# A BIZTONSÁG HÁLÓZATA – A KONTROLLOK BIZTONSÁGI HÁLÓZATA

Kemendi Ágnes

**Absztrakt:** A hálózatok, valamint a hálózatszerű működés napjaink meghatározó jelenségeivé váltak. Ezzel párhuzamosan a vállalatok az ipar 4.0, ill. 5.0 korszakában komplex biztonsági kihívásokkal szembesülnek, melyek a vállalatoktól megkövetelik a hosszú távú sikeresség érdekében, hogy megfelelő biztonsági rendszerrel rendelkezzenek. A kutatás ezt a két témát ötvözi; célja a vállalatok biztonsági hálózatát képező elemek meghatározása. A kvalitatív kutatási módszertanon alapuló kutatás a Magyarországon működő autóipari vállalatok éves beszámolóinak feldolgozásán és elemzésén alapul. A kutatás eredményei összhangban vannak a szakirodalmi elemzés alapján azonosított előzetes várakozásokkal. A biztonsági hálózat a kockázatkezelés eredménye; biztonságot ad, és funkciója, amennyiben hiba is akad a folyamatokban, nem engedi, hogy az bekövetkezzen, illetőleg biztosítja, hogy az esetleges hibahatások elfogadható mederben maradjanak. A hálózatszerű működés megjelenik a vállalati biztonsági rendszerekben. A biztonság hálózatának megteremtéséhez kontrollok szükségesek, és az „kemény", és „lágy" elemekből áll. A kontrollhálózat meghatározó tartópillérei az információs és kommunikációs technológiák, IKT rendszerek, és a rendszereket működtető emberek. A vállalati folyamatok hálózatába épített kontrollok a belső kontrollrendszer építőkövei.

**Abstract:** Networks, including operations functioning as networks, are today's defining phenomena. In parallel, industry 4.0 and 5.0 era's companies face complex security challenges requiring companies to have proper security systems in place for long-term corporate success. Research combines these themes and aims to explore and to identify the elements of organizations' safety-net. Qualitative research methodology is based on the processing and analysis of annual reports of automotive companies operating in Hungary. Research results are in line with preliminary expectations identified based on literature analysis. Safety-net is the result of risk management and provides security. Even when a fault or incident occurs in a process, the safety-net prevents its occurrence or ensures its effects are within an acceptable range. Enterprise security systems are characterized by network-like operation. Creating a safety-net requires controls which consists of "hard" and "soft" elements. Key pillars of control network are the information and communication technologies (ICT), systems and the people operating those systems. Controls built into the network of corporate processes are the building blocks of the internal control system.

*Kulcsszavak:* vállalati belső kontroll, kontrollok biztonsági hálózata, vállalati biztonság

*Keywords:* corporate internal control, security network of controls, corporate security

## 1. Bevezetés

A vállalatok a folyamatosan változó üzleti környezetben komplex biztonsági kihívásokkal szembesülnek. Az ipar 4.0, és 5.0, a digitalizáció, a digitális transzformáció, ill. a nem várt események, mint a COVID-19 pandémia a kockázatkezelési folyamat jelentőségét még kritikusabbá teszik (pl.: emelkedett kiberbiztonsági-, információbiztonsági-, csalási kockázat etc.). A biztonság nem egy statikus állapot, hanem azt folyamatosan fenn kell tartani. A kívánt biztonsági szint eléréséhez megfelelő kockázatkezelés szükséges. A kutatás azt vizsgálja, milyen biztonsági intézkedések és a biztonsági folyamatok milyen hálózata azonosítható a vállalatoknál, mely hozzájárul a vállalatok működési biztonságához, a sikeres

ISSN 1788-7593 (Nyomtatott) DOI: https://doi.org/10.14232/jtgf.2022.1-2.77-90
ISSN 2676-9867 (Online)

vállalati működéshez, és a reziliencia megteremtéséhez az ipar 4.0, ill. 5.0 által generált lehetőségek és kihívások közepette.

A kutatás célja a szervezetek védelmi hálójának feltárása, meghatározása annak, hogy milyen „biztonsági elemekből", kontrollokból épül fel a szervezetek védelmi rendszerének hálózata. Kontrollok alatt azokat a tevékenységeket értem, melyek biztosítják, hogy a folyamat hibamentesen, ill. adott elfogadható tűréshatáron belüli hibaszázalékkal következik be. Kontroll funkció alatt azokat a tevékenységet értem, melyek a belső kontroll rendszer megvalósulását, és működését segítik; a belső kontrollrendszer szinonimájaként használom, mely több szinten megjelenik a vállalati működés során, része valamennyi vállalati folyamatnak, és működését nagyobb, jellemzően tőzsdei vállalatoknál önálló támogató funkció (belső kontroll csoport) segíti. A folyamatokhoz rendelt kontrollok hálózata tulajdonképpen a belső kontrollrendszer megvalósulása a vállalati folyamatokban.

A kutatás célja bemutatni a kontrollok hálózatának szerepét a vállalatbiztonság elérésében. Továbbá azonosítani azt, hogy külső megfigyelő / érintett milyen információkat tud kinyerni a vállalati biztonsági hálózatról a vállalati éves beszámolókból anélkül, hogy egyéb formális, és informális forrásokat használna. A kvalitatív kutatás a Magyarországon működő autóipari vállalatokat vizsgálja, ahol a téma jól definiáltan értelmezhető.

## 2. Szakirodalmi elemzés

### 2.1. Hálózatok és vállalat

Az információs és kommunikációs technológiák (IKT) áthatják az új társadalmi struktúrát, a hálózati társadalmat, ahol az alkalmazkodás képessége folyamatosan szükséges a vállalatok és munkavállalók szintjén is (Castells, 2010). Az információgazdaság következménye, hogy a huszadik századi irányadó vállalati struktúra, az ún. vállalati fastruktúra háttérbe szorul, és elmozdulás tapasztalható a horizontális, hálózatos szerkezet irányába. A vállalati fastruktúra szerint a vállalat szerkezete egy feje tetejére állított fához hasonló hálózatra épült, ahol a vezérigazgató a fa gyökere, a gyökértől távolodva csökken a felelősség. A fa modell merev, és nem képes a változásokhoz alkalmazkodni. A változó üzleti környezetben a dinamikus, hálózatos szervezeti felépítés válik szükségessé. Megnő többek között a munkacsoportok, munkaerőkölcsönzés szerepe, sok helyen megszüntetik a középvezetői állásokat, és kisegítőket emelnek ki fő felelőssé (Barabási, 2008).
„Hálózatok mindenhol vannak" (Barabási, 2006). A vállalkozások maguk is hálózati működésben gondolkodnak. A vállalati működés során jellemző a hálózati tagság. Vállalkozók körében végzett felmérés szerint a hálózatóké a jövő (In. Blahó et al., 2016). „Fenntartható hálózati csomópontként csak az tud fennmaradni, akinek az elosztás során követett méltányosságában a többi hálózati szereplő megbízik" (Bakacsi, 2018, p. 291). „A vállalatok soha nem egyedül élik életüket" (Barabási, 2008, p. 219). Kiemelkedő fontosságú a felsővezetők kapcsolata a többi céggel, a más szervezetektől való tanulás, mely kapcsolatokban a hálózatosság alapvető szerephez jut (Barabási, 2008).

A szervezet működését meghatározó folyamatok az egymással kapcsolatban lévő folyamatlépésekkel írhatók le, melyeket vizuálisan a folyamatlépésekről készített folyamattérképek ábrázolnak. A hagyományosan ismert vállalati folyamatok hierarchiája a stratégiaitól, a taktikai és az operatív szintek irányába halad (In. Blahó et al., 2016; Chikán, 2020; Chikán–Demeter, 2004; Dobák–Antal, 2016; Jelen–Mészáros, 2018; Kadocsa, 2009; Poór, 2017). Az egyes szintekhez szabályzatok, folyamatleírások kapcsolódnak, melyeknek megfelelő kezelése a vállalat ellenállóképességét, és integritását erősíti, valamint alapját jelentik a sikeres változáskezelésnek, és külső minősítéseknek. Meghatározó a „vezetőség hangja" és a szervezeti kultúra „lágy" eleme, a folyamatok mögött lévő ember is. A vállalati folyamatok, mint a beszerzés, értékesítés, vagy könyvvitel egymáshoz kapcsolódó folyamatlépések hálózataként is értelmezhetők. A hálózatok fogalma értelmezhető a vállalatokra, több vonatkozásban adaptálhatók a vállalati folyamatokra az üzleti életben, és több szinten is megjelennek a vállalatok „belső" és „külső" működésében. Hálózatot alkotnak a vállalatok és vevők, banki utalások, szállítási rendszerek, a vállalati folyamatok, a folyamatot képező folyamatlépések, de egy projekt is. A vállalatok belső struktúrája is szorosan kapcsolódik a hálózatokhoz. A hálózatok a szervezet egészét lefedik, ill. beépülnek a folyamatokba. A hálózati struktúra értelmezhető az anya-, és leányvállalati kontextusban, továbbá a folyamatszervezés során is. Hálózati szempontból speciális eset az egyes folyamatlépések és a folyamatok összvállalati szinten történő centralizált végrehajtása.

