INTEGRATED RISK MANAGEMENT | INTEGRÁLT KOCKÁZATKEZELÉS

KEMENDI Ágnes[1]

Abstract

In order to maintain a long-term successful operation, complex security challenges need to be managed by companies. With the proliferation of information and communication technologies (ICTs), more and more risks are emerging. The quality of the risk management process is crucial. Integrated risk management includes the management of ICT risks at a strategic level. The publication examines the role of risk management and discusses risk management systems, methods, and potential ways of working. The publication focuses on the sales process and reviews corporate risks and possible controls; and it builds the risk matrix of a fictitious company in the form of a case study on ICT risks. The risk management process must be continuously operated as part of the company's strategic considerations, and risks must be assessed and managed on a cycle basis. Managing the risks associated with particularly large-scale projects is essential for successful corporate operations. Risk management contributes to the successful and secure operation of companies in the long run, which requires significant resources to be considered.

Keywords

integrated risk management; risk matrix; ICT; control; sales

Absztrakt

A vállalatok komplex biztonsági kihívásait a hosszú távú sikeres vállalati működés érdekében kezelni kell. Az információs és kommunikációs technológiák (IKT) intenzív térnyerésével újabb és újabb kockázatok merülnek fel. A kockázatkezelési folyamat minősége meghatározó. A kockázatok stratégiai szinten történő integrált kezelése magában foglalja az IKT kockázatok stratégiai szinten történő kezelését is. A publikáció a kockázatkezelés szerepét vizsgálja, a vállalati kockázatokból kiindulva tárgyalja a kockázatkezelési rendszereket, módszereket és lehetőségeket, továbbá az értékesítési folyamatra fókuszálva áttekinti a vállalati kockázatokat, és lehetséges kontrollokat, és az IKT kockázatokra vonatkozóan esettanulmány jelleggel felépíti egy fiktív vállalat kockázati mátrixát. A kockázatkezelési folyamatot körfolyamat jelleggel a vállalati stratégiai megfontolások részeként folyamatosan kell működtetni. A jelentős volumenű projektekkel járó kockázatok kezelése a sikeres vállalati működéshez elengedhetetlen. A kockázatkezelési folyamat a hosszú távon sikeres és biztonságos vállalati működéshez járul hozzá, amely mögötti számottevő erőforrás-ráfordítást mérlegelni szükséges.

Kulcsszavak

integrált kockázatkezelés; kockázati mátrix; IKT; kontroll; értékesítés

[1] kemendi.agnes@@uni-obuda.hu | ORCID: 0000-0002-6452-8563| PhD. Student Óbuda University Doctoral School on Safety and Security Sciences | PhD. hallgató Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A sikeres vállalati működés szempontjából meghatározó a vállalati kockázatkezelés szerepe, a kockázatok feltárásának folyamata, a várható valószínűségek azonosítása, és a még elfogadható kockázat mértékének meghatározása. A vállalatok folyamat-szervezésével kapcsolatos kockázatok átfogó, szisztematikus áttekintésével a szervezeti kockázati tényezőkről nyerhető információ. Az érintett területek, kockázatok, és hibaforrások feltárása, valamint a kockázatkezelési eszközök alkalmazása a hosszú távú sikeres vállalati működéshez elengedhetetlen. Az általános vállalati kockázatkezelés rendszerén belül az informatikai kockázatok értékelése kulcsfontosságú. Az IKT-k a vállalati folyamatok szerves részévé váltak. Az IKT technológiák alkalmazása vállalati értéknövelő tényezőként jelenhet meg, hozzájárulva a piaci versenyképességhez, és naprakészséghez. A rendszer, ill. szoftver-implementáció mögötti beruházási döntések megfigyelése képet ad a vállalati stratégiai megfontolásokról is. A publikáció célja az integrált kockázatkezelési megközelítésen alapulóan ismertetni a vállalati kockázatokat, keretrendszert teremteni a vállalati kockázatok strukturálásához és értékeléséhez. A publikáció középpontba helyezi az IKT-k (információs – és kommunikációs technológiák) szerepét az integrált kockázatkezelés keretei között. A publikáció a vállalati kockázatok áttekintésén keresztül vezeti fel a tématerületet, és vizsgálja a kockázatkezelési keretrendszereket és szabványokat, azok eszköztárait, és megjelenését a vállalati gyakorlatban. A publikáció a vállalati kockázatokat integrált megközelítéssel mutatja be; a vállalati értékesítési folyamat példáján keresztül ismerteti a főbb kockázatokat és lehetséges kontrollokat, valamint esettanulmány jelleggel levezeti egy elektronikus kereskedelmi (e-kereskedelmi) piacra lépési projektben érintett fiktív vállalat IKT kockázati mátrixának elkészítésének folyamatát, és lehetséges kockázatkezelési megoldásokat azonosít.

VÁLLALATI KOCKÁZATOK ÁTTEKINTÉSE

A kockázatok elleni védelem az egész szervezet működését áthatja, ebből kifolyólag a szükséges és elégséges védelmi háló több szinten is megjelenik a kapcsolódó kockázatokhoz kötődően. A védelem kérdésköre stratégiai jelentőségű, ennek részterületei: személy- és vagyonvédelem, az adat-, információ- és információtechnológiai védelem, az integritási, korrupciós és egyéb humán kockázatok kezelése, az üzletbiztonság, az üzletmenet-folytonosság és a váratlan havária események (kockázatok) kezelése, illetve azok elhárítása [1].

A potenciális kockázatok belső -, és külső kockázatok formájában vannak jelen. Külső kockázatok a jogszabályi kockázatok, országkockázat, hitel-/kamat-/árfolyamkockázatok, beszállítói/partner kockázat, ügyfélkockázatok, természeti-, környezeti kockázat, biztosítási kockázatok [1]. A belső kockázatok a szervezeti működésre vezethetőek vissza, melynek részei a berendezések meghibásodásával kapcsolatos technológiai kockázatok, vagyoni-, gazdálkodási-, likviditási- és adósságkockázatok, reputációs kockázatok, informatikai kibertér és információs technológia, HR, valamint az etikai és korrupciós kockázatok is [1]. A vállalati életben az IKT-hoz kapcsolódó projektek a szervezeti változás motorjaiként jelennek meg. Ezek a projektek - a kapcsolódó bizonytalanság, illetőleg a szervezetre, annak eredményességére gyakorolt hatásai miatt - megfelelő kockázatkezelést tesznek szükségessé. A biztonság az alkalmazásfejlesztők számára a fejlesztés során sokszor nem elsődleges prioritás, így az alkalmazások jóváhagyása és bevezetése során erre különös tekintettel kell

lenni. A technológiai fejlesztésekkel párhuzamosan biztonsági kérdések folyamatos kezelése is szükségessé válik.

