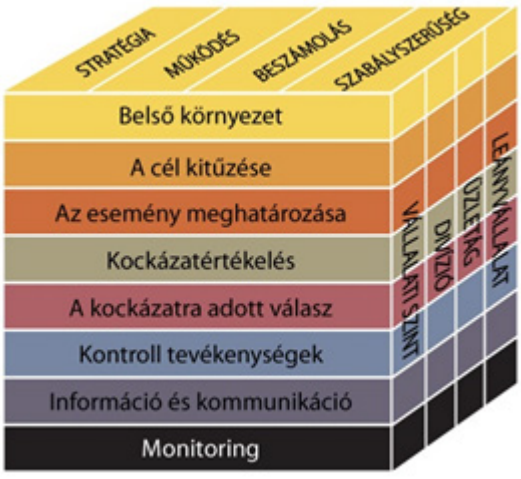
A COSO-t (Committee of Sponsoring Organizations of the Treadway Commission) 1985-ben alapították az Egyesült Államokban azzal a céllal, hogy szakmai oldalról támogassa a csalárd pénzügyi jelentések kivizsgálásával a törvényhozás által létrehozott bizottságot. A Treadway Commission feladata volt, hogy feltárja az okokat, amelyek a hamis beszámolókhoz vezettek, illetve ajánlást dolgozzon ki a belső kontrollok hatékonyságnak és a jelentések megbízhatóságának javítása érdekében. A COSO alapítói olyan szervezetek voltak[2], amelyek az amerikai gazdasági közösséghez tartoztak és fontos szerepet játszottak az üzleti tevékenység, a pénzügyi szabályozás és az ellenőrzés terén, akik mellett részt vettek a független bizottságban az ipar, a pénzügyi szolgáltatások, a könyvvizsgálók, a befektetési vállalkozások és a New York-i tőzsde képviselői is.

Az 1992-ben egységes formában kiadott COSO Belső kontroll keretrendszer (COSO Internal Control Framework) volt az első olyan kezdeményezésük, amely széles körben gyakorlati alkalmazásra került. A dokumentum iránymutatást adott a vállalatoknak a belső kontroll kialakításában és értékelésében, segítette az érintett felek (például a vállalatvezetés, a tulajdonosok és befektetők) döntéshozatalát a célok elérésében, a törvényi előírásoknak való megfelelésében és a megbízhatóbb pénzügyi jelentések kibocsátásában. A keretrendszer különösen nagy súlyt kapott a Sarbanes-Oxley törvény elfogadását követően a 2000-es évek elején, amikor nagy szükség volt a tőkepiaci bizalom visszaszerzésére a sorozatos vállalati botrányok után.

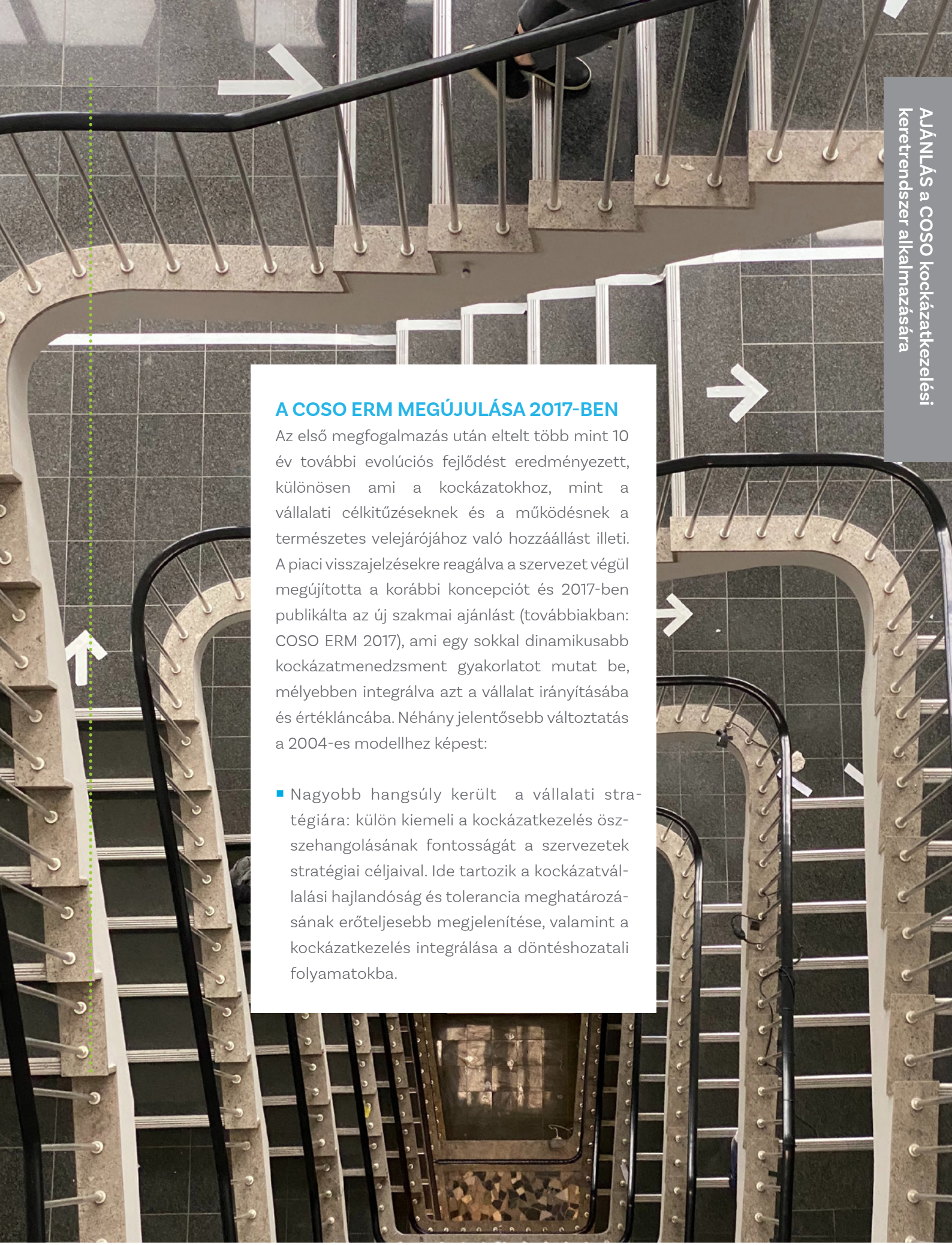
[1] A "kockázatmenedzsment" (risk management) a magyar szaknyelvben "kockázatkezelés" kifejezésként honosodott meg, ami félreértésekre adhat okot a folyamatokba ágyazott és operatív válaszlépéseket jelölő tevékenységek ugyanezen szóval illetett elnevezése okán (risk treatment). Jelen ajánlásban nem célunk ennek részletes magyarázata és tisztázása, az egyszerűség kedvéért a "kockázatmenedzsmentet" és a "kockázatkezelést" egymás szinonimáiként használjuk a vállalatirányítás részét képező, stratégiai szintű keretrendszer tekintetében.