A vállalatok üzleti modellje a küldetés megvalósítására kiválasztott tevékenységek hálóját takarja, annak konkretizálása (Chikán, 2020). Az üzleti modell tevékenységeken, és azok kapcsolatain keresztül teremt értéket az érintetteknek, kiemelten a fogyasztóknak és a tulajdonosoknak (Chikán, 2020). A vállalatok biztonsági hálója szorosan kötődik ezekhez a tevékenységekhez, és kapcsolatokhoz. A vállalati folyamatok az emberi tényező és az információs és kommunikációs technológiai (IKT) rendszerek „együttműködése" által valósulnak meg. A vállalati folyamatok egymáshoz kapcsolódó lépések láncolatai, nélkülözhetetlen a különféle folyamatok összekapcsolódása. A hatásos és biztonságos szinten történő működéshez szükséges többek között a munkafolyamatok összhangja, a vállalati funkciókat képviselő emberek közötti együttműködés, és transzparencia. Szükséges látni a folyamatok közötti összefüggéseket, mely segíthet kiküszöbölni bizonyos hibák, ill. biztonsági események előfordulásának valószínűségét.

## 2.2. A biztonság hálózata

A biztonság hálózatának megteremtéséhez megfelelő kockázatkezelés szükséges. A kockázatkezelés kulcsszereppel bír a kívánt biztonsági szint elérésében. A vállalati folyamatok működése során a biztonsági elemek, kontrollok biztosítják a szükséges biztonságot. A munkafolyamatokba épített kontrollok a vállalati folyamatok hálózatának szerves részét képezik. A kontrollok hálózata megjelenik a vállalati folyamatokban, melyet többek között a vállalati stratégia, a szervezeti struktúra, az

irányítási rendszerek, az etikai kódex intézményesülése, a szervezeti biztonsági kultúra, és a folyamatokat kísérő, működtető emberi tényező határoz meg.

A folyamatok működése a rendszer-, és az emberi tényezők együttese által valósul meg. Az információs és kommunikációs technológiák (IKT) intenzív térnyerésével az információbiztonsági-, és informatikai biztonság szerepe nő (Kemendi, 2022). Az IKT rendszerek biztonsága kiemelt jelentőségű. Az emberi tényező külön kockázati kategóriát képez. Az emberi tényezőhöz a szükséges szakképzett munkaerő, a kritikus tudás, tapasztalat mellett szorosan kapcsolódik a formális, és az informális kapcsolati háló. Biztonsági szempontból az alapvető értékek, mint etikus magatartás, elkötelezettség és a bizalom fogalma kimagasló jelentőséggel bírnak (Kemendi, 2021). Az etikai kódex elveit követve erős szervezeti kultúra alakul ki, mely hosszabb távon „értékként" jelenik meg. Csalási, sikkasztási, és pénzmosási esetek is megelőzhetők az etikai elvek követésén keresztül. A vállalati szintű kockázatkezelés értelmében „a kockázat mindenki felelőssége" (Hall, 2007). A kontrollfolyamatok a szervezeti célok megvalósítása érdekében szükségesek, amihez a szervezet valamennyi tagjának hozzá kell járulnia. A vállalati folyamatok biztonságát az IKT-, és humán kockázatok együttes kezelése határozza meg. A vállalati biztonsági hálózatát képező kontrollok meghatározása során az IKT és HR kockázatok egyidejű kezelése szükséges.

A különféle kockázatkezelési módszerek jellemzően közös alapokon nyugszanak. A kockázatkezelés szorosan kapcsolódik a belső kontrollrendszerhez. A COSO keretrendszer a belső kontrollrendszer integrált keretrendszerét írja le (angolul: „COSO Internal Control – Integrated Framework, a.k.a. COSO"), melyet 1992-ben adtak ki, és 2013-ban jelent meg a frissített változata (COSO, 2013a). A COSO keretrendszer három célkategóriát fogalmaz meg a szervezetben, az operatív, beszámolási (reporting) és megfelelés (compliance) célokat. A keretrendszer öt integrált, összefüggő komponensből áll, melyek a célok elérését segítik: kontrollkörnyezet, kockázatértékelés, kontrolltevékenységek, információ és kommunikáció, monitoring. Az öt komponenshez kapcsolódóan az alapvető koncepciót tizenhét elv reprezentálja, melyeket a következőkben ismertetek. A kontrollkörnyezethez kapcsolódó elvek között szerepel a vállalati elköteleződése az integritás és etikai értékek felé, a munkavállalók felelőssége a belső kontrollokért, kompetens munkatársak kiválasztása, fejlesztése és megtartása, menedzsmenttől független igazgatótanács, megfelelő jogosultságok és felelősségi körök. A kockázatértékelés komponenshez kapcsolódóan olyan célok meghatározása szükséges, melyek lehetővé teszik a kockázatok azonosítását és értékelését az adott célhoz kapcsolódóan. A szervezet meghatározza a célok elérését veszélyeztető kockázatokat, mérlegelve a csalás kockázatát, és a változásokat, melyek a belső kontrollrendszert jelentősen befolyásolni tudják. A szervezet olyan kontrolltevékenységeket határoz meg, melyek képesek elfogadható szintre mitigálni a célok elérését veszélyeztető kockázatokat. A szükséges kontrolltevékenységeket szabályzatokban fekteti le. Az információs és kommunikációs komponens megfelelő minőségű, és releváns információt használnak, és generálnak. A belső kontrollrendszer működéséhez szükséges információk a szervezeten belül

kommunikálásra kerülnek. A szervezet a külső felekkel kommunikál a belső kontrollrendszer működését érintő ügyekben. Monitoring tevékenységek szükségesek, melyek biztosítják, hogy a belső kontroll rendszer elemei megfelelőek, és az esetleges hiányosságok kezelése megtörténik (COSO, 2013b).

A 2004-ben megjelent „Vállalati szintű kockázatkezelés – integrált keretrendszer" (COSO ERM) már a stratégiai célokat is tartalmazza, ill. a kockázatértékelés komponensét elemeire bontva ismerteti (COSO, 2004). A COSO iránymutatás legfrissebb változata a 2017-ben került publikálásra „Vállalati szintű kockázatkezelés – integráció a stratégiával és teljesítménnyel" elnevezéssel (Anderson–Frigo, 2020).

A vállalati védelmi rendszer szintjei az elsődleges, másodlagos, és harmadlagos védelmi vonal mentén is értelmezhetők. A vállalati védelmi vonalak (IIA, 2020) a vállalati működés valamennyi szintjén megjelennek. Az effektív kockázatkezelés és kontroll ún. három védelmi vonal modelljét az IIA (The Institute of Internal Auditors) 2013. januári állásfoglalásában definiálta. Az elsődleges védelmi vonal maga az üzleti folyamatokba ágyazott kockázatkezelés. Az üzleti folyamatok vezetőinek felelősségi körébe tartozik a hatáskörükbe tartozó vállalati folyamatok kockázatainak azonosítása, megfelelő kezelése és kontrollok működtetése. Az elsődleges védelmi vonal az operatív folyamatok szintjén nyújt aktív védelmet. A másodlagos védelmi vonal a kockázatkezelés - és megfelelés funkció, mely szintén a szervezeten belüli védelmi háló eleme, azonban már az üzleti folyamatoktól elkülönülten tekint a vállalati folyamatokra, monitorozza- és ellenőrzi az elsődleges folyamatok működését. A harmadik védelmi vonal független funkcióként tesztel és ellenőriz, belső vagy külső audit formájában. Az IIA 2020-ban adta ki a modell frissített változatát, mely a modern kockázatkezelés és irányítás területén bekövetkezett változásokra reflektál (Chambers, 2020). Az erős irányítás és kockázatkezelés megteremtése érdekében a kulcs szervezeti szereplők együtt dolgoznak (IIA, n.d.).