Az ipar 4.0. kontextusában az információbiztonság, és vele együtt az IKT biztonság szerepe nő, és meghatározó a hosszú távú sikeres vállalati működés szempontjából. Az IKT technológiák biztonságtechnikai szempontból számos „rést" hagynak nyitva, melyek támadási célpontok lehetnek. Az IKT biztonság a vállalatok számára stratégiai kérdéssé, illetőleg céllá vált, melyhez kötődően megfelelő „védelmi" terv készítése, és működtetése vált szükségessé a kockázatkezelési folyamat részeként. IKT projektekhez kapcsolódóan a reális projektterv, a projekt kezdetén különösen alapos kockázatelemzés, és - kezelés, a bizonytalansági tényezők alapos feltárása és számbavétele, gyökérokok feltárása, valamint a folyamatos visszacsatolások (monitoring) a siker kulcstényezőiként jelennek meg.

A rendszerek és folyamatok működtetése során információ-biztonsági elvek követése és kontrollok működtetése szükséges. A megfelelően kontrollált folyamatok a vállalatbiztonság megteremtését segítik. Ehhez azonban jól kiépített támogató infrastruktúra kiépítése, működtetése és monitorozása szükséges. Fontos a teljesség, teljeskörűség, valamennyi érintett vállalati folyamat feltérképezése és lefedése, mely megvalósítása szétaprózott, fragmentált folyamatok esetében nem várt nehézségekbe ütközhet, és különös odafigyelést kíván.

KOCKÁZATKEZELÉSI KERETRENDSZEREK ÉS SZABVÁNYOK

A kockázatkezelés hagyományos és vállalati szintű kezelése között határozott különbség van [2]. A két kockázatkezelési megközelítés közötti alapvető különbségeket a KPMG LLP. cég foglalta össze, és bemutatja, hogy a hagyományos kockázatkezelési megközelítés leginkább a kockázatok kezelésének folyamatos és reaktív rendszere [3]. A vállalati kockázatkezelés célja, hogy egy olyan keretrendszert teremtsen, amely képes biztosítani, hogy a vállalat a kockázatokat, és bizonytalanságokat kezelni tudja [4].

A kockázatkezelés folyamata a vállalatok stratégiai fejlesztésének része, és azt a legmagasabb szinten kell meghatározni. Az integrált kockázatkezelés értelmében valamennyi kockázatot értékelni, kontrollálni, és monitorozni kell a vállalat kitettségének megfelelően [4]. Az ISO 31000 kockázatkezelési szabvány a kockázatot a bizonytalanság vállalati célokra való hatásaként értelmezi [5; 6], mindez rámutat arra, hogy a kockázatkezelés a vállalati stratégiai célok szintjén integráltan kezelendő. A vállalati szintű kockázatkezelés során a kockázatok az üzleti stratégia kontextusába vannak helyezve, és „a kockázat mindenki felelőssége", mellyel szigorúan elhatárolódik a megközelítés attól, hogy a szervezet tagjai arra hivatkozhassanak, hogy mindez nem tartozik az ő felelősségi körükbe [3]. A kockázatkezelés integrált keretrendszere azt a lényegi összefüggést mutatja be, amely a vállalati stratégiai célok megvalósítása és az IKT rendszerek szerepe - vállalati üzleti célok -, vezetői döntéshozatal -, valamint a stratégiai versenyelőny támogatása [7] – között húzódik.

A szabványok, pl. ISO 31000 kockázatkezelési szabvány erőteljesen befolyásolják a kockázat, és biztonság területet, annak ellenére, hogy erőteljes kritikai hangok kérdőjelezik meg a minőségüket [8]. Az ISO 31000 szabvány értelmében a kockázatkezelés célja értékteremtés és annak védelme. Az integrált kockázatkezelés ISO 31000 szerinti megvalósítása segíti a vállalatot céljai elérésében, és a reziliencia megteremtésében negatív hatások esetén [9]. A szabványok elősegítik a transzparenciát, az összehasonlíthatóságot, és ezáltal a költséghatékonyabb ellenőrzést is. A szabványokban a hatályuk alá tartozó terület pontosan le

van fektetve, ezáltal beazonosítható, hogy mire vonatkozik, és mire nem. Nem elvárható, hogy taxatív megoldást kínáló lexikont keressünk benne, hanem inkább egy jógyakorlatokat tartalmazó keretrendszerként érdemes rájuk tekinteni, amit adaptálni kell.

A COSO keretrendszer a vállalati célokat stratégiai, operatív, riporting és megfelelési célok szerint értelmezi. A COSO keretrendszer a belső kontrollrendszer integritását mutatja be, és szemlélteti, hogy az üzleti célok - stratégiai, operatív, riporting és megfelelési célok – érdekében milyen kontrollfolyamatok valósulnak meg a különféle szervezeti szinteken [10]. A COSO vállalati kockázatkezelés integrált keretrendszere (COSO Enterprise Risk Management – Integrated Framework) fókuszba helyezi a kockázatkezelést. A COSO ERM keretrendszer a kontrollkörnyezet, célok felállítása, események azonosítása, kockázatértékelés, kockázati válaszok, kontrolltevékenységek, információ és kommunikáció, és monitoring elemeket tartalmazza [10].