[2] American Institute of Certified Public Accountants (AICPA) - Könyvvizsgálók Amerikai Intézete, American Accounting Association (AAA) - Amerikai Könyvelési Egyesület, Financial Executives International (FEI) - Pénzügyi Vezetők Nemzetközi Szervezete, Institute of Internal Auditors (IIA) - Belső Ellenőrök Intézete és az Institute of Management Accountants (IMA) - Vezetői Könyvelők Intézete

Az idő előrehaladtával világossá vált, hogy belső kontrollok koncepciója bár szükséges, de nem elégséges feltétele a kockázatok átfogó és a vállalat minden elemét integráló menedzselésének. Ez vezetett a COSO következő jelentős kezdeményezéséhez, az ERM (Enterprise Risk Management) 2004-es keretrendszerének kiadásához, ami pontosította és elmélyítette a kockázatkezelési folyamatot, annak céljait, valamint a szervezeti érintettség számos aspektusát. A szakmában sokak által ismert az ún. „COSO-kocka" ennek a keretrendszernek a vizuális ábrázolását tette lehetővé (1. ábra):



1. ábra



A COSO ERM MEGÚJULÁSA 2017-BEN

Az első megfogalmazás után eltelt több mint 10 év további evolúciós fejlődést eredményezett, különösen ami a kockázatokhoz, mint a vállalati célkitűzéseknek és a működésnek a természetes velejárójához való hozzáállást illeti. A piaci visszajelzésekre reagálva a szervezet végül megújította a korábbi koncepciót és 2017-ben publikálta az új szakmai ajánlást (továbbiakban: COSO ERM 2017), ami egy sokkal dinamikusabb kockázatmenedzsment gyakorlatot mutat be, mélyebben integrálva azt a vállalat irányításába és értékláncába. Néhány jelentősebb változtatás a 2004-es modellhez képest:

- Nagyobb hangsúly került a vállalati stratégiára: külön kiemeli a kockázatkezelés összehangolásának fontosságát a szervezetek stratégiai céljaival. Ide tartozik a kockázatvállalási hajlandóság és tolerancia meghatározásának erőteljesebb megjelenítése, valamint a kockázatkezelés integrálása a döntéshozatali folyamatokba.

- A kockázat definíciója is módosult: az új keretrendszer már nem kizárólagosan kedvezőtlen jelenségként tekint rá, hanem elismeri, hogy a kockázat bekövetkezése jelenthet pozitív hatást is a vállalat céljaira vonatkozóan. Továbbra is a kockázatok körébe értjük a stratégiai, üzleti, pénzügyi jelentéstételi és megfelelési kockázatokat, kiegészülve a távoli jövőre vonatkozó ún. feltörekvő kockázatokkal.
- A kultúra és a vállalatirányítás szerepének kiemelése: a keretrendszer a korábbinál is mélyebben részletezi a kockázattudatosság és felelősségvállalás kultúrájának kialakítását, az irányító testület és a felsővezetés szerepét a kockázatkezelés felügyeletében.
- A technológiai környezet külön részletezése: a digitalizáció megjelenése a kockázatkezelésben, ideértve a kiberbiztonsági és más technológiai kockázatokkal kapcsolatos kihívások kezelését is.

A keretrendszer kiadását követően a COSO és az azt támogató szervezetek (mint pl. The IIA) számos gyakorlati útmutatót is megfogalmazott, amik hasznos források lehetnek a kockázatmenedzsment keretrendszert bevezetni és alkalmazni kívánó szervezetek számára. Az alábbiakban néhány példa a mindenki számára szabadon elérhető ajánlások közül[3]

- környezeti, társadalmi és vállalatirányítási (ESG) kockázatok (2018)
- kiberkockázat (2019)
- értékteremtés és -megőrzés az ERM 2017 bevezetésével (2020)
- kockázatvállalási hajlandóság (2020)
- megfeleltetési kockázat (2020)
- felhő alapú számítástechnika (2021)
- mesterséges intelligencia (2021)
- agilis szervezet (2022)

A COSO ERM 2017 ÉS A COSO INTEGRÁLT KONTROLL KERETRENDSZEREK KAPCSOLATA

A két koncepció, lényegüket és tartalmukat tekintve számos eltérést mutat, ugyanakkor szakmai szempontból kapcsolódnak egymáshoz, így jól kiegészíthetik egymást egy-egy szervezet kockázatkezelési és belső kontroll erőfeszítéseiben.

A COSO Integrált Kontroll (IC) Keretrendszer arra nyújt iránymutatást, hogyan lehet hatékony belső kontroll folyamatokat tervezni és megvalósítani egyes kiemelt kockázati témákban. Ezzel szemben, ahogy az láthatóvá válik a továbbiakban, a COSO ERM 2017 egy szervezet kockázatkezelési folyamatainak tervezéséről, megvalósításáról és értékeléséről szól. Amíg az IC dedikáltan a pénzügyi jelentésekre, a megfelelésre és a hatékonyságra ható kockázatok belső ellenőrzési folyamataira összpontosít, addig az ERM 2017 már nem szűkíti le a kockázati univerzumot, hanem lehetővé teszi, hogy a szervezet azonos alapokra helyezze és egységesen menedzselje az összes kockázatot, amivel szembesülhet.