A vállalati védelmi háló pilléreit fedik le az ún. GRC rendszerek: irányítás (governance), kockázatkezelés (risk), és megfelelés (compliance). A GRC rövidítést 2003-ban használták először, és az első lektorált tudományos kiadvány 2007-ben jelent meg (OCEG, n.d.). Az Irányítás, Stratégia, Kockázatkezelés, Audit, Jog, Megfelelés, Információs technológia, Etika és vállalati társadalmi felelősségvállalás, Minőségirányítás, valamint a Humán tőke és kultúra mind olyan területek, melyek a GRC-hoz kapcsolódó folyamatokhoz tartoznak (Mitchell, 2007). Ezek a folyamatok a szervezetet hozzásegítik céljai eléréséhez, igazodva annak határaihoz (Mitchell, 2007). A GRC rendszerek leegyszerűsítve a stratégiai üzleti célok védelmét szolgálják, és képesek összhangot teremteni a vállalati folyamatok szintjén felmerülő, a hármas védelem modell által definiált védelmi kívánalmaknak (Michelberger–Kemendi, 2020).

A kontrolling funkció a vállalati hálózatok, és a biztonsági hálózat meghatározó eleme. A kontrolling szabályozókör – a tervezés, az irányítás (mérés, elemzés) és a visszacsatolás – a stratégiai, operatív és diszpozitív irányítás szintjén is érvényesül (Maczó, 2007). A menedzsmentkontroll folyamat a szervezet stratégiájának

megvalósítására irányul (Anthony–Govindarajan, 2009). „A kontrolling a múlt hibáit a jövőépítés szempontjából vizsgálja” (Francsovics, 2011, p. 13). A kontrolling funkció a szervezeti tanulás képességén keresztül hosszabb távon jelentős hozzáadott értéket teremthet, és a biztonság eszközeként is jelentős a szerepe.

## 3. Kutatás módszertan

A kutatás célja a kontrollok hálózati szerepének vizsgálata a vállalatbiztonság elérésében, melynek feltárásához a következő kutatási kérdésekből indulok ki:

1. Hogyan jelenik meg a kontroll funkció / belső kontrollrendszer a vállalatok éves beszámolójában? Milyen modellt követ? Mely kapcsolódó funkciók azonosíthatók? Hogyan jelenik meg a biztonság és védelem pl. információ biztonság (information security), biztonság és védelem (safety and security) a vállalatok éves beszámolójában?
2. Hogyan jelennek meg a kockázati tényezők, és bizonytalanságok a vállalati éves beszámolójában?
3. A humán erőforrás szerepe miként azonosítható biztonság és védelmi kontextusban?
4. Rés a pajzson esetek. Vállalati éves jelentésben szerepelnek vállalati botrányok, csalások? Amennyiben igen, milyen a vezetőség válasza?

Milyen kontextusban jelenik meg a hálózat (network) kifejezés a vállalat éves beszámolójában? Mennyiben jelenik meg a vállalati belső kontrollrendszer hálózatként, és miként definiálható a hálózati struktúra?

A tématerületet kvalitatív kutatás segítségével vizsgálom (Malhotra–Simon, 2009; Gyulavári et al., 2017; Kelemen-Erdős–Mitev, 2017; Kelemen-Erdős, 2019). A kutatáshoz a kvalitatív módszertanon belül a tényanyag adatfeldolgozására és elemzésére a tartalomelemzést választottam (Graneheim et al., 2017, Lindgren et al., 2020. A vizsgált minta a Magyarországon jelen lévő autóipari cégek populációja, ahol a biztonság kérdésköre stratégiai célként jelenik meg. A mintába a Magyarországon működő négy autóüzem - Suzuki, Opel, Audi, Mercedes – anyavállalata kerül. A vizsgált vállalatok közül három vállalat tőzsdén jegyzett anyavállalathoz kötődik (Audi, Mercedes, Suzuki), míg egy vállalat (Opel) jelenleg magáncég tulajdona. Az autóipari szektor választását indokolja, hogy az autóiparon belül kiemelkedően megjelennek az ipar 4.0. által generált technológiai újdonságok, lehetőségek és fenyegetettségek, folyamatos változások, fejlesztések, melyek napjainkban meghatározó jelentőséggel bírnak. A szektor magasan standardizált folyamatokkal operál. A gyártás során a mesterséges intelligencia alkalmazása jelentős. A gyártósorokon az ember és robot együttesen dolgozik. Megjegyzem, a választott iparágat magát is jellemzi a hálózatszerű működés, példaként említhető a Catena-X Autóipari Hálózat, melynek célja, hogy egységes szabványt hozzon létre az információk és az adatok megosztására az autóipari értéklánc egészében.

A tulajdonosi érdek védelme kapcsán magas kontroll tudatosság, illetőleg az ICFR (Internal Control over Financial Reporting, azaz a belső kontroll a pénzügyi beszámoló felett) elemeinek megjelenése, továbbá a vállalatméretből kifolyólag

nagyfokú rendszerszemlélet, kontrolltudatosság, dokumentáltság feltételezhető. A kutatás tárgya a kontroll hálózat feltárása, melyhez a minta jó alapul szolgál.

A kutatási kérdések vezérfonala mentén a vizsgált vállalatok kontrollrendszerét, és kontrollfolyamatainak hálózatatát a vállalatok éves beszámolói alapján „külső szemlélőként" vizsgálom. A kapcsolódó vállalati folyamatok ismertetése a vizsgált beszámolókban különböző szintű. Az éves beszámolók tartalomelemzése tételes adatrögzítő íveken kerül rögzítésre (ld. *1-5. táblázat*).

## 4. Eredmények és értékelésük

A következőkben az éves beszámolókat – úgymint AUDI vállalat (Audi AG Annual Report, 2020), MERCEDES vállalat (Daimler Group Annual Report, 2020), SUZUKI vállalat (Suzuki Annual Report, 2020), OPEL vállalat (Groupe PSA Annual Report, 2019) – a főbb kutatási célok mentén értékelem. (Megjegyzés: az adatrögzítő íveken az 1-5. táblázatban feltüntetett oldalszámok az éves beszámolókban szereplő tényleges oldalszámok, mely eltér a pdf dokumentum fejlécén szereplő oldalszámtól.)

A vizsgált vállalatok esetében közös az a transzformációs folyamat, mely az iparágat jellemzi, és mindez meghatározó a vállalati stratégia, valamint kockázatkezelés szempontjából is.

### 4.1. A belső kontrollrendszer / Kontroll funkció megjelenése az éves beszámolóban

A belső kontrollrendszer és kontroll funkció szabályzatok szintjén is megjelenik. Az Audi és Mercedes esetében tételes megnevezésre került, hogy a COSO modellt követi a belső kontrollrendszer. A Suzuki és Opel éves beszámolója nem tartalmaz konkrét modellt. Ugyanakkor az Audi éves jelentésében kiemeli, hogy a kockázatkezelési architektúra szisztematikus strukturálása érdekében az Audi csoport követi a három védelmi vonal modellt. A három védelmi vonal kifejezés maga nem jelenik meg a többi vállalat éves beszámolójában, egyes elemei azonban fellelhetőek esetükben is különböző részletezettséggel (ld. *1. táblázat*: A belső kontrollrendszer / Kontroll funkció megjelenése az éves beszámolóban).