Az informatikai biztonság a vállalati biztonság része. Az informatikai rendszerek a vállalati folyamatokról adnak állapotjelentést, és a vállalati stratégia mindennapi megnyilvánulásaként is értelmezhetőek. Az IKT technológiák hatékony alkalmazása értéket állít elő, hozzájárul az üzleti célokhoz, és ezáltal a hosszú távú vállalati sikerességhez. Az informatikai kockázatok kulcskockázatok a vállalati biztonság szempontjából, melyek kezeléséhez speciális kockázatkezelési keretrendszerek nyújtanak támaszt.

A COSO keretrendszernek is része az információ és kommunikáció, azonban mint IT folyamatspecifikus funkcionális területre vonatkozóan több szabvány és ajánlás is alkalmazható, mint a CObIT 5.0 az IT irányítás- és menedzsment keretrendszere és a NIST 800-53-as amerikai biztonsági és adatvédelmi ellenőrzések dokumentum [11; 12].

Az információbiztonsági irányítási rendszer az átfogó irányítási rendszernek az információvédelmet biztosító része, amely figyelembe veszi a működési kockázatokat [13]. Az információbiztonság területére vonatkoznak az ISO/IEC 2700x információbiztonság-irányítás szabványai. Az információbiztonság kockázatmenedzsmenttel foglalkozó szabványa az ISO/IEC 27005 szabvány, mely információbiztonsági kockázatokra vonatkozik, pl. IT vagyonelemek, fenyegetések, meglévő folyamatszabályozások, sérülékenységek, következmények [14].

A CObIT (Control Objectives for Information and related Technology) alkalmazása többek között az IT kockázatkezelés megvalósítását segíti.

A CObIT 5 alapelvek és annak megvalósítását segítő tényezői lehetővé teszik a szervezet számára, hogy IT beruházásait a céljaival összhangba hozza, hogy a beruházásokon keresztül realizálni tudja azok értékét. Az alapelvek – az érintettek igényeinek kielégítése; a vállalat teljes körű lefedése; egyetlen integrált keretrendszer alkalmazása; holisztikus megközelítést lehetővé tétele, és az irányítás (governance) és menedzsment szeparálása – lehetővé teszik az irányítás és menedzsment holisztikus keretrendszerének megteremtését, mely megvalósulását az elvek, szabályok és keretrendszerek; folyamatok; szervezeti struktúrák; vállalati kultúra, etika és viselkedés; információ, szolgáltatások, infrastruktúra és alkalmazások, valamint humán erőforrás, képességek és készségek teszik lehetővé [11].

A CObIT 5 frissített változata, a CObIT 2019 hat alapelve átstruktúrálva és pontosítva jeleníti meg az eredeti öt alapelvet: értékteremtés az érintettek számára; holisztikus megközelítés, dinamikus irányítási rendszer, az irányítás és menedzsment külön funkciók; vállalati igényekre szabott, és teljes körű (end-to-end) irányítási rendszer [15]. Az irányítási rendszer jelenti az integrált keretrendszert.

A COSO és CObIT keretrendszerek folyamatleírásai az ISO/IEC 15504-2 Információs technológia – folyamatképesség-felmérés (Software Process Improvement and Capability dEtermination (SPICE)) szabvány követelményeinek megfelelő folyamat referencia modellek felállítására is alkalmasak [16; 17].

A keretrendszerek megjelenítik azt, hogy a vállalati kockázatkezelési folyamatok egyes elemei összekapcsolódnak, azok integráltan kezelendők, beleértve az IKT folyamatokat.

Kockázatértékelés [18]

A kockázatértékelés során az események hatásának és valószínűségének alapján hozzárendelt értékeket kockázati mátrixon lehet táblázatba foglalni, ill. kockázati térképen lehet ábrázolni. A kockázati mátrix egy táblázat. A kockázati térkép egy ábra, ahol az egyes kockázatok helyét a tengelyeken hozzárendelt értékek határozzák meg.

A kockázati mátrix és a kockázati térkép esetében is a két tengely ugyanaz, valószínűség és súlyosság. Az egyes események kockázata általában (bekövetkezés valószínűsége) x (bekövetkezés hatása) [19].

A kockázati tűréshatároknak megfelelően a kockázatok lehetnek:

- Lehetőség – alacsony kockázat, ahol egyes kontrollok „elengedésével" költségcsökkentésre nyílik lehetőség, ill. kockázatosabb területekre lehet fókuszálni.
- Normál, elfogadható kockázat – ahol jellemzően semmi extra tevékenységre nincs szükség, a jelenlegi kontrollokon, ill. folyamatokon felül.
    - Nem elfogadható kockázat – emelkedett kockázat, amely az elfogadható kockázat szintjét meghaladja, és mitigációt, ill. egyéb adekvát választ követel meg szoros határidőn belül.
    - Egyáltalán nem elfogadható kockázat – jóval meghaladja az elfogadható kockázat szintjét, és azonnali kockázatra adott választ követel meg.

Az azonosított kockázatokhoz kapcsolódóan meg kell határozni a kockázati választ, melyet számos tényező befolyásol. Ilyen tényezők:

- társuló költségvonzat, pl.: biztosítási költség kockázatmegosztás esetén, vagy a kontrollok bevezetésének költsége mitigáció esetén;
- kockázat pozíciója a kockázati térképen, azaz milyen a gyakorisága és nagyságrendje;
- társaság kockázatmenedzsment folyamatának érettsége (minél érettebb, annál szofisztikáltabb megoldás lehet célravezető);
- kockázati válasz eredményessége, azaz mennyire képes csökkenteni a kockázat gyakoriságát, ill. mértékét;
- kockázati válasz hatékonysága, azaz a kockázati válasz relatív előnyei más IT-val kapcsolatos beruházásokhoz, ill. más kockázati válaszokhoz képest.

A vállalat által alkalmazott kockázatkezelési stratégia összefügg a vállalat általános stratégiájával [20]. A különféle kockázatokhoz eltérő kockázati válaszok szükségesek (kockázatkerülés, kockázatcsökkentés/mitigáció, kockázatmegosztás / átruházás, kockázat elfogadása) [18; 20; 21; 22; 23; 24]. Az egyes kockázati válaszok adott körülmények esetén megfelelőek (ld. 1. Táblázat: Kockázatra adott válaszok).