A két keretrendszer logikai kapcsolata úgy fogalmazható meg, hogy miközben a hatékony kockázatkezelési folyamatok egyben erős belső kontrollokat igényelnek (lévén azok egyik eszköze), addig a stabil kontrollkörnyezet

[3]https://www.coso.org/guidance-erm

és kontroll tevékenységek vissza is hatnak a veszélyforrások felismeréséhez, bekövetkezésük valószínűségének és/vagy hatásainak csökkentéséhez. A COSO ERM 2017 tartalmazza a kontroll rendszer fogalmát az összetevői között, míg az IC a kontroll tevékenységek céljai között kiemeli az üzleti folyamatokkal és a pénzügyi jelentésekkel kapcsolatos kockázatkezelési tevékenységhez való hozzájárulást. A COSO ERM 2017 a „Teljesítmény" komponens „13. Kockázati válaszok meghatározása" című alapelvének kifejtésében közvetlenül is meghatározza a kapcsolódási pontot az IC keretrendszerhez.

A COSO ERM 2017 SZERKEZETE ÉS TARTALMA

2. ábra

A COSO ERM 2017 öt kulcsfontosságú komponensből áll (2. ábra):

1. **Vállalatirányítás és kultúra:** ez a komponens hangsúlyozza a kockázat-tudatos kultúra létrehozásának fontosságát a szervezetben, valamint biztosítja a kockázatkezelés integrálását a szervezet irányítási struktúrájába.

2. **Stratégia és célkitűzések meghatározása:** arra összpontosít, hogy a szervezet kockázatkezelési tevékenységeit összhangba hozzák az általános stratégiai célokkal és célkitűzésekkel.

3. **Teljesítmény:** arra fókuszál, hogy a szervezet minden szintjén figyelje és kezelje a kockázatokat és olyan mutatókat határozzon meg, amelyekkel nyomon követheti a kockázatok változását.

4. **Felülvizsgálat és módosítás:** kiemeli, hogy rendszeresen felülvizsgálják és frissítsék a szervezet kockázatkezelési politikát és eljárásait, és szükség szerint módosítsák azokat a gazdasági környezet változásainak tükrében.

5. **Információ, kommunikáció és jelentés:** kifejti a kockázati információk hatékony kommunikációjának és jelentésének fontosságát a szervezeten belül, illetve azon kívül, a külső érdekeltek irányában.

III. Az alapelvek bemutatása

A COSO a fenti öt komponenst 20 további alapelvben bontja ki a kockázatmenedzsment megszervezésére, működtetésére és felügyeletére vonatkozó praktikus ajánlások céljából (3. ábra).

3. ábra

Az új modell implementációjára a legjobb gyakorlatok a moduláris (azaz: az alapelvek kiválasztott csoportjainak időben eltolt) bevezetés irányába mutatnak, ezért ismerkedjünk meg ezekkel az alapelvekkel kicsit részletesebben.

III.1.
VÁLLALATIRÁNYÍTÁS ÉS KULTÚRA

A "Vállalatirányítás és kultúra" komponens annak a fontosságát hangsúlyozza, hogy a szervezetben alakuljon ki egy olyan kockázattudatos kultúra, amely az irányítási mechanizmusokba integrálja a kockázatkezelést, ösztönzi a folyamatos fejlődést és úgy tekint a kockázatkezelésre, mint a teljesítmény és a siker kulcsfontosságú hajtóerejére. Ez a komponens felismeri, hogy egy erős és pozitív kockázati kultúra elengedhetetlen a hatékony vállalati kockázatkezelési program sikeres bevezetéséhez és működtetéséhez, tovább azt, hogy a vezetőkre kulcsszerep hárul ebben. Ezáltal a szervezet olyan környezetet teremthet, ahol a kockázatkezelés a siker kulcsfontosságú tényezőjeként van jelen, nem pedig akadályként. Ez segíthet biztosítani, hogy a vállalat jobban tudja azonosítani, értékelni és hatékonyan kezelni a kockázatokat, ami javítja a teljesítményt és növeli a rugalmasságot a bizonytalanságokra adott válaszok során. Az idetartozó alapelvek a következők:

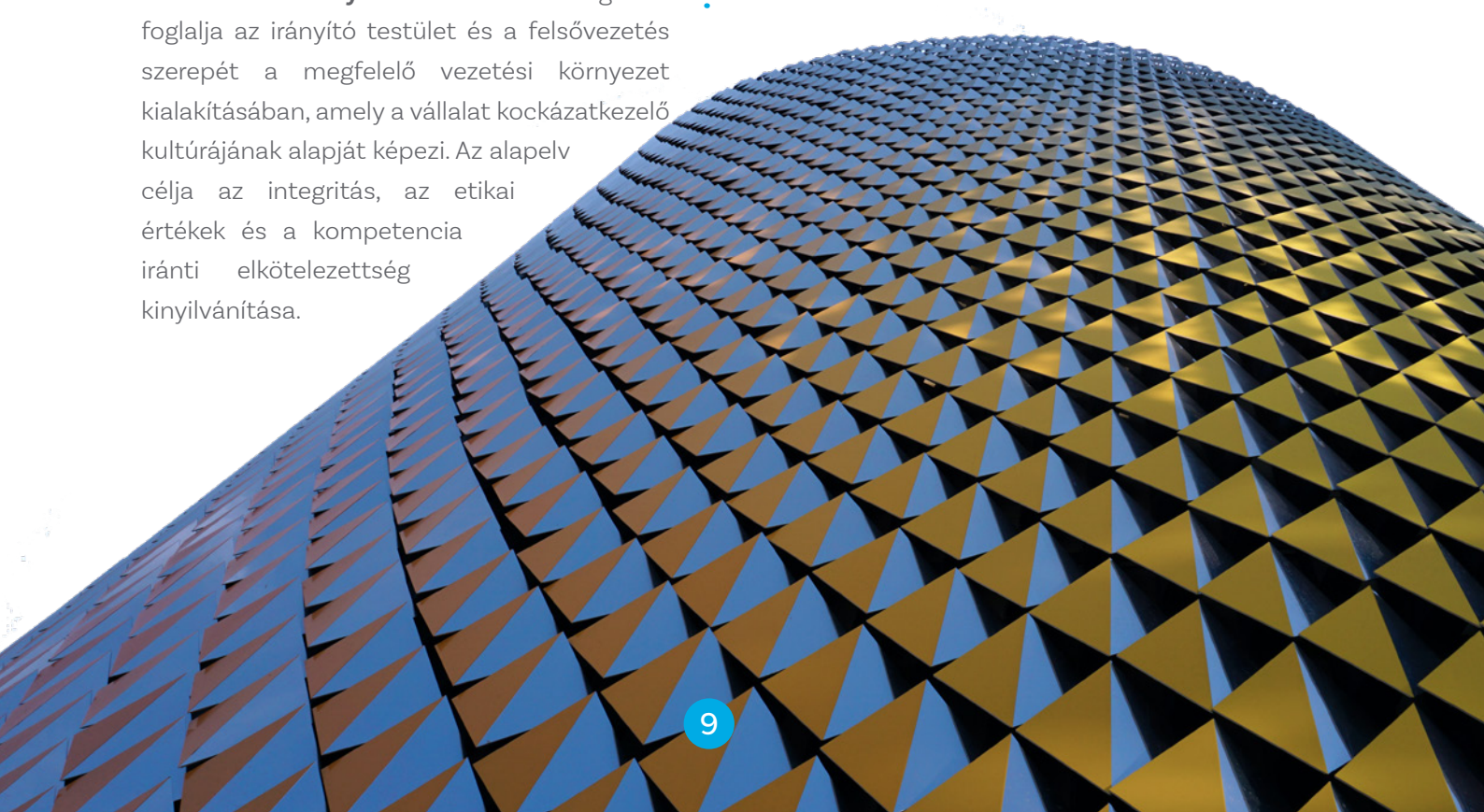
1. A vezetői környezet kialakítása magában foglalja az irányító testület és a felsővezetés szerepét a megfelelő vezetési környezet kialakításában, amely a vállalat kockázatkezelő kultúrájának alapját képezi. Az alapelv célja az integritás, az etikai értékek és a kompetencia iránti elkötelezettség kinyilvánítása.