## *1. táblázat:* A belső kontrollrendszer / Kontroll funkció megjelenése az éves beszámolóban

| Kutatási kérdés | AUDI vállalat | MERCEDES vállalat | SUZUKI vállalat | OPEL vállalat |
|---|---|---|---|---|
| **1. Hogyan jelenik meg a kontroll funkció a vállalat éves beszámolójában?** | | | | |
| **Hogyan jelenik meg a kontroll funkció a vállalatok éves beszámolójá-ban?** | - támogató pillér<br>- vállalati célok, átláthatóság, kockázat, megfelelés, integritás biztosítása, tudatosság erősítése<br>- megfelelő és stabil folyamatok biztosítása<br>- belső kontrollrendszer (ICS) kiterjedt felülvizsgálata és kiterjesztése.<br>- kockázatkezelés (RMS) kiegészül a belső kontrollrendszerrel<br>- központi GRC funkcióhoz szorosan kapcsolódik az RMS/ICS<br>- kombinált riport az Igazgatótanács, Felügyelő Bizottság, Audit Bizottság számára (RMS, ICS, CMS- megfelelési rendszer)<br>(pp. 71, 121-122) | - új vállalati struktúra<br>- Daimler AG operatív és stratégiai menedzsment holding<br>--> kontrolling, irányítási - és igazgatási funkciók, szolgáltatások a vállalatcsoport tagjai számára<br>- központi szinten Pénzügy és Kontrolling, HR, Integritás és Jog (pp. 26, 37) | - megfelelési és kockázatkezelési rendszerek teljeskörű felülvizsgálata<br>- valamennyi működési terület lefedése<br>- belső kontrollrendszer erősítése<br>(p. 2-3) | - belső kontroll -, és kockázatkezelő funkciókért a menedzsment felel<br>- pénzügyi beszámolási folyamat monitorozása, valamint a belső kontroll, - és kockázatkezelési rendszerek hatékonysága, illetve ahol relevàns, a belső audit a számviteli és pénzügyi riporting eljárásokat illetően. Felelős: Pénzügy és Audit Bizottság.<br>(p. 107) |
| Milyen modellt követ a belső kontroll rendszer? Keretrendszer (COSO; Turnbull report) | COSO (p. 122) | COSO (p. 115) | *Konkrét modellt az éves beszámoló feldolgozása során nem azonosított a szerző.* | *Konkrét modellt az éves beszámoló feldolgozása során nem azonosított a szerző.* |
| A három védelmi vonal modell elemei hogyan érvényesülnek az éves beszámolóban? | - a kockázatkezelési architektúra szisztematikus strukturálása érdekében az Audi csoport követi a három védelmi vonal modellt<br>- a vállalat védelmét célozza jelentős kockázat bekövetkezése ellen<br>- minden vonal rendszeresen és függetlenül jelent az Igazgatótanács és a Felügyelő Bizottság Audit Bizottsága felé<br>- Első vonal: operációs kockázatkezelés divíziószinten; Második vonal: központi GRC funkció felelős az RMS/ICS és CMS alapvető működtetéséért; harmadik vonal: Belső audit, továbbá az RMS/ICS-t számviteli oldalról független auditor is vizsgálja.<br>(pp. 123-125) | *A három védelmi vonal kifejezés maga nem jelenik meg a beszámolóban, egyes elemei azonban fellelhetőek. (pp. 69, 74, 82, 84, 114, 115, 116)* | *A három védelmi vonal kifejezés maga nem jelenik meg a beszámolóban, egyes elemei azonban fellelhetőek.*<br>*(pp. 3, 26-41)* | *A három védelmi vonal kifejezés maga nem jelenik meg a beszámolóban, egyes elemei azonban fellelhetőek.*<br>*(pp. 107-108)* |
| Mely kontroll témakörhöz kapcsolódó funkciók azonosíthatók (stratégia, megfelelés (compliance), vállalatirányítás (corporate governance), kockázatkezelés (risk management), kontrolling, etika stb.)? | Etikus működés, Adatvédelem és adatbiztonság, Vállalatirányítás és Megfelelés, Vállalati kultúra, Korrupcióellenes működés, Stratégia<br>(pp. 10, 79, 315, 318) | - integritás és megfelelőség (p. 82), stratégia (p. 26), műszaki megfelelési irányítási rendszer (tCMS) autóipari részlegekben.<br>- a cél az összes jogi és szabályozási követelmény betartását biztosítani a teljes termékfejlesztési és tanúsítási folyamat során (p. 85),<br>- antitröszt-megfelelés (p. 85), korrupcióellenes megfelelés (p. 85), adat-megfelelés (p. 86), pénzügyi bűncselekmények elleni megfelelés (p. 86), humán jogok tiszteletben tartása rendszer (p. 86) | Vállalatirányítási kódex, Etikai kódex, Megfelelés- és kockázatkezelés<br>(pp. 26, 31) | Pénzügyi stratégia, pénzügyi kockázatkezelés (pp. 8, 70, 86) |
| Hogyan jelenik meg a kontroll funkció és a kockázatok kapcsolata? (internal controls and risks) (components of internal control: control environment, risk assessment, control activities, information and communicatio, and monitoring activities)? | - kockázatoknak megfelelő belső kontrollok a teljes értéklánc mentén<br>- RMS/ICS további fejlesztése<br>- prioritás a rendszer szoros összekapcsolása a vállalati pénzügyi tervezéssel és menedzsmenttel, valamint a számviteli rendszerekkel<br>- RMS/ICS szabályozási keretrendszere stratégiai jelentőségű. Belső vállalati politikában, szabályzatokban szilárdan megjelenik.<br>(p. 123) | - a belső kontrollrendszer hatékonyságának szisztematikus értékelése a vállalati számviteli folyamat szempontjából.<br>(kockázatelemzés; jelentős kockázatok azonosítása a vállalati számviteli és pénzügyi beszámolási folyamatokhoz; az ellenőrzések meghatározása és dokumentálása a csoportszintű irányelveknek megfelelően; rendszeres tesztelés véletlenszerű mintákon (kontrollok hatékonyságának felmérése, önértékelés alapja, ellenőrzési gyengeségek kiküszöbölése).<br>- az Igazgatóság és a Felügyelő Bizottság Audit Bizottsága rendszeresen tájékoztatása<br>- Felügyelő Bizottság; Belső ellenőrzési osztály; Külső auditorok szerepe (pp. 115-116) | A belső kontrollrendszerre vonatkozó alapvető szabályok a Megfelelési és Kockázatkezelés szekció alatt vannak ismertetve.<br>(pp. 31-34) | Kockázati tényezők és bizonytalanságok' szekció alatt az éves management riport részeként, az éves beszámoló 8. oldalán található hivatkozás a belső kontrollokra.<br>- A Csoport különböző működési egységei azonosítják és felmérik a kockázatokat, és folyamatosan értékelik a kapcsolódó belső kontrollokat, éves jelentéstétel az Igazgatóságnak. (p. 8) |
| Milyen kontroll funkcióhoz kapcsolódó kézikönyvek, szabályzatok-hoz és eljárásrendhez azonosíthatók? (handbooks, policies and procedures) (eg. Compliance, AML, stb.) | Magas stratégiai jelentősége miatt az RMS / ICS szabályozási keretrendszere mind a belső vállalati politikában mind a szabályzatokban szilárdan megjelenik. (p. 123) | A (belső kontroll) rendszer alapelveket és eljárásokat, valamint megelőző és detektív ellenőrzéseket tartalmaz." (p. 115) | Vállalatirányítási kódex (p. 26), Suzuki Group magatartási kódex (p. 26, 31), Megfelelési kézikönyv (Compliance Handbook) (pp. 33, 35), CSR Guidelines for Suppliers (biztonság és minőség elve elsődleges) (pp. 52-53) | Pénzügyi kockázatkezelési politika (p. 70), PSA Csoport kamatlábkockázat-kezelési politika (p. 71), PSA-csoport általános kockázatkezelési politika (p. 71), fedezeti politika (p. 73), devizapolitika (p. 73), tőkekezelési politika (p. 92) |
| Milyen kiemelt elemei vannak az éves beszámolónak a biztonság és védelem pl. információ biztonság (information security), biztonság és védelem (safety and security) szempontjából? | A személyes adatok globális védelme és felelősségteljes kezelése (p. 292) | Vállalatbiztonság, Adatbiztonság, Információbiztonság, IT biztonság. Kiberbiztonság, Foglalkoztatottság biztonsága (pp. 40, 84, 115) | Személyes információ védelme (p. 35), Információbiztonság (p. 36), Katasztrófavédelem (p. 36), Biztonság és egészség védelme (p. 48), BCP (pp. 33, 36, 41, 52), Termékminőség/ Termékbiztonság (ISO 9001-et adaptálta) (pp. 46-47) | Egészségügyi és biztonsági kockázatok (p. 8), pénzügyi biztonság (p. 70), ügyfeleknek szállított áruk és szolgáltatások ellenértékének fizetési biztonsága (p. 73), jelentős meghibásodás, üzemzavar vagy biztonsági sérülés, amely veszélyezteti az informatikai rendszereket v, a társaságok járműveiben található elektronikus vezérlő rendszereket (p. 109) |

Forrás: az éves beszámolók alapján a szerző szerkesztése.