Kockázatra adott válasz	Alkalmazási terület
Kockázatkerülés	a kockázatot jelentő tevékenység megszakítása, ill. a kockázatot jelentő körülményekből való kilépés. Jellemzően magas, v. extrém kockázatok, amelyek nem könnyen mitigálhatóak. Alkalmazása: amikor más kockázati válasz nem megfelelő pl.: elutasítani egy olyan projektben való részvételt, aminél jelentős a kudarc kockázata; elkerülni az ingatlanvásárlással járó kockázatokat, ahelyett bérelni; terrorizmussal sújtott régió elkerülése; jogi, vagy szabályozói kockázatok, amik a kockázatelkerülést teszik szükségessé
Kockázatcsökkentés/ Mitigáció	a kockázat felderítését követően a kockázat gyakoriságának és/ vagy hatásának csökkentésére intézkedéseket tesznek pl.: hatáskörök elkülönítésével (Segregation of duties) kapcsolatos „konfliktusok" mitigálása, amennyiben a feladatkörök elkülönítése nem valósítható meg; biztonsági intézkedések; szabályzatok
Kockázatmegosztás/ Átruházás	a kockázat gyakoriságának vagy hatásának csökkentését jelenti a kockázat egy részének átruházása vagy más módon történő megosztása, mely nem mentesíti a vállalatot a kockázatoktól, de bevonja másik fél készségeit a kockázat kezelésébe és csökkentheti a kockázatok esetleges pénzügyi következményeit, pl.: IT-val kapcsolatos biztonsági eseményekre vonatkozó biztosítás megkötése; az informatikai tevékenység egy részének kiszervezése vagy IT projektkockázat megosztása a szolgáltatóval rögzített áru megállapodások révén; szerződéses klauzúrák, ill. egyéb formális megállapodások; szakértő alkalmazása
Kockázat elfogadása	nem történik ilyenkor intézkedés a kockázathoz kapcsolódóan, az esetleges nem kívánatos esemény felmerülésekor történik könyveli el a vállalat a veszteséget. IT-val kapcsolatos kockázatot csak a menedzsment, és üzleti folyamatok tulajdonosai fogadhatnak el az IT funkcióval együttműködve, ill. az IT funkció által támogatva. Az álláspontot kommunikálni kell az szenior menedzsment és az igazgatóság felé.

Táblázat: Kockázatra adott válaszok, Saját szerkesztés, készült: [18; 20; 21;22;23;24] alapján

Az erőforrás-korlátok miatt a kockázati válaszok priorizálása válik szükségessé. A kockázati válaszokat ezért kategorizáljuk aszerint, hogy

- „gyors győzelem" (hatékony és eredményes kockázati válasz magas kockázatra)
- üzleti hatástanulmány készítése (alapos elemzést és vezetői döntést kívánó kockázati válasz esetén, pl.: költségesebb vagy komplikáltabb kockázati válasz magas kockázat esetén vagy hatékony és eredményes kockázati válasz alacsony kockázat esetén)
- késleltetés (költséges válasz alacsony kockázatra).

VÁLLALATI KOCKÁZATOK INTEGRÁLT MEGKÖZELÍTÉSŰ BEMUTATÁSA

COSO ERM fókuszú kockázati modell

A COSO ERM fókuszú kockázati modell (2. Táblázat: COSO ERM fókuszú kockázati modell) a stratégiai, megfelelési, riporting és operatív kockázatok szerint kategorizálva mutatja be a kockázatokat, melyek a COSO kocka vertikális oszlopain jelennek meg. A besorolások mentén további alkategóriák képezhetőek [3]. A modell átfogóan kezeli a vállalati kockázatokat, és egyben rámutat arra, hogy a vállalati folyamatok összefüggő rendszert képeznek. A stratégiai szemlélet a vállalati működést meghatározza. A kontrollkörnyezet hatással van a vállalati működésre.

Kockázatok

Stratégiai	Megfelelési	Riporting	
Külső	Külső megfelelés	Külső jelentések	
- változás a törvényekben és rendeletekben	- jogszabályi megfelelés - szerződéses megfelelés	- számviteli, - és pénzügyi jelentések	
- kormányváltás		- belső kontrollok - szabályozói jelentéstételi kötelezettségek	
- versenytársak	- adósságmegfelelés	- adózás	
- koncentráció	- peres ügyek		Információ
- gazdasági	- engedélyek		- hozzáférések
- hírnév	- etc.		- adatintegritás
- ipari			- infrastruktúra
- technológia			- elérhetőség
- politika			- etc.
Belső	Belső megfelelés	Belső jelentések	
- szövetségek kialakítása	- etika - csalás, jogellenes tevékenységek	- pénzügyi tervezés és előrejelzés - menedzsment jelentések	
- márka/ márkanév			
- üzleti stratégia	- szabályzatok	- teljesítménymérés	
- vevőelégedettség		- etc.	
- célmeghatározás/ összeghangolás			
- irányítás			
- piackoncentráció			
- árazás			
- termék			
- erőforrásallokáció			

(megjegyzés: a táblázat a következő oldalon folytatódik)

Operatív kockázatok			
Általános	Kereskedelmi	Pénzügyi	Emberi erőforrás
- beszerzés, és elidegenítés	- üzleti folyamatok	- tőke rendelkezésre állása	- jogosultsági szintek
- üzemszünet	- szállítás	- tőke költsége	- változási hajlandóság
- üzletmenet-folytonosság	- emissziós kreditek	- cash flow/ likviditás	- kollektív tárgyalások
- kapacitás	- üzemanyag árak	- készpénzkezelés	- kommunikáció
- katasztrófa események	- üzemanyag beszerzés	- partnerkockázat, hitelkockázat	- emberi erőforrás elosztás
- környezeti kockázatok	- piaci likviditás	- hitelminősítés	- vezetőség/kulcs munkavállalók
- egészség - és biztonság	- portfolió optimalizáció	- árfolyamkockázat	- emberi erőforrások toborzása
- elavulás	- elszámolás és számlázás	- pénzügyi piacok	- szervezeti struktúra
- üzemi hatékonyság	-kereskedelmi ügylet befogadása és végrehajtása	- kamatláb	- kiszervezés
- ellátási lánc kezelése	- átadás nehézségei	- nyugdíjfinanszírozás	- teljesítményösztönzők
- terrorista támadás		- kockázatáthárítás	
- időjárás			

2. Táblázat: COSO ERM fókuszú kockázati modell, Forrás: [3], p8.
(Risk model example, Institute of Internal Auditors)

Az értékesítési folyamat kockázatainak integrált szemléletű áttekintése

A vevői elégedettség stratégiai cél. Az ipar 4.0. és pandémia világában a kereskedelmi csatornák átrendeződése meghatározó hatással bír a vállalatok értékesítési folyamataira. Az IKT megoldások szerepe és az e-kereskedelem szerepe nő [25]. „A megújulásra való képesség előfeltétele a gazdasági szereplők életképességének [26].”