2. A működési struktúra kialakítása kifejti a megfelelő irányítási struktúra kialakítását, a kockázatkezelési szerepek és felelősségek meghatározását, valamint hatékony kockázatkezelési politikák és eljárások kidolgozását.

3. A kívánt kultúra meghatározása hangsúlyozza a kockázatkezelő kultúra meghatározásának fontosságát, amelyet összehangolnak a szervezet értékeivel, céljaival és stratégiájával. Olyan környezet létrehozását célozza meg, amelyben értékelik a kockázatkezelést és integrálják azt az intézmény döntéshozói folyamataiba.

4. Az alapvető értékek (integritás, átláthatóság és felelősségvállalás) iránti elkötelezettségnek része az etikai kódex létrehozása, annak oktatása minden dolgozó részére, valamint az alapvető értékeknek való megfeleltetés mérése.

5. Tehetséges munkatársak felvétele, fejlesztése és megtartása, melynek célja egy tehetségmenedzsment stratégia kidolgozása, amely azonosítja és fejleszti a kockázatkezeléshez szükséges készségeket, egyben biztosítja a szervezet kockázatkezelési tevékenységeinek támogatásához szükséges erőforrásokat.



III.2.
STRATÉGIA ÉS CÉLKITŰZÉSEK

Fontos üzenete a COSO ERM 2017-nek, hogy a kockázatmenedzsment már a stratégiaalkotás és a célkitűzés során elkezdődik. A helyes, felelős és jövőbetekintő hozzáállás a vállalatvezetés részéről nem merül ki abban, hogy csupán a már eldöntött stratégiai és hozzájuk kapcsolódó operatív célok vonatkozásában felmerülő kockázatokat menedzseljük, hanem az, hogy a kockázattudatosság eleve beépül azok meghatározásába. Az új keretrendszerben a stratégia és a célok kijelölésének alapelvei a következők:

6. Az üzleti összefüggések (körülmények) elemzése: a szervezetnek mérlegelnie kell a különböző trendeket, a külső és belső környezetet, az érintettek érdekeit, illetve egyéb, a célok elérését befolyásoló információk kockázati profilra (azaz a kockázatok számosságára és mértékére, típusaira és eloszlására a szervezeten, illetve az egyes kockázati kategóriákon belül) gyakorolt potenciális hatását. Ennek keretében ajánlott az alábbi területek áttekintése, akár PESTEL[4] elemzéssel:

- vevőigények modellezésének megfelelősége;
- az ellátási lánc teljesítménye határidő és költségkeret tekintetében;
- új versenytársak megjelenésének esélye;
- az ellátandó feladat(ok)hoz kapcsolódó technológiai infrastruktúra megfelelősége, színvonala.

[3]https://www.coso.org/SitePages/Guidance.aspx

7. A kockázatvállalási hajlandóság meghatározása: melyet az értékteremtés, -megőrzés és -realizálás keretein belül, azokat szem előtt tartva kell megtenni. A kockázatvállalási hajlandóság mértékét a következő tényezők befolyásolják:

- a szervezet jelenlegi kockázati profilja;
- kockázat-befogadóképesség: a kockázatok azon maximális szintje, amit a szervezet el tud viselni céljai megvalósítása során;
- kockázati tűrőképesség/tűréshatár: a kockázat elfogadható szintje, illetve annak elfogadható mértékű ingadozása, melyet az adott szervezet céljai megvalósítása során vállal;
- kockázati attitűd: a szervezet hozzáállása, állásfoglalása a növekedéshez és a megtérüléshez, illetve az ezekkel járó kockázatokhoz;
- a menedzsment képességei és fejlettségi szintje.

Egyes szervezetek a kockázatvállalási hajlandóságot kvalitatív alapon írják le, mások inkább mérőszámokkal fogalmazzák meg. Mindkét eset lehet jó megoldás, a lényeg, hogy összhangban legyenek a kockázatelemzés és -értékelés, illetve a kockázati mutatókhoz és határokhoz használt módszertani megközelítéssel. A kockázatvállalási hajlandóság a körülmények hatására változhat, ezért időről időre felül kell vizsgálni.

8. Az alternatív stratégiák elemzése: a szervezetnek meg kell vizsgálnia a lehetséges stratégiai elképzeléseket és azok kockázati profilját. A stratégiai elképzelések kialakítása és a megfelelő stratégia kiválasztása (melyek során a menedzsment és az igazgatóság szorosan együttműködik) végső soron egy optimalizálási és kompromisszumkötési feladat a kockázatvállalási hajlandóság, a rendelkezésre álló erőforrások és a vágyott növekedés/nyereség hármasa között. Ezen a ponton érdemes figyelembe venni, hogy minden szervezetnek egyre nagyobb mértékű változékonysággal és komplexitással kell szembenéznie. Az olyan jelenségek és trendek, mint az adatalapú folyamatirányítás vagy az automatizáltság és a mesterséges intelligencia terjedése mindenképpen hatással vannak az egyes szervezetek kockázatmenedzsmentjére és stratégia-alkotására is, ráadásul eredményes válaszlépéseket és gyors döntéshozatalt követelnek meg. A stratégiának összhangban kell lennie a szervezet missziójával és alapvető értékeivel, amelyek jelentőségét nem lehet alábecsülni egy gyorsan változó világban, hiszen megalapozzák a szervezetek ellenállóképességét (rezilienciáját). Ezen túl a választott stratégiának igazodnia kell a kockázatvállalási hajlandósághoz is.