### 4.2. Kockázati tényezők és bizonytalanságok az éves beszámolóban

Az irányítás (governance), kockázatkezelés (risk), és megfelelés (compliance) szerepe az éves beszámolókban domináns. Míg a kontroll funkció a vállalati kockázatkezeléssel együtt jellemzően stratégiai jelentőségű támogató pillérként azonosítható. A kockázatkezelés önálló szekcióként jelenik meg az éves beszámolókban (ld. *2. táblázat*: Kockázati tényezők és bizonytalanságok az éves beszámolóban).

*2. táblázat:* **Kockázati tényezők és bizonytalanságok az éves beszámolóban**

| Kutatási kérdés | AUDI vállalat jellemzői | MERCEDES vállalat | SUZUKI vállalat | OPEL vállalat |
|---|---|---|---|---|
| **2. Hogyan jelennek meg a kockázati tényezők, és bizonytalanságok a vállalati éves beszámolóban? Hogyan jelenik meg a kockázatkezelés szerepe?** | | | | |
| Hogyan jelennek meg a kockázati tényezők, és bizonytalanságok a vállalati éves beszámolóban? | - Kockázatok és lehetőségek jelentése szekció alatt az éves beszámoló ismerteti a kockázatkezelési rendszert, lehetőségkezelés működési elvét, valamint az Audi csoport "kockázatait és lehetőségeit"<br>- Integritás, Megfelelés- és Kockázatkezelés funkció<br>- Vállalati kockázatkezelésünk és a kockázatkezelési rendszer (RMS), vállalati irányelveink, a belső kontrollrendszer (ICS) és a Compliance Management System (CMS) támogatják munkájuk alappilléreit. (a vállalat céljainak fenntarthatóan védelme, az átláthatóság megteremtése és a kockázatok, a megfelelés és az integritás tudatosságának erősítése érdekében)<br>(pp. 68, 71, 121) | - A Kockázat - és lehetőségkezelés a Csoport tervezési, kontrolling és jelentés folyamatának erőteljes eleme.<br>- A Kockázat - és lehetőség jelentés önálló rész az éves beszámolóban.<br>- "Az üzleti kockázatok és lehetőségek korai stádiumban történő azonosítása, valamint azok aktív felmérése és kezelése érdekében hatékony irányítási és kontrollrendszereket kell összeállítani egy átfogó kockázat- és lehetőségkezelési rendszerben, alkalmazzák. Az információs technológiai kockázatok és lehetőségek, valamint a személyi kockázatok és lehetőségek fel vannak tüntetve kockázati kategóriákként." (pp. 74, 114-129, 142) | A Vállalatirá-nyítás szekció alatt Megfelelési- és kockázat-kezelési rendszer, ill. a Működési kockázatok szekció alatt.<br>(pp. 31-41) | Kockázati tényezők és bizonytalanságok' szekció az éves management riport részeként, az éves beszámoló 8. oldalán, ahol a főbb csoportra jellemző, valamint üzleti kockázatok jelennek meg.<br>A kockázatkezelést főként a Vállalati Pénzügy funkció végzi, azonosítja a kockázatokat és csoport szabályzatokat határoz meg azok kezelésére. Pénzügyi kockázatkezelési politika (p. 70).<br>(Kockázatok megjelennek az ún. statutory audit jelentés részeként is, ahol specifikus kockázatok lettek azonosítva fő audit kockázatokként. ld. statutory audit riport p. 105-106)) |
| Hogyan jelenik meg a kockázatkezelés szerepe? | "- A lehetőségek és kockázatok konstruktív és nyílt kezelése elengedhetetlen az Audi számára a vállalkozói tevékenység tartós sikerének biztosítása érdekében.<br>- A hatékony kockázatkezelési rendszer (RMS) konkrét célja - a törvényi előírások teljesítése mellett - a vállalkozás céljainak érvényesítése, az érdekeltek védelme a negatív vállalati fejlemények ellen, a kockázatok messzemenően gondos kezelési kötelezettségének teljesítése a hosszú távú életképesség és versenyképesség védelmeként. "<br>(p. 121) | A Csoport tervezési, kontrolling és jelentés folyamatának erőteljes elemeként jelenik meg (p. 74). | *Az éves beszámoló alapján egyre nagyobb hangsúlyt kap a funkció.* | Pénzügyi kockázatkezelési politika (p. 70), PSA Group kamatlábkockázat-kezelési politika (p. 71), PSA-csoport átfogó kockázatkezelési politika (p. 71). A Banque PSA Finance kockázatkezelési bizottsága (p. 87). |

Forrás: az éves beszámolók alapján a szerző szerkesztése.

## 4.3. Emberi tényezők biztonsági szerepe

Az emberi erőforrások szerepe megjelenik stratégiai vonatkozásban, a vállalati kultúra kontextusában, a szervezeti tanulásban, és megjelennek etikai vonatkozások. További közös elem a vállalatok érintettsége a dízel emissziós botrányban. (Kapcsolódó forrásként ld. European Court of Auditors, 2019 tájékoztató dokumentumát.) Az eset erőteljes vezetőségi választ követelt meg. A „Rés a pajzson" eset kapcsán a biztonság és védelem, a belső kontrollrendszer korszerűsítése, fejlesztése, valamint a vállalati kultúra és tudatosság, szervezeti tanulás szerepe középpontba került (ld. *3. táblázat*: Emberi tényező biztonsági szerepe).