A vállalati működés elsődleges folyamata a „bevételszerzési”, azaz értékesítési folyamat, melynek kockázatait a következőkben átfogóan tekintem át teljes körű (end-to-end) szemlélettel. A vállalati bizalmi kultúra hozzájárul a gördülékeny folyamatokhoz, a folyamatok sebessége nő, a költségek csökkennek [27]. Kontroll szempontból a sikeres működést jellemzi a „bízz, de ellenőrizz” szemlélet, ahol a jól működő folyamatok mellett jelen vannak a megfelelő kontrollok és ellenőrzések. Kontroll alatt azokat a tevékenységeket értem, melyek biztosítják, hogy a folyamat hibamentesen, ill. adott elfogadható tűréshatáron belüli hibaszázalékkal következik be.

A bevételszerzési folyamat során a vállalati stratégia valósul meg. A stratégiai szinten azonosított kockázatok meghatározóak a bevételszerzési/értékesítési folyamat szempontjából (ld. 2. Táblázat: COSO ERM fókuszú kockázati modell). Úgyszintén igaz ez az integrált kockázatkezelési modell további vetületeire, azaz a megfelelési, riporting és operatív kockázatokra. A rendszerek a vállalati folyamatok működését biztosítják, ebből kifolyólag a folyamatban lévő kockázatok összekapcsolódnak a mögöttes IKT kockázatokkal.

Az értékesítési folyamat kapcsán tipikus kockázatok, ill. kockázatos területek: fiktív ügyfél létrehozása; törzsadatok módosítása; a megrendelések nem rendelkeznek megfelelő jóváhagyással; alkalmazott árazás nem megfelelő, nem jóváhagyott, jogosulatlan engedmények, kenőpénz elfogadása; értékesítési csoport teljesítményértékelése; tranzakciók nem a megfelelő periódusra lettek könyvelve; ügyfélminősítési folyamat, új, ill. meglévő ügyfelek

minősítése; esedékességet meghaladó vevői követelések; egyedi tranzakciók kezelése; visszáru kezelése; jogosultsági szintek; hozzáférés-kezelés és hatáskör-átlépések.

Az azonosított kockázatokhoz kapcsolódóan meg kell határozni azok hatásait, és a bekövetkezés gyakoriságát. A kockázati mátrix kétdimenziós táblázatban szemlélteti az azonosított kockázat következményét, ill. a kockázat bekövetkezési valószínűségét, gyakoriságát. A kockázati mátrix felosztása általában 3x3 és 7x7 között változik [19]. Egy lehetséges kockázati mátrixot mutat be a 3. Táblázat: Kockázati mátrix példa.

Valószínűség	Következmény				
[0; 1]	jelentéktelen [0; 1)	mérsékelt [1; 2)	közepes [2; 3)	súlyos [3; 4)	kritikus [4; 5]
elhanyagolható [0]					
csekély (0; 0,1)					
alacsony, nem valószínű [0,1; 0,4)					
valószínű [0,4; 0,6)					
nagyon valószínű [0,6; 0,9)					
majdnem biztos [0,9; 1]					

Jelölések:
elhanyagolható kockázat, lehetőség kontrollerőforrás átcsoportosítására
alacsony, elfogadható kockázat - jellemzően nincs szükség a jelenlegi kontrollokon, folyamatokon felül extratevékenységre, a kockázat felvállalható
normál, elfogadható kockázat - megfelelő folyamatkontrollok, kontrolltevékenységek szükségesek, intézkedés egyéni mérlegelés alapján
magas, nem elfogadható kockázat - kockázatkezelési eszközök szükségesek szoros határidőn belül
kritikus, egyáltalán nem elfogadható - azonnali kockázati választ követel meg

3. Táblázat: Kockázati mátrix példa, Saját szerkesztés, készült [18; 19; 28; 29] felhasználásával

A folyamatlépések elválaszthatatlan részét jelentik a technológiai megoldások, ebből eredően az IKT kockázatok az értékesítési folyamatokhoz szorosan kapcsolódnak. A folyamat megfelelő működéséhez a kockázatok kezeléséhez kontrolltevékenységek szükségesek. Ugyanaz a kontrolltevékenység több kockázat kezelését is biztosíthatja. A kontrollelemek a „tudatos", „biztonságos" szervezet folyamatain keresztül jelennek meg. A kontrollok hatékony érvényesülése akkor valósul meg, ha az rutin jellegű, és működése véletlenül sem marad el.

Az ipar 4.0 fejlesztéseivel lépést tartó innovációra nyitott vállalatok esetében a kockázatkezelési megoldások a vállalati folyamatok transzformációján keresztül valósulnak meg, mely ideális feltételeket teremt jól működő, hatékony kockázatkezelési folyamatok megvalósítására. Az 1. Melléklet: Értékesítési folyamat kockázatai és kontrolltevékenységei c. az értékesítési folyamat főbb területeire vonatkozóan mutat be egy-egy kockázati területet, és tipikus kontrolltevékenységeket, valamint jógyakorlatokat [30].