9. Az üzleti célok meghatározása: a szervezet a stratégiai elképzelésekkel és tervekkel összhangban alakítja ki és bontja le különböző szintekre az üzleti, operatív célokat, melynek során az egyes üzleti célokhoz kapcsolódó konkrét kockázatok meghatározására is szükség van. Egy jól megfogalmazott operatív céltól elvárás, hogy konkrét, mérhető vagy megfigyelhető, továbbá elérhető és releváns legyen. A szervezet jövője és növekedése szempontjából nélkülözhetetlen, hogy az üzleti célok szorosan beilleszthetők legyenek a stratégiai célok egyes kategóriáiba (pl. piaci részesedés, vevő fókusz, társadalmi felelősségvállalás stb.). Szintén kulcsfontosságú, hogy az üzleti célok elérésének mérése, nyomon követése megvalósuljon, amelyet meg kell előznie a kívánt teljesítmény(ek) és célértékek, valamint a hozzájuk kapcsolódó kockázati tolerancia szintek meghatározásának.

III.3. TELJESÍTMÉNY

Az ajánlás ezen része a klasszikus kockázatazonosítási és -mérési folyamatot fedi le. Az

itt felsorolt, a teljesítményhez kapcsolódó öt alapelv szorosan összekapcsolódik, annyira, hogy az egyik alapelv kimenete a másik alapelv inputjának is tekinthető.

10. A kockázatok azonosítása. Az első lépés, hogy a szervezet leltárba vegye a kockázatait, illetve a korábban azonosított kockázatokról eldöntse, hogy azok relevánsak-e még. Olyan kockázatokat kell azonosítani, amelyek a stratégia és az üzleti célok elérését jelentős mértékben befolyásolják a szervezet kockázati profiljának megváltoztatásán keresztül. Ilyen lehet például egy új technológia megjelenése, az adatelemzés egyre növekvő szerepe, a természeti erőforrások szűkülő rendelkezésre állása, a munkaerő növekvő mobilitása vagy szűkössége, az életvitelben, egészségügyben vagy demográfiában történő változások vagy a politikai környezet változása. A kockázatok számbavétele a napi munka részeként is történhet, de működhet célzott adatelemzésen keresztül is (például a múltban előfordult incidensek elemzésével, illetve kulcskockázati mutatók alkalmazásával), továbbá interjúk, workshopok segítségével. A kockázatok azonosítása egyúttal új lehetőségek azonosítását is jelenti.

11. A kockázatok mértékének értékelése. Mind a kockázatok azonosításakor mind a súlyosságuk meghatározásakor fontos az egységes terminológia használata, a kockázatok csoportosítása, valamint az, hogy a tevékenységet a szervezet minden szintjén el kell végezni – a funkcionális és folyamati-szinttől kezdve a stratégiai célokat érintő kockázatokig. A kockázatok számszerűsítésének leggyakrabban használt mérőszámai a becsült hatás és a gyakoriság (vagy valószínűség). A kockázatértékelésnek lehetnek kvalitatív módszerei (interjú, workshop, benchmarkolás, kérdőív) és kvantitatív megoldásai (pl. valószínűségi modellek, stressztesztek vagy szcenário-analízis), illetve ezek hibrid formái. A kockázatértékelés során – a kockázati intézkedések bevezetése előtti – az eredendő (inherens) kockázatból kell kiindulni, meg kell határozni a maradvány (reziduális) kockázat értékét, majd a kettőt összevetve el lehet dönteni, hogy milyen kockázatkezelési stratégiák és válaszlépések vezethetnek a kívánt eredményre. A felmérés eredményének plasztikus ábrázolása végett javasolt ún. hőtérképen ábrázolni, a hatás és a gyakoriság koordinátarendszerében feltüntetve a kockázatokat.

12. A kockázatok rangsorolása. A kockázatok priorizálására azért van szükség, mert a szervezet általában nem rendelkezik annyi erőforrással, hogy az összes kockázatát egyszerre és azonnal a kívánt szintre hozza. Ugyanakkor azokat a kockázatokat mindenképpen csökkenteni kell belátható időn belül, amelyek a szervezet kockázatvállalási hajlandóságának meghaladásával vagy valamely üzleti cél ellehetetlenítésével fenyegetnek. A sorbarendezést így előre lefektetett kritériumok alapján kell elvégezni, mint például a szervezet adott kockázathoz való alkalmazkodóképessége, a kockázatok összetettsége, a kockázat terjedési sebessége és hatásának hossza bekövetkezés esetén, illetve, hogy milyen erőfeszítéseket igényelne a károk helyrehozatala és a normális működés visszaállítása. A módszertan eredményeként elképzelhető, hogy két „közepes" hatásúnak értékelt kockázatnak más sorszámot ad a menedzsment a prevenciós források tervezésekor és a reagálás sorrendjének meghatározásakor.

13. A kockázati válaszok meghatározása. A szervezet vezetése minden azonosított kockázatra készít egy kockázati választ, amelynek során figyelembe veszi a kockázat súlyát, kockázati sorrendben elfoglalt helyét, a kockázati válasz költségét és előnyeit, a kapcsolódó üzleti célt, valamint a kockázatvállalási hajlandóságot. Jellemzően az alábbi öt válaszstratégiából szoktak választani:

- A kockázat elfogadása: ezt általában akkor alkalmazzák, ha a kockázat a kockázatvállalási hajlandóságon belül van.
- A kockázat elkerülése: jelentheti például az adott üzletág értékesítését is vagy egy stratégiai irányváltást.
- A kockázatos tevékenység folytatása: a kockázatot a teljesítmény növelésével tervezi ellensúlyozni a vállalat, de nem elhanyagolva a szükséges felügyeleti kontrollok erősítését.
- A kockázat csökkentése és a kockázat megosztása: például biztosítás vagy fedezeti ügylet kötésével, partnerséggel vagy a kockázatos tevékenység speciálistához való kiszervezésével.