*3. táblázat***: Emberi tényezők biztonsági szerepe**

| Kutatási kérdés | AUDI vállalat | MERCEDES vállalat | SUZUKI vállalat | OPEL vállalat |
|---|---|---|---|---|
| **3. A humán erőforrás szerepe miként azonosítható biztonság és védelmi kontextusban?** | | | | |
| A humán erőforrás szerepe miként azonosítható biztonság és védelmi kontextusban? | - munkahelyi egészség - és biztonság,<br>-stratégiai HR tervezés,<br>-"vállalbiztonság",<br>- emberi jogok tréning,<br>- vállalati kultúra - motivált csoport képes a transzformációt megvalósítani, és kellőképp innovatív szakértelmet felhalmozni,<br>- fenntartható koncepció a digitalizációhoz kapcsolódóan<br>(pp. 60-62, 264, 272-274, 346) | - Integritási kódex - kötelező forma; törvények, szabályok betartása, elkötelezettség, vállalati értékek követése a gyakorlatban.<br>- Értéktermelési folyamatok -> munka digitalizációja. Digitális átalakítás - munkabiztonsági garancia. Munkaköri leírások, feladatok és a követelményprofilok változása.<br>- Változási folyamatok támogatása - képzési intézkedések a teljes munkaerőnek (pp. 77, 78, 83) | -Az emberi erőforrások - és munkavédelem fejlesztése kiemelt szerepet kap.<br>- HR releváns biztonság és védelmi kérdések az éves beszámolóban<br>- Személyes információk védelme, Biztonság és egészség védelme.<br>(pp. 2-3, 33, 35, 37, 48-49) | Munkahelyi egészség és biztonsági kockázatokra talált hivatkozást a szerző. (p. 8) |
| Azonosítható az éves beszámolóból, hogyan biztosítja a vállalat, hogy a munkavállalók ismerik a kontrollokat? (Trainings) | Hálapénzről szóló szabályzat az összeférhetetlenség és korrupció elkerüléséről; Web-alapú tréningek a korrupcióellenes, ill. közhivatalnokok kezelésével kapcsolatos témában; Web-alapú Etikai kódex és etikus döntéshozatal tréning (minden munkavállalónak kötelező); Web-alapú „Megfelelés-tudatosság" (Compliance awareness) tréning (pp. 79, 346) | Kiterjedt megfelelőségi tanfolyamokat kínálnak, amelyek az integritási kódexünkön alapulnak. A képzések tartalma és témái az adott célcsoport szerepéhez és funkcióihoz igazodnak. Rendszeresen elemzik a képzési programok szükségességét, szükség szerint kibővítik vagy adaptálják, és értékeléseket folytatnak. (p. 85) | - Megfelelési és a Kockázatkezelési rendszer (pp. 31) részeként jelenik meg az éves beszámolóban.<br>- HR Osztály folyamatos szemináriumai vezetőknek és alkalmazottaknak megfelelés témáról, vmint az egyes törvényekről / előírásokról (pp. 31).<br>- kockázatkezelési tréning igazgatóknak, tisztségviselőknek, ügyvezető igazgatónak (pp. 33).<br>- tréningek a munkavállalók részére autógyártással kapcsolatos törvényekről és rendeletekről (p. 33), visszaélést bejelentő rendszer használatának elősegítése / oktatás, poszterek (p. 33). | Oktatásra és tréningre vonatkozó hivatkozást a K+F-re vonatkozó kontextusban azonosított a szerző. (p. 38) |
| Milyen a kockázat és kontroll tudatosság a szervezetben? | Szoros együttműködés a vállalati -és HR stratégiák között, stratégiai HR tervezés, vállalati kultúra fejlesztése pl. Role Model Program (p. 62, 70, 78, 254, 261, 269, 272) | - a vállalat rendszeresen ellenőrizi, hogy a Csoport egységes pénzügyi beszámolási, értékelési és számviteli irányelveit folyamatosan frissítik, rendszeresen oktatják és betartják;<br>- a belső kontrollrendszer hatékonyságát szisztematikusan értékelik a vállalati számviteli folyamat szempontjából<br>- folyamatokat határoznak meg a feladatok szétválasztására és a „négy szem elvére" a pénzügyi kimutatások elkészítése során, valamint arra, hogy léteznek-e engedélyezési és hozzáférési szabályok a vonatkozó informatikai számviteli rendszerek számára stb. (p. 114) | A "Rés a pajzson" eset (ld. 5. pont) kapcsán kiemelkedő hangsúlyt kap a tudatosság, a biztonság és védelem, valamint a vállalati kultúra szerepe is.<br>- az alapoktól áttekintik a megfelelési - és a kockázatkezelési rendszerünket, hogy lefedjük a Társaság összes tevékenységét, és megerősítsük a belső ellenőrzés felügyeletét. - a belső kontrollrendszer korszerűsítése.<br>(pp. 2-3) | *A vizsgált éves beszámoló alapján tételes választ nem azonosított a szerző.* |

Forrás: az éves beszámolók alapján a szerző szerkesztése.

## 4.4. „Rés a pajzson” esetek

A „Rés a pajzson” esetek kapcsán azonosított akciólépések sorozata számos független, mégis összekapcsolódó elemet tartalmaz (ld. *4. táblázat*). A vállalati kultúra fejlesztése, az etikai elvek követése, a munkavállalók, és vezetőség oktatása közvetetten, és a konkrét napi feladatok végrehajtása során tulajdonképpen közvetlenül is hozzájárul a belső kontrollrendszer erősítéséhez, és ezáltal a vállalat biztonsági szintjének növeléséhez. Ezek az elemek a kontrollok hálózati jellegét támasztják alá, és kontrollhálózat teremtette biztonság és védelmi faktor szerepét definiálják.

*4. táblázat:* **„Rés a pajzson” esetek**

| Kutatási kérdés | AUDI vállalat | MERCEDES vállalat | SUZUKI vállalat | OPEL vállalat |
|---|---|---|---|---|
| **4. Rés a pajzson esetek. Vállalati éves beszámolóban szerepelnek vállalati botrányok, csalások? Amennyiben igen, milyen a vezetőség válasza?** | | | | |
| Vállalati éves beszámolóban szerepelnek vállalati botrányok, csalások? | igen, dízel botrány<br>pp. 23, 64, 68, 69, 80) | igen, dízel kipufogógáz-kibocsátással kapcsolatos botrány<br>pp. 16, 17, 40, 76) | Igen, a nem megfelelő magatartás a járművek utolsó ellenőrzésénél, 2017-ben feltárt incidens - nem megfelelő mintavétel az üzemanyag-fogyasztás és a kipufogógáz ellenőrzése során. (pp. 2-3, 33, 35, 40) | Igen, emissziós kontroll rendszer; beépített navigációs rendszer kapcsán törvényszegés a jogdíjfizetés elmaradása miatt (függő kötelezettségek) (p. 97) |
| Amennyiben igen, milyen a vezetőség válasza? | -integritás és megfelelés program (ECI - etikus vállalati elvek)<br>-Etikai Kódex, bejelentő rendszer és tréningek, kulturális változások. Aktív ún. speak up kultúra, integritás nagykövetek aktív hálózata. Integritás és vállalati kultúra központi kérdés. erősítette a rendszereit és folyamatait a korrupció megelőzés és trösztellenes viselkedés ellen és bevezette az üzleti partnerek átvilágítási folyamatát.<br>-A csoport "ellapította a hierarchiát", laposabb struktúrát hozott létre, decentralizálta a döntéshozatalt és új vezetési és kollaborációs modellt vezetett be. Transzformáció.<br>-Független Megfelelés Monitor megerősítése, hogy a csoport megtette a szükséges lépéseket a dízel botránnyal kapcsolatban.<br>-Az amerikai EPA adminisztratív megállapodást kötött 2019-ben az Audi AG-val, mely megállapodás elismeri az intézkedéseket, melyeket 2015 óta a vállalat tett, hogy erősítse a megfelelés és kockázatkezelés funkciókat. (pp. 68-73) | -közös peres (class action) eljárás rendezése az USA-ban a dízel kipufogógáz-kibocsátással kapcsolatban (kb. 250 000 dízelmotoros jármű kibocsátáskontroll rendszere volt érintett).<br>-műszaki megfelelőségi irányítási rendszer erősítése, szervizintéz-kedések az érintett járművek számára; országos kibocsátás-csökkentő program, és további projektek<br>-Integritás "frissítése" - integritás kultúra további fejlesztése a Csoportban. A Felügyelő Bizottság foglalkozott az antitrószt eljárásokkal, és részletes jelentést kapott a dízel kipufogógáz-kibocsátással kapcsolatos kérdésekről. (pp. 16, 17, 40) | -őszintén elnézést kértek helytelen magatartásuk miatt az üzemekben végzett végső járművizsgálat kapcsán<br>-vezetői vállalati tudatosság növelése, szervezeti kultúra fejlesztése, cél biztosítani a törvények és előírások alapos betartását a Társaság valamennyi működési szintjén<br>-végső ellenőrzési műveletek fejlesztése, pl. az ellenőrök terheinek csökkentését az ellenőrök számának növelésével és az ellenőrzési létesítmények fejlesztését, és előmozdították a vonatkozó intézkedéseket, hogy megbízhatóbb és pontosabb ellenőrzéseket lehessen végezni. További fejlesztések.<br>- 2017-es incidens - nem megfelelő mintavétel az üzemanyag-fogyasztás és a kipufogógáz ellenőrzése-kapcsán az incidens feltárásának napjára megemlékeznek, aznap leáll a vállalat működése, feleleveníve, hogy mennyire fontos megőrizni a nem megfelelő cselekedetekkel szembeni tudatosságot.<br>-biztonság és védelem kiemelt prioritás;<br>- "minőség javítása" (pp. 2-3, 33, 35, 40) | *A vizsgált éves beszámolóban részletes esetismertetést és vezetőségi választ nem azonosított a szerző.* |

Forrás: az éves beszámolók alapján a szerző szerkesztése.

## 4.5. Hálózatok az éves beszámolóban

A hálózati jelleg megjelenik a globális vállalati hálózat (a termékek világszerte eljutnak a fogyasztókhoz), és kereskedői hálózat kontextusában is, mely mögött a vállalati üzleti modell hálózati jellege azonosítható.

Az információ- és adatbiztonság tématerület valamennyi éves beszámoló közös metszete. A Suzuki éves beszámolója a hálózatok szerepét emeli ki az információ biztonság kontextusában, előtérbe kerül az információellenőrzés/ információ kontroll szerepe. Az információrendszer és hálózat célja, hogy az információszivárgást és jogosulatlan hozzáféréseket megakadályozza, ill. fejlessze/elősegítse az információhoz való hozzáférést.