Esettanulmány vállalati IKT kockázati mátrix készítéséhez
OTC vállalat e-kereskedelmi piacra lépési projekt – IKT kockázati mátrix

Az esettanulmány célja a kockázati mátrix készítésének lépéseinek egyszerűsített bemutatása. OTC vállalat egy fiktív, stabil bevétellel rendelkező kiskereskedelmi hálózat, mely a pandémia idején lépést tartva a vevői igények átrendeződésével az e-kereskedelmi csatornájának fejlesztésére fókuszált. OTC vállalat korábban aktívan nem volt jelen az e-kereskedelmi piacon a pandémiát megelőzően. Kezdetleges jelleggel csak webes felületről indított e-mailes megrendeléseket fogadtak. Vevői köre széles spektrumot lefed, azonban direkt értékesítési ügyfélköre jellemzően a 30-60 éves korosztály, akik vásárlásaik során jellemzően 50-50%-ban készpénzes, ill. bankkártyás fizetést választottak. OTC vállalat számára a pandémia hatására a bevételek direkt értékesítés során olyan mértékben csökkentek, hogy megkérdőjeleződött az üzletmenet-folytonosság elvének biztosítása. A vállalati vezetés stratégiai célként tűzte ki az erőforrások e-kereskedelmi piacra történő átcsoportosítását, és elsődlegesen az e-kereskedelmi csatornából történő jövedelemszerzést.

Az új stratégiához kapcsolódóan IKT beruházások történtek. A projekt célja, hogy az online értékesítés megfelelő keretei biztosítva legyenek. A rendelkezésre álló költségvetés korlátozott volt. A beruházás a legszükségesebbek területekre korlátozódott. A beruházások és fejlesztések rövid időn belül lezajlottak, és a vállalat megkezdte az e-kereskedelmi tevékenységet.

A vállalat tapasztalt szereplőként volt jelen a piacon.

A munkavállalók elkötelezettek. Az ún. Pulse survey alapján a munkavállalói elégedettség szint magas. A jogszabályi környezet ismerete és a megfelelési prioritás mindig fontos prioritás volt a vállalat számára. Jogszabályi megfelelés területén felkészült volt és megfelelt a vállalat az e-kereskedelmi kívánalmaknak. A személyes adatok védelme (GDPR) területén GDPR 30. cikk szerinti adatkezelési nyilvántartással, valamint adatvédelmi szabályzattal rendelkezik. A kiépített adatvédelmi rendszer megfelelőnek tekinthető. Jellemző az adatvédelmi, ill. általános biztonsági tudatosság.

A vállalat az üzembe helyezett új e-kereskedelmi rendszer működése során biztonságot veszélyeztető hatásokkal, fenyegetésekkel, ill. biztonsági incidensekkel találta szembe magát. A gyors beruházási - és üzembe helyezési folyamat következtében biztonsági rések keletkeztek. A vállalat vezetősége a belső vizsgálatok gyökérok elemzése során megállapította, hogy egyes bekövetkezett biztonsági események a biztonsági rendszer sebezhetőségére, annak hiányosságaira, ill. gyengeségeire utalnak, azokat a meglévő biztonsági szabályzatok és folyamatok már nem fedték le. Továbbá több biztonsági hiányosság együttes bekövetkezése fokozott problémát okozhatott, ahogy azt a Reason által ismertetett svájci sajt modell példája is illusztrálja [31; 32]. Megállapítást nyert, hogy a projektkockázatok kezelése során nem került valamennyi érintett kockázat feltárásra, és kezelésre, ebből kifolyólag a biztonsági rendszert erősíteni kell. A biztonsági terv részeként a vállalat az aktuális kockázatok alapján új IKT kockázati mátrixot készített, és meghatározta a lehetséges kockázatkezelési lehetőségeket.

A 4. Táblázat: IKT kockázatok áttekintése – OTC vállalat tartalmazza az azonosított kockázati területeket, a kockázat bekövetkezésének becsült valószínűségével és hatásával. (A hatás-, és valószínűség értékek szubjektív értékek az esettanulmány kockázati mátrixának felvázolásához.)

Jel	Kockázat	Kockázathoz kapcsolódó megjegyzések	Hatás valószínűsége (0,1,2,3,4,5)	Hatás (1,2.3,4,5)
A	**adatbiztonsági kockázatok (A)** - nem jogosult egyén hozzáférése, - nem jogosult felhasználó módosítja, - nem hozzáférhető a szükséges időpontban és szükséges időtartam alatt	Az információbiztonság megteremtését a bizalmasság, sértetlenség és elérhetőség elvei (CIA) határozzák meg.	3	5
B	**adatvesztés (B)**	Adatbiztonsági kockázat. Az üzletmenethez szükséges, és annak során keletkező adatok rendelkezésre állásának kockázata. Az adatok tárolásának, adott törvényi határidőn belüli visszakereshetőségének, ill. auditálhatóságának biztosítása sérülhet. Az adatvesztés elkerülésének fontossága.	2	5
C	**adatszivárgás (data leakage) (C)**	Adatbiztonsági kockázat. Annak a kockázata, hogy az adatok illetéktelen kezekbe kerülnek, és azáltal anyagi kár, reputáció vesztés következik be. A fokozódó online jelenlét miatt Kapcsolódik az emberi erőforrás kockázathoz is.	1	5
D	**emberi erőforrás (D)**	A biztonsági események bekövetkezése sokszor az emberi tényezőhöz köthető, mely lehet egyszeri véletlen hiba, szándékos mulasztás vagy tudatos manipuláció (social engineering) következménye is.	2	4
E	**jogszabályi nem megfelelés (E)**	A jogszabályi környezet ismeretének és a megfelelésnek követelménye. E-kereskedelmi tevékenységhez kapcsolódóan biztosítani kell, hogy a vállalat az online értékesítés felületénaz EU szintű online vitarendezési platformhoz, az Online Dispute Resolution, azaz ODR-hez linket tartalmazzon és email címe rendelkezésre álljon (Kemendi, 2021).	2	5