Fontos rámutatni, hogy az adott kockázati válasz megváltoztathatja a szervezet kockázati profilját, és akár új kockázatok, de lehetőségek felmerülését is elősegítheti!

14. Kockázati portfólió nézet kifejlesztése. A kockázatok összesítése és portfólióba rendezése abban segít, hogy a szervezet vezetésének legyen egy összképe a szervezetet érintő (akár egy adott szervezeti egység szintjén azonosított) kockázatok típusáról, súlyosságáról, a kockázatok közötti kapcsolatokról és hogy ezek hogyan járulnak hozzá a szervezet teljesítményéhez. Többféleképpen lehet összesíteni az azonosított kockázatokat, az integrálás szintjétől függően, kezdve az egyedi kockázatok felsorolásától, a kockázatok kategóriákba való rendezésén és az adott üzleti célokhoz kapcsolódó kockázati profilok felállításán át a teljes integrálásig (ami a portfólió alapú megközelítést jelenti). A portfólió-nézet segít megérteni a kockázat és a teljesítmény közötti kapcsolatot, és további elemzésekre is alkalmat ad. A portfólió stresszelése során a vezetőség áttekintheti az egyes kockázatokhoz kapcsolódó feltételezéseknek, illetve az egyedi kockázatoknak stresszhelyzetben kimutatható változásait, a kockázatok közötti függőségeket/kapcsolatokat, valamint a kockázati válaszstratégiák és akciótervek eredményességét; vagyis összességében a szervezet alkalmazkodó képességét.

III.4. FELÜLVIZSGÁLAT ÉS MÓDOSÍTÁS

A szervezeteknek folyamatosan figyelniük kell a külső környezet változásait és ehhez kapcsolódóan felül kell vizsgálniuk az üzleti céljaikat, az azokhoz kapcsolódó stratégiájukat, valamint a kockázatkezelési gyakorlatukat. A

kockázatkezelési tevékenységnek ki kell terjednie a szervezet külső és belső környezetére, az alkalmazott módszereket pedig folyamatosan fejleszteni kell.

15. Lényeges változások értékelése. A kockázatkezelés során a szervezeteknek azonosítaniuk és értékelniük kell azokat a változásokat, melyek jelentősen befolyásolhatják az üzleti célok elérését, valamint a stratégiát. Továbbá meg kell vizsgálniuk, hogy a jelenlegi kockázatkezelési gyakorlatuk még mindig megfelelően támogatja-e üzleti céljaik elérését, szükség esetén pedig módosítaniuk kell azt. Ez azért fontos, mert a megváltozott külső környezet olyan új kockázatok kialakulásához vezethet, amelyek befolyással vannak a stratégia alapjául szolgáló főbb feltételezésekre. Ezen túlmenően a megváltozott külső környezet hatással lehet a szervezetek belső környezetére és kultúrájára is. Ebből kifolyólag a kockázatkezelés során szükség van a külső és belső környezeti változások, valamint a kultúra változásainak azonosítására. A szervezeteknek ki kell alakítaniuk a rendszeres felülvizsgálatok – és szükség esetén módosítások – gyakorlatát, majd azt be kell építeniük az operatív folyamatokba.

16. A kockázatok és a teljesítmény felülvizsgálata. A szervezetek munkájuk során szembesülhetnek azzal, hogy tevékenységüket már nem végzik olyan hatékonyan, mint ahogyan azt tervezték, elvárták és ez kockázatot jelent a teljesítményükre nézve. Ha a menedzsment azt tapasztalja, hogy a vállalat teljesítménye már nem az elvárt mértékű vagy megváltozott a kockázati profil, akkor szervezett módon korrekciós lépéseket kell tennie.

A korrekciós intézkedések mértékének összhangban kell lennie a teljesítménybeli eltérések mértékével, az üzleti célok fontosságával, továbbá figyelembe kell venni a kockázati portfólió megváltoztatásával járó költségeket és hasznokat.

A felülvizsgálat során értékelni kell a szervezet képességeit, valamint azok teljesítményre való hatását. A korrekciós intézkedések közé tartozhat az üzleti célok felülvizsgálata, alternatív stratégiák kialakítása vagy az erőforrások átcsoportosítása.

17. A vállalati kockázatkezelés fejlesztésének elősegítése. Még azok a szervezetek is hatékonyabbá tudják tenni vállalati kockázatmenedzsment rendszerüket, melyeknek ezen tevékenysége alapvetően megfelelő. A hatékonyság javításához fontos, hogy beépítsék az üzletviteli tevékenységükbe a folyamatos értékelések gyakorlatát. Ily módon szisztematikusan azonosítani tudják a vállalati kockázatmenedzsment javítási, illetve fejlesztési lehetőségeit.

A javítási, fejlesztési lehetőségek azonosítását el lehet végezni akár egy-egy területre (funkció, divízió) vagy az értéklánc egy-egy jelentősebb folyamatára koncentrálva, de akár átfogóan, az egész szervezetre vonatkozóan is.

III.5. INFORMÁCIÓ, KOMMUNIKÁCIÓ ÉS JELENTÉSEK

Egy jól működő integrált kockázatmenedzsment rendszer tartalmazza azokat a feltételeket is, amik biztosítják a szükséges információk begyűjtését külső és belső forrásokból, továbbá ezek megosztását a szervezet egészében vertikálisan és horizontálisan egyaránt. Kiemelt fontosságú, hogy ezek az információk és adatok a megfelelő időben és helyen, releváns tartalommal álljanak rendelkezésre, de ugyanúgy kritikus sikertényező, hogy a címzett oldaláról, legyen az a vállalatirányítás bármely szintje, a megfelelő súllyal kerüljön értelmezésre és felhasználásra.