Az Audi éves beszámolójában a work@Audi kezdeményezés alatt megnevezi, hogy elmozdulás történik a tradicionális struktúrák és merev hierarchiáktól, át akarják gondolni a vezetést, nyitottságra, őszinteségre és tiszteletre van szükség az információ cserék és témák megvitatása során. A Csoport „ellapította a hierarchiát”, decentralizálta a döntéshozatalt és új vezetési - és kollaborációs modellt hozott létre. Mindez a jó visszajelzési kultúra és az új és agilis együttműködés alapja is. A felvázolt működési modell a Barabási-Albert László által megjelenített szervezeti transzformáció jelenségével hasonlatos, ld. fentebb, miszerint elmozdulás szükséges a merev fa modelltől a változó üzleti környezetben a dinamikus, hálózati modell felé.

Megjegyzendő, hogy az Opel anyavállalata magántulajdonú, a vállalat éves beszámolója elsődlegesen a pénzügyi folyamatokra fókuszál, pénzügyi kockázatkezelés, pénzügyi stratégia jelennek meg kontroll témakörhöz kapcsolódó funkciókként. (A menedzsment felelőssége a kontroll-és kockázatkezelés funkció felett megjelenik, továbbá kirajzolódik a monitorozási folyamat.) A szöveges terjedelem a legrövidebbre szorítkozik, nagyságrendileg egy oldal. Az éves beszámoló „külső szemlélő" számára nem tárja fel érdemben a vállalati folyamatokat. A beszámolókból kigyűjtött tényanyagot ld. *5. táblázat*: Hálózatok az éves beszámolóban.

*5. táblázat:* **Hálózatok az éves beszámolóban**

| Kutatási kérdés | AUDI vállalat | MERCEDES vállalat | SUZUKI vállalat | OPEL vállalat |
|---|---|---|---|---|
| **5. Milyen kontextusban jelenik meg a hálózat (network) kifejezés a vállalat éves beszámolójában?** | | | | |
| Mennyiben jelenik meg a vállalati belső kontrollrendszer hálózatként, és miként definiálható a hálózati struktúra? (NB: Belső kontrollrendszer átszövi a szervezet egészét, valamennyi tevékenységbe beágyazódik… Szervezeti célok elérését segíti elő. Szervezetirányítás elválaszthatatlan eszköze.) | -"integritás nagykövetek hálózata", Az integrált és inkluzív irányítási megközelítés részeként az RMS / ICS szorosan össze-kapcsolódik a megfelelőségi funkcióval (Központi Governance, Risk & Compliance (GRC) szervezet). RMS célja.<br>- elmozdulás jelenik meg a tradicionális struktúráktól és merev hierarchiáktól a work@Audi kezdeményezés alapján (ld. Barabási)<br>- "content wheel" középen az Audi csoport stratégiával (pp. 62, 122, 123, 318) | - a (belső kontroll) rendszer alapelveket és eljárásokat, ill. megelőző és detektív ellenőrzéseket tartalmaz (p. 115)<br>- a hálózat szó: globális gyártási hálózat (p. 123), értékesítési hálózat (p. 28), rugalmas gyártási hálózat (p. 37, 42), globális K+F hálózat (p. 41), iparági, ill. iparágak közötti hálózatok (p. 80), mérnöki hálózat (p. 39), kontakt személyek hálózata (p. 83), Globális megfelelési területet összefogó hálózat (p. 86).<br>- lokális kapcsolattartók nemzetközi hálózata a dolgozók számára integritás, megfelelés és jogi témákban. Cél, megfelelés a megfelelési területre vonatkozó standardoknak (p. 83). A hálózat kiértékeli a feltett kérdéseket, és amennyiben szükséges, megfelelő intézkedéseket tesz.<br>Kiterjesztették az "integritás hálózatukat" is, mely az integritás további beágyazására törekszik a mindennapi rutinba (p. 83). | - a hálózatok szó a vállalat globális hálózatának (p. 5, 11) (termékek világszerte eljutnak a fogyasztókhoz), illetőleg információ biztonság (p. 36) kontextusában<br>- az információs rendszer és hálózat célja, az információszivárgás és jogosulatlan hozzáférések megakadályozása, ill. az információhoz való hozzáférés fejlesztése/elősegítése. szervereket, melyek leállása súlyos kimenetelű hatást okozhat, és melyek a biztonság szempontjából fontos adatokat, pl. személyes adatokat mentenek, egy zárható kiszolgálóhelyiségbe telepítik, szeizmikus izolátorokkal stb. (p. 36)<br>- bizalmas információ-ellenőrzési/ információ kontroll promóciós értekezlet; az egész Suzuki-csoport információ-ellenőrzési / információ kontroll rendszerének megerősítése (p. 36)<br>- ISO 27001 minősítést szerzett 2020-ban. (p. 36) | A hálózatok szó a kereskedői hálózat kontextusában jelenik meg (pl. pp. 7, 30, 37). |

Forrás: az éves beszámolók alapján a szerző szerkesztése.

## 5. Következtetések

A szakirodalmi elemzésben feltárt előzetes várakozások megjelennek a vállalatok éves beszámolói alapján végzett tartalomelemzés során. A vizsgált vállalatok egy intenzív transzformációs folyamatban vesznek részt, mely összvállalati szinten alkalmazkodást kíván meg úgy a rendszerek, mint az emberi erőforrások stratégiai kezelése során is.

A hálózati struktúra visszatükröződik az üzleti modell szintjén, jellemző a globális hálózatszerű működés. A hálózatos jelleg a belső vállalati folyamatokban is megjelenik, mint például az információbiztonság hálózatszerű kezelése során. A vállalati védelmi vonalak – üzleti folyamatokba ágyazott kontrollok, kontroll- és megfelelés funkciók és külső/belső auditok – szintén hálózatszerűen jelennek meg a vállalati működésben. Az irányítás, a megfelelés, és a kockázatkezelés (GRC) funkciók integrált kezelése jellemző, és szerepük domináns. A kontroll funkció a vállalati kockázatkezeléssel együtt jellemzően stratégiai jelentőségű támogató pillérként jelenik meg. A belső kontrollrendszer egyes elemei – a kontrollkörnyezet, kockázatértékelés, kontrollok, információs és kommunikációs folyamat, és monitoring – összefüggő rendszert képezve a vállalati biztonsági rendszer komplex, az egész vállalatot átszövő, behálózó elemei. A belső kontrollrendszer és kontroll funkció megjelenik szabályzatok szintjén is. A vállalati - üzleti, logisztikai és technológiai - folyamatok szabályozása, leírása, és a működés megfelelő monitorozása a kívánt biztonsági szint elérését segíti. A belső kontrollrendszer egyes elemei szorosan összekapcsolódnak, és megfelelő működés esetén az egyes elemek

egymást erősítik. Az autóipari vállalatok esetében a dízelkibocsátási botrány példázza, hogy az esetleges hibák, „rések a pajzson" kontrollhiányosságokra világítanak rá. A vezetőség adekvát válasza, megfelelő javító intézkedések szükségesek az észlelt hiányosságok „orvoslására", a belső kontrollrendszer korszerűsítésére és fejlesztésére. Egyes esetekben mindez a korábbi hiányosságokon túlmutató rendszerfejlesztéseket, egy komplex tanulási folyamatot, a szervezeti kultúra, valamint a kontrolltudatosság fejlesztését is eredményezheti. A nem megfelelő cselekedetekkel szembeni tudatosság, az integritás, az etikai elvek követése és a vállalati kultúra a vállalati biztonsági háló „lágy" eleméhez, az emberi tényezőkhöz köthetőek.