Jel	Kockázat	Kockázathoz kapcsolódó megjegyzések	Hatás valószínűsége (0,1,2,3,4,5)	Hatás (1,2.3,4,5)
F	**GDPR nem megfelelés, büntetések, hírnévkockázat (F)**	A személyes adatok védelme (GDPR, EU General Data Protection Regulation 2016/679) területén jelentős adatvédelmi követelményeknek kell megfelelni.	2	5
G	**bankkártyaadatokkal és szenzitív azonosító adatokkal kapcsolatos kockázatok /PCI DSS/, bankkártya csalások (G)**	A bankkártya-adatok biztonságos kezelését globális adatbiztonsági sztenderd követeli meg (PCI DSS – Payment Card Industry Data Security Standard).	2	5
H	**IKT kitettségek (H)**	A vállalati üzletmenet folyamatai információs és kommunikációs technológia (IKT) rendszerekben mennek végbe.	3	5
I	**IoT-vel kapcsolatos adatvédelmi és biztonsági kockázatok, kiber kockázatok (I)**	Az Internet of things (IoT) nagyfokú térnyerése és alkalmazása biztonsági kockázatokat rejt. Az internet vezérelt eszközök fejlesztése során a biztonsági kérdések gyakran háttérbe szorulnak, így a technológiai innovációk alkalmazásán keresztül létrejövő biztonsági rések kockázata magas.	2	5
J	**hálózati biztonság (J)**	A hálózati biztonság az IKT biztonság kritikus eleme. A hirtelen megnövekedett API adatforgalom következtében az API-n keresztüli adatforgalom biztonsága prioritás.	3	5
K	**biztonsági incidensek (K)**	A fenyegetések a vállalat sebezhetőségét kihasználva biztonsági eseményhez vezethetnek. A kockázat valós eseménnyé válik, és tényleges hatása tesz.	2	4
L	**üzletviteli zavarok pl. hardware hiba, tűzeset, árvíz, emberi erőforrás elvesztésének kockázata (L)**	A vállalati üzletmenet-folytonosságra váratlan, vis major esetek veszélyt rejthetnek. Ritka, azonban nagy hatású események.	1	5

4. Táblázat: IKT kockázatok áttekintése – OTC vállalat, Saját szerkesztés

A fenti kockázatokat (Jel=A, B,…,.L) a vállalat az alábbi kockázati mátrixban ábrázolta (5. Táblázat: IKT kockázati mátrix – OTC vállalat).

Valószínűség [0; 1]	Következmény jelentéktelen [1]	mérsékelt [2]	közepes [3]	súlyos [4]	kritikus [5]
elhanyagolható [0]					
csekély (0; 0,2)					C, L
alacsony [0,2; 0,4)				D, K	B, E, F, G, I
közepes [0,4; 0,6)					A, H, J
valószínű [0,6; 0,8)					
nagyon valószínű, gyakori [0,8; 1]					

Jelölések:

elhanyagolható kockázat, lehetőség kontrollerőforrás átcsoportosítására

alacsony, elfogadható kockázat - jellemzően nincs szükség a jelenlegi kontrollokon, folyamatokon felül extratevékenységre, a kockázat felvállalható

normál, elfogadható kockázat - megfelelő folyamatkontrollok, kontrolltevékenységek szükségesek, intézkedés egyéni mérlegelés alapján

magas, nem elfogadható kockázat - kockázatkezelési eszközök szükségesek szoros határidőn belül

kritikus, egyáltalán nem elfogadható - azonnali kockázati választ követel meg

5. Táblázat: IKT kockázati mátrix – OTC vállalat, Saját szerkesztés

Valamennyi kockázat a vállalat kockázati mátrixában súlyos, nem elfogadható, ill. kritikus, egyáltalán nem elfogadható következménnyel jár. A vállalat kockázatkezelési csoportja az azonosított IKT kockázatokhoz kapcsolódóan jellemző jógyakorlatokat határozott meg, amelyeket lehetséges kockázatkezelési javaslatként fognak értékelni, és a kockázatkezelési terv részeként bevezetni (6. Táblázat: IKT kockázatok és kockázatkezelési megoldások). A bevezetésre kerülő intézkedések eredményeként a vállalati vezetőség a kockázati szint csökkenését várja. Kockázatokkal arányos védelem kiépítése a cél.

Jel	Kockázat	Lehetséges kockázatkezelési javaslat
A	**adatbiztonsági kockázatok (A)** - nem jogosult egyén hozzáférése, - nem jogosult felhasználó módosítja, - nem hozzáférhető a szükséges időpontban és szükséges időtartam alatt	„zárt védelem” /IT-, fizikai-, és személyi biztonság/, hozzáférések minimalizálása, minimum funkció elve, négy szem elve, szabályzatok adekvát működtetése, technológiai megoldások adekvát beépítése /kockázatokkal arányos védelem/
B	**adatvesztés (B)**	biztonsági mentések/back up-ok, legutolsó biztonsági másolat visszatöltése, archiválás, hozzáférés-kezelés, logging
C	**adatszivárgás (data leakage) (C)**	„tiszta asztal” politika, IT eszközök- és adathordozók védelme, tréning, átvilágítás

Jel	Kockázat	Lehetséges kockázatkezelési javaslat
D	**emberi erőforrás (D)**	kiválasztás (HR kompetencia), átvilágítás, tréning, megfigyelés/monitorozás, elbocsátás, jelszó használat, titkosítás, limitált hozzáférés, felelősségi körök kialakítása, szabályzatok, folyamatok, munkafolyamatba épített kontrollok, változáskezelés, tudásmenedzsment, a tudás védelme, etikai kódex, etikai nagykövetek, a „vezetőség hangja”, példamutatás
E	**jogszabályi nem megfelelés (E)**	megfelelés ellenőrzése és tesztelése, auditok, belső folyamatok vizsgálata, „akció tervek” készítése, GRC szoftverek adekvát működtetése
F	**GDPR nem megfelelés, büntetések, hírnévkockázat (F)**	GDPR folyamatok, GDPR felelős
G	**bankkártyaadatokkal és szenzitív azonosító adatokkal kapcsolatos kockázatok /PCI DSS/, bankkártya csalások (G)**	biztonsági folyamatok, kontrollok, információbiztonsági szabályok, hálózatok és rendszerek biztonsága, tárolt kártyaadatok védelme, nyilvános hálózaton keresztüli adatforgalom titkosítása
H	**IKT kitettségek (H)**	kockázatkezelési terv, és kockázatok értékelése, szabályzatok, intézkedési tervek, monitorozás
I	**IoT-vel kapcsolatos adatvédelmi és biztonsági kockázatok, kiber kockázatok (I)**	hálózati adatforgalom kontrollja pl. biztonsági router, felhasználó azonosítás stb.
J	**hálózati biztonság (J)**	biztonsági átjárók, tűzfalak, vírusvédelem, API biztonság
K	**biztonsági incidensek (K)**	incidens kezelési folyamat, gyökérokok feltárása (teljes körű), intézkedési terv, monitorozás, folyamatdokumentáció-, és szabályzatok frissítése, kockázatkezelés (korai azonosítás, felismerés, ill. megelőzés)
L	**üzletviteli zavarok pl. hardware hiba, tűzeset, árvíz, emberi erőforrás elvesztésének kockázata (L)**	Üzletmenet-folytonosság menedzsment (BCM), Üzletimenet folytonossági – (BCP), és Katasztrófaelhárítási terv (DRP); erőforrás-tervezés, IT erőforrás-helyreállítási terv, tesztelés, folyamatos monitoring, incidens – és vészhelyzet szimuláció, hatástanulmány készítése, helyreállítási idő meghatározása

6. Táblázat: IKT kockázatok és kockázatkezelési megoldások, Saját szerkesztés [33] alapján

KÖVETKEZTETÉSEK

A kockázatkezelési folyamat alapvetően egy folyamatosan működtetett körfolyamat. Egyes események direkt indukálják azt. A projektkockázatok integrált szemléletű kezelése szükséges. A vállalati stratégiai tervekhez kapcsolódóan a kockázatokat értékelni, és kezelni kell. Az ipar 4.0. dinamikusan változó világában a vállalatok alkalmazkodási képessége fontos sikerkritérium. A változó környezethez való alkalmazkodásra, – ahol szinte csak a válto-

zás állandó – valamennyi üzleti-, ill. támogató funkciónak fel kell készülnie. Az üzleti stratégia változása - pl. erőforrás-átcsoportosítás egy új értékesítési csatornára - a sikeres projektmegvalósítás részeként adekvát kockázatkezelést követel meg. Az egyes kockázatkezelési lehetőségek erőforrás-ráfordításokkal járnak, melyet a vállalati vezetőségnek mérlegelni kell. A kockázatarányos védelem elve segíti a döntéshozatalt. A kívánt biztonsági szint megteremtését segíti a vállalati folyamatok leírása és szabályozása. A kockázatokat teljes körű (end-to-end) szemlélettel kell kezelni ahhoz, hogy valamennyi érintett terület feltárásra kerüljön, ezáltal csökkenthető annak a valószínűsége, hogy több hiba, ill. nem várt negatív esemény együttes bekövetkezése azok egyéni bekövetkezési valószínűségéhez képest jóval nagyobb kárt okozzon, pl. teljes rendszer, ill. folyamatleálláshoz vezet. A sikeres kockázatkezelés eredménye a kívánt biztonsági szint elérése.

ÖSSZEGZÉS

A publikációban bemutattam a főbb vállalati kockázatokat, és kockázatkezelési keretrendszereket, ill. a releváns szabványok funkcióját. A publikációban tárgyaltam a kockázatkezelési folyamat egyes elemeit, bemutattam az értékesítési folyamat specifikumait kockázatkezelési szempontból, és jógyakorlatokat fogalmaztam meg a kontrollkörnyezet kiépítésével kapcsolatban. Esettanulmány jelleggel bemutattam egy fiktív vállalat e-kereskedelmi piacra lépési projektjéhez kapcsolódó IKT területre fókuszáló kockázati mátrix készítését, és lehetséges kockázatkezelési megoldásokat ismertettem.

A hosszú távú vállalati sikeresség, és a biztonságos vállalati működés szorosan összekapcsolódik. Az ipar 4.0. világában a reziliencia, az alkalmazkodás képessége központi szerepet kap. A vállalat relatív biztonsága a sikeres működés alapja. A vállalat biztonságának kérdése stratégiai jelentőségű, összefonódik a kockázatkezeléssel, és kontrolltudatossággal. Az informatikai biztonság, és vele párhuzamosan az emberi tényező által generált kockázatok kezelése a szervezeti biztonsági rendszerében kiemelt jelentőséggel bírnak.

A kockázatkezelési folyamat a kockázatok azonosításán, értékelésén, és kockázatkezelési eszközök meghatározásán alapul. A sikeres kockázatkezelés értéket jelent a vállalat számára, a vállalat ezáltal eléri a kívánt biztonsági szintet. Az IKT kockázatok kezelését a vállalati stratégiával összhangban kell megvalósítani. A kockázatok integrált kezelése a vállalati stratégiához illeszkedik.

HIVATKOZÁSOK

[1] Kocziszky G., & Kardkovács K. (2020). *A compliance szerepe a közösségi értékek és érdekek védelmében.* Akadémiai Kiadó

[2] Banham, R. 2004. Enterprising views of risk management. *Journal of Accountancy 197* (6), 65-71.

[3] 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

[4] Dionne, Georges: *Corporate Risk Management: Theories and Applications,* John Wiley & Sons, Incorporated, 2019. ProQuest Ebook Central, ISBN 9781119583172

[5] ISO 31000: 2018 Risk management – Guidelines https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

[6] Trusted Business Partners Kft. (in Eds. Iványos János). (2014). *Kockázatkezelési kézikönyv.* 2014. http://www.trusted.hu/attachments/article/91/Kock%C3%A1zatkezel%C3%A9si%20K%C3%A9zik%C3%B6nyv%20v2.pdf
[7] Ahlan, A. R., & Arshad, Y. (2012). Understanding Components of IT Risks and Enterprise Risk Management, *Risk Management for the Future - Theory and Cases*, Jan Emblemsvag, IntechOpen, https://doi.org 10.5772/32023. Available from: https://www.intechopen.com/chapters/36108
[8] Aven, T., & Ylönen, M. (2019). The strong power of standards in the safety and risk fields: A threat to proper developments of these fields?, *Reliability Engineering & System Safety, 189*, pp. 279-286, https://doi.org/10.1016/j.ress.2019.04.035, https://www.sciencedirect.com/science/article/pii/S0951832018312250
[9] IWA 31:2