18. Az információk és a technológia felhasználása. A hatékony működéshez elengedhetetlen ezen a területen is a megfelelő információk feldolgozása. Az információkat mind az alaptevékenységekhez, mind a kiépített kontrollok vonatkozásában gyűjteni és értékelni kell annak érdekében, hogy a kockázatok, illetőleg a kockázati kontrollok nem megfelelő működése mielőbb azonosításra kerülhessenek.
Az információkat és a technológiai megoldásokat a kockázatértékelési folyamat valamennyi szakaszában, különösen a korai előrejelző rendszerekben, valamint a vezetők részére készített összefoglaló jelentésekben használni javasolt, így a vállalati célokat veszélyeztető helyzetek időben kezelhetők lesznek. A kockázatkezelésben, a kontrollok értékelésében a technológiai megoldásokat arányosan kell alkalmazni.
Kiemelendő, hogy a kockázatkezeléshez kapcsolódó adatfolyamatok ne kizárólagosan a kockázatkezelés hatás- és feladatkörébe tartozzanak, hanem inherens részét kell képezniük a szervezet működésének.

19. A kockázati információk kommunikációja. A kommunikáció létfontosságú eleme a keretrendszernek. Ennek legtriviálisabb megjelenése a különböző vezetőségi jelentések, de a rendszer működéséhez elengedhetetlen a kockázattudatos viselkedés beépülése a vállalati kultúrába. Ehhez a szervezet minden munkavállalójának, vezetőjének tisztában kell lennie a kockázatok azonosításában, kezelésében betöltött szerepével, melyet a szervezeti szintű és specifikus képzések, tájékoztatók is támogathatnak.
Akkor lesz igazán sikeres a kockázatalapú működés, ha a kommunikáció két-irányú, azaz a követelmények üzleti egységek felé történő kommunikációja mellett ugyanennyire erős a központi kockázatkezelő funkciók felé, az üzleti területektől érkező információ is. Így az elmélet nem szakad el a gyakorlattól, a felmerülő új kockázati esetek beépíthetőek a rendszerbe.
Az időbeli és megfelelő válaszok kialakításához az ún. eszkalációs jelentések kommunikációs formáit is ki kell alakítani.

20. A kockázatokról, a kultúráról és az eredményekről szóló jelentések. A kommunikációhoz szervesen kapcsolódnak az azokról készülő jelentések és riportok különböző formái és gyakorlatai.
A jelentések címzetti köre jellemzően a vezető testületek, a bizottságok, a felső vezetés, az egyes funkciók közép- és alsóbb szintű vezetői. Feladatkörüket figyelembe véve különböző

mélységű és gyakoriságú jelentéseket ajánlott számukra kialakítani.
A vezető testületek számára olyan jelentéseket kell felépíteni, mely az egész kockázatkezelési rendszer átfogó működését, esetleges hiányosságait, fejlesztési területeit mutatják be. Ebbe beleérthetőek a kockázati és kockázati kontroll mutatók értékei, a kockázatkontroll vizsgálatok eredményei, az azokra megfogalmazott intézkedések státuszai, de a kockázattudatosság növelése érdekében elvégzett különböző oktatások eredményei is. A szervezet alsóbb szintjein már egyre részletesebb és az adott területre specifikus információkat tartalmazzák a jelentések.
Ugyanakkor hasznosak lehetnek az egységes, rendszeres, teljes szervezetre kiterjedő és azt elérő jelentéstételi módszerek, kockázati jelentések is. Így minden érintett megismerheti a vállalatára vonatkozó kockázati térképet, annak kritikus pontjait és azonosítani tudja saját szerepét a kockázatok megfelelő kezelésében.

Végül érdemes a jelentésekre, értékelésekre megfelelő, akár IT alkalmazással támogatott dokumentációs rendszert felépíteni, hiszen az incidensek nyilvántartásához, a korábbi időszakok eredményeinek elemzéséhez, a kockázatértékelések és a kockázatkezelési tevékenységek átlátható és elszámoltatható működéséhez ez elengedhetetlen.

IV. A belső ellenőrzés helye és szerepe

A COSO vállalatirányítási alapelvek általában a vállalatok vezetési gyakorlataira, a szervezetek átlátható és hatékony működésére és az ezekre vonatkozó jelentések megbízhatóságára tesznek javaslatot. Mindezekhez a független belső ellenőrzési terület is nagy mértékben hozzá kell, hogy járuljon. Nem véletlen, hogy az IIA kezdetektől képviselteti magát a COSO sztenderdalkotó bizottságában.
Az ERM tekintetében alapvető szerepe az, hogy objektív bizonyosságot nyújtson a kockázatkezelés hatékonyságáról és hatásosságáról. A belső ellenőrök értékteremtésének két legfontosabb módja az, hogy 1) objektív

biztosítékot nyújtanak arra vonatkozóan, hogy a főbb üzleti kockázatokat megfelelően kezelik, és 2) biztosítékot nyújtanak arra vonatkozóan, hogy a kockázatkezelés és a belső ellenőrzési keretrendszer eredményesen működik.
A belső ellenőrzés szakmai gyakorlatának IIA által kiadott, a jelen Ajánlás készítésekor aktuális nemzetközi normáiban (IPPF 2017) megtalálhatóak azok a kapcsolódási pontok, melyeken keresztül a belső ellenőrzési területek segíteni tudják a szervezeteket céljaik elérésében

.

2110 – IRÁNYÍTÁS

A belső ellenőrzési tevékenységnek értékelnie kell az irányítási folyamatot, és megfelelő javaslatokat kell tennie a szervezetirányítási folyamat javítására, hogy elérje a következő célkitűzéseket:

- stratégiai és operatív döntések meghozatala
- a kockázatkezelés és a kontrollok felülvizsgálata
- megfelelő etikai elvek és értékek érvényesülésének elősegítése a szervezetben
- hatékony szervezeti teljesítménymenedzsment és számonkérhetőség biztosítása
- a kockázatokkal és a kontrollokkal kapcsolatos információk hatékony kommunikálása a szervezet megfelelő területei felé
- a vezető testület, a külső és belső ellenőrök, egyéb bizonyosságot szolgáltató szervezetek, valamint a vezetés tevékenységeinek hatékony koordinálása, köztük
- az információk eredményes átadása.

2120 – KOCKÁZATKEZELÉS

A belső ellenőrzési tevékenységnek értékelnie kell a kockázatkezelés folyamatainak hatékonyságát, és hozzá kell járulnia azok javításához.

2600 – A KOCKÁZATVÁLLALÁS KOMMUNIKÁLÁSA

Ha a belső ellenőrzési vezető úgy tapasztalja, hogy a vezetés felvállal egy olyan szintű kockázatot, amely a szervezet szempontjából elfogadhatatlan lehet, akkor ezt meg kell tárgyalnia a felső vezetéssel. Ha a belső ellenőrzési vezető úgy látja, hogy a kérdés megoldásában nem tudnak megállapodásra jutni, akkor az ügyről tájékoztatnia kell a vezető testületet.

A belső ellenőrzés a kockázatkezelés keretrendszerének működéséről nyújtott objektív bizonyosságon túlmenően támogathatja a vezető testületet tanácsadói kapacitásában is a kockázatkezelés területén. A belső ellenőrzés olyan tanácsadási szolgáltatásokat nyújthat, amelyek javítják a szervezet irányítási, kockázatkezelési és ellenőrzési folyamatait, például:

- a belső ellenőrzés által használt eszközök és technikák elérhetővé tétele a vezetés számára a kockázatok és kontrollok elemzése érdekében;
- a szervezetre vonatkozó általános ismereteinek felhasználásával, valamint a kockázatkezelés és kontrollok terén meglévő tapasztalatának kihasználásával az ERM bevezetésében aktív részvétel;
- tanácsadás, workshopok szervezése, a szervezet segítése és fejlesztése a kockázatok és kontrollok megértésében, valamint a közös nyelvezet, keretrendszer és a kockázatkezelés kialakításának előmozdítása;
- a kockázatok koordinálásának, nyomon követésének és jelentésének központi elemeként (motorjaként) való fellépés; és
- a vezetők támogatása a kockázatcsökkentés legjobb módjának azonosításában.

A fenti szolgáltatások megkezdése előtt tisztázni kell, hogy a tanácsadási feladatok összeegyeztethetők-e a bizonyosságot nyújtó szereppel, illetve világossá kell tenni, hogy a belső ellenőr *alap esetben* nem vállal menedzsment szerepet és felelősséget.

Mindezek mellett is előfordulhat, hogy a belső ellenőrzési vezető felkérést kap a felső vezetéstől, hogy ideiglenesen vagy tartósan ellássa a kockázatmenedzseri szerepet, ami – nem megfelelő előkészítés esetén - csorbíthatja a belső ellenőrzés szervezeti függetlenségét és objektivitását. Ezért az ilyen esetben a „1112 – A belső ellenőrzési vezető feladatai a belső ellenőrzésen túl" című norma alapján kell eljárni. E szerint az irányító testület felülvizsgálati szerepe biztosíthatja és kezelheti a szituációt úgy, hogy rendszeresen felülvizsgálja a belső ellenőrzési vezető tevékenységét mindkét kapacitásában és alternatív intézkedéseket alkalmaz (pl. külső fél bevonását az objektív bizonyosság megszerzésére a kockázatkezelés területén).

Összefoglalva: a belső ellenőrzésnek az is hozzáadott értéke a COSO ERM 2017-es keretrendszer tükrében, hogy vizsgálja és értékelje a stratégiai és operatív célok meghatározásának és a kockázatkezelésnek a folyamatait (hatékonyság, eredményesség, gazdaságosság, megfelelőség szempontjából), azok kapcsolódásait illetve összhangját, e két téma dinamikáját (változások követése, felülvizsgálatok/intézkedések megtétele), a kapcsolódó információáramlás megfelelőségét, a teljesítmények elérését, valamint az ezekről készített beszámolók hitelességét.

V. Összefoglaló

Az integrált kockázatmenedzsment lényege tehát, hogy részévé válik a szervezet irányításának, végig kíséri az értékláncot a stratégiaalkotástól kezdve a tevékenységről szóló belső és külső beszámolókig. Túlmutat az egyes szervezeti egységeken, folyamatokon és védelmi vonalakon, ezért minden eleme fontos és hangsúlyos. Ugyanakkor az alkalmazásánál ügyelni kell a szervezeti és környezeti sajátosságokra, a költség-haszon elv érvényesülésére és a közös megértésre, az elfogadásra. Ha ezek a szempontok háttérbe szorulnak, akkor megnő a veszélye, hogy az értékteremtés helyett egy bürokratikus rutinná válik, jelentős erőforrások lekötése mellett. Az alábbi néhány példa is erre az eredményre vezethet, pusztán a helytelen értelmezésből fakadóan:

- Az ERM azonosítása egy funkcióval vagy szervezeti egységgel, ami a kockázatokkal kapcsolatos felelősségek áthárításához vezet.
- Az ERM végeredménye egy kockázati lista, ugyanakkor hiányoznak a mélyebb információk a kockázatok belső függőségeiről a folyamatok, a szervezetek és a rendszerek között, továbbá a konkrét fejlesztési tervekről.
- Az ERM adatbekérésekre összpontosít anélkül, hogy kialakulna egy közös megértésen és motiváción alapuló, a valós működési dilemmákat átfogó együttműködés a védelmi vonalak között.
- Az ERM outputja egy színes jelentésre korlátozódik, vagyis a menedzsment pillanatfelvételeket kap a kockázatok állapotáról, ugyanakkor nem tudatosítja sem saját szerepét és felelősségét, sem azokat a szervezeti feladatokat, amelyek egy élő és minden ízében a működéshez kapcsolódó kockázatkezeléshez szükségeltetnek.

A COSO ERM nem egy szabályrendszer, ami univerzálisan és teljeskörűen előírja a kockázatmenedzsment egyetlen és kötelező megvalósítási formáját. Valójában úgy kell tekinteni rá, mint legjobb gyakorlatok egyfajta egységes rendszerére, aminek ésszerű, a szervezeti specifikumokat is tükröző testreszabásával tovább tudjuk erősíteni a vállalat ellenállóképességét, biztosítva a célok elérését és a növekedést. A helyes értelmezés és megközelítés lehetővé teszi, hogy vállalati mérettől, fejlettségi szinttől és komplexitástól függetlenül fel lehessen használni.

A megújított COSO ERM keretrendszer 2017 óta óta bizonyította aktuálisát, szakmailag elfogadott és világszerte bevezetett módszer, egyre több stratégiai és kockázati téma kapcsán nyúlnak hozzá, mint vezérfonalhoz. Ezért tartjuk aktuálisnak a témakör mélyebb megismerését és az alkalmazás megfontolását, és erre bíztatunk mindenkit, függetlenül attól, hogy egy szervezetben hol és milyen szerepet tölt be a kockázatok menedzselésének folyamatában.