A hálózatszerű működés megjelenik a vállalati működésben és a biztonsági rendszerekben is. Hálózatszerűen működnek a vállalati működés alrendszerei, mint a kockázatkezelés, vagy a kontrolling tevékenység. A biztonság hálózatának megteremtéséhez kontrollok szükségesek, melyek a kockázatkezelési tevékenység eredményei. A belső kontrollrendszer hálózatszerűen működik, hálózatszerűen összekapcsolódó és egymást erősítő elemekből áll. A belső kontrollrendszer erősíti a vállalatbiztonságot, ezáltal értéket állít elő. A belső kontrollrendszer integráló jellegű, kapcsolódik a vállalati stratégiához, a vállalati működés valamennyi szintjén megjelenik, része a vállalati folyamatoknak és az üzleti célok érdekében szükséges. A vállalati folyamatok hálózatába épített kontrollok a belső kontrollrendszer építőkövei, melyek a vállalat kontrollhálózatát képezik. A kontrollhálózat tartópillérei az információs és kommunikációs technológiák, a rendszerek, és a folyamatokat működtető emberi tényező. A vállalati biztonsági háló „kemény" és „lágy" elemeinek együttesen kell, hogy biztosítsák a folyamatok biztonságát és a hosszú távú sikeres vállalati működést.

## Irodalomjegyzék


Anderson, R. J., Frigo, M. L. (2020): Creating and Protecting Value, Understanding and implementing Enterprise Risk Management

Anthony, R. N., Govindarajan, V. (2009): *Menedzsmentkontroll-rendszerek*. Panem Kft.

Audi AG Annual Report. (2020). <https://www.audi.com/en/company/investor-relations/annual-reports.html>

Bakacsi, G. (2018): A hálózatoké a jövő. In: Aczél, P. Csák, J. & Z. Szántó, O. (szerk.), *Társadalmi jövőképesség – Egy új tudományterület bemutatkozása*. Budapest, Budapesti Corvinus Egyetem Társadalmi Jövőképesség Kutatóközpont, pp. 269–300.

Barabási, A. L., Albert, R. (1999): Emergence of scaling in random networks. *Science* 286 (5439), pp. 509–512. https://doi.org/10.1126/science.286.5439.509

Barabási-Albert, L. (2006): A hálózatok tudománya: a társadalomtól a webig, *Magyar Tudomány*, 2006/11, p1298. <http://www.matud.iif.hu/06nov/03.html>

Barabási-Albert, L. (2008): *Behálózva – A hálózatok új tudománya*. Helikon Kiadó

Blahó, A., Czakó, E., Poór, J. (szerk.). (2016): *Nemzetközi menedzsment*. Akadémiai Kiadó. https://doi.org/10.1556/9789630597548.

Castells, M. (2010): *The Rise of the Network Society*. Wiley-Blackwell A John Wiley & Sons, Ltd. Publication.

Chambers, R. (2020): New IIA Three Lines Model Offers Timely Evolution of a Trusted Tool, Internal Auditor, <https://iaonline.theiia.org/blogs/chambers/Pages/New-IIA-Three-Lines-Model-Offers-Timely-Evolution-of-a-Trusted-Tool.aspx>

Chikán A. (2020): *Vállalatgazdaságtan*. Akadémiai Kiadó. https://doi.org/10.1556/9789634545897.
Chikán, A., Demeter, K. (2004): *Az értékteremtő folyamatok menedzsmentje*. Aula Kiadó
Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004): Enterprise Risk Management - Integrated Framework Executive Summary, <https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf>
Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013a): Internal Control - Integrated Framework Executive Summary, <https://www.coso.org/documents/990025p-executive-summary-final-may20.pdf>
Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013b): COSO Internal Control — Integrated Framework Principles. <https://www.coso.org/documents/coso-icif-11x17-cube-graphic.pdf>
Daimler Group Annual Report. (2020): <https://www.daimler.com/documents/investors/reports/annual-report/daimler/daimler-ir-annual-report-2020-incl-combined-management-report-daimler-ag.pdf>
Dobák M., Antal Z. (2016): *Vezetés és szervezés*. Akadémiai Kiadó. https://doi.org/10.1556/9789630598262.
European Court of Auditors. (2019): The EU's response to the „dieselgate" scandal, Briefing paper. <https://www.eca.europa.eu/lists/ecadocuments/brp_vehicle_emissions/brp_vehicle_emissions_en.pdf>
Francsovics, A. (2011): Vezetői számvitel és controlling elektronikus jegyzet. Óbudai Egyetem Keleti Károly Gazdasági Kar Budapest
Graneheim, U. H., Lindgren, B. M. & Lundman, B. (2017): Methodological challenges in qualitative content analysis: A discussion paper, *Nurse Education Today*, 56, pp. 29-34.
Groupe PSA Annual Report. (2019): <https://www.groupe-psa.com/en/publication/2019-annual-results/>
Gyulavári T., Mitev A. Z., Neulinger Á., Neumann-Bódi E., Simon J., Szűcs K. (2017): *A marketingkutatás alapjai*. Akadémiai Kiadó. https://doi.org/10.1556/9789630598880.
Hall, J. (2007): Internal Auditing and ERM: Fitting in and Adding Value, The Institute of Internal Auditors Research Foundation, <https://global.theiia.org/about/about-the-iia/Public%20Documents/Sawyer_Award_2007.pdf>
Híradó.hu. (2018): Csúcson a magyarországi autógyártás, <https://hirado.hu/belfold/gazdasag/cikk/2018/08/04/csucson-a-magyarorszagi-autogyartas-nem-most-kezdodott/>
Institute of Internal Auditors (IIA). (2013): The Three Lines of Defense in Effective Risk Management And Control January 2013 Position Paper, pp. 1–7.
Institute of Internal Auditors (IIA). (2020): The IIA's three lines model An update of the Three Lines of Defense Position Paper
Institute of Internal Auditors. (n.d.): The IIA's New Three Lines Model An update of the Three Lines of Defense
ISACA Control Objectives for Information and related Technology - COBIT: COBIT 5, COBIT 2019
ISO/IEC 15504-5:2012 Information technology – Process assessment – Part 5: An exemplar software life cycle process assessment model
Jelen, T., Mészáros, T. (2018): *Tervezés*. Akadémiai Kiadó. https://doi.org/10.1556/9789634542193.
Kadocsa, Gy. (2009). *Menedzsment mérnöki ismeretek*. Amicus Kiadó
Kelemen-Erdős, A., Mitev, A. (2017): Holisztikus szolgáltatásélmény - vendég-utazás és kölcsönös értékteremtés dimenziói az art- és romkocsmák példáján. *Marketing és Menedzsment*, 50(3-4), pp. 88–101.
Kelemen-Erdős, A. (2019): Dead-end development or real progress? Paradigm shift initiatives in marketing theory. In: Živan, Ž. (szerk.) *An international serial publication for theory and practice of Management Science*: IMCSM Proceedings, University of Belgrade, pp. 26–38.
Kemendi, A. (2021): HR process safety & security in the industry 4.0. era, *Bánki Közlemények* (Bánki Reports), 4 (1)
Kemendi, A. (2022): Integrált kockázatkezelés, *Biztonságtudományi Szemle*, 4 (1)

Lindgren, B.-M., Lundman, B., Graneheim, U. H. (2020): Abstraction and interpretation during the qualitative content analysis process, *International Journal of Nursing Studies*, 108, https://doi.org/10.1016/j.ijnurstu.2020.103632.

Kertész, J. (2006): Súlyozott hálózatok: a tőzsdétől a mobiltelefóniáig, *Magyar Tudomány*, 2006/11, p.1313. http://www.matud.iif.hu/06nov.html

Maczó, K. (2007): Controlling a gyakorlatban Kempelen Farkas Hallgatói Információs Központ, Digitális Tankönyvtár

Malhotra, N. K., Simon J. (k. m.). (2009): *Marketingkutatás*. Akadémiai Kiadó

Michelberger, P., Kemendi, A. (2020): Data, Information and IT Security - Software Support for Secucity Activites, *Problems of Managment in the 21st Century*, 15 (2), pp. 108–124.

Mitchell, S. L. (2007): GRC360: A framework to help organisations drive principled performance. *Int J Discl Gov* 4, 279–296, https://doi.org/10.1057/palgrave.jdg.2050066

OCEG. (n.d.): What is GRC?, <https://www.oceg.org/about/what-is-grc/>

Poór J. (szerk.) (2017): *Menedzsment-tanácsadási kézikönyv*. Akadémiai Kiadó. https://doi.org/10.1556/9789634540113.

Suzuki Annual Report. (2020). <https://www.globalsuzuki.com/ir/library/annualreport/pdf/2020/2020.pdf> <https://www.globalsuzuki.com/ir/library/annualreport/pdf/2020/2020_fs.pdf>

Technical Department of ENISA Section Risk Management ENISA. (2006): Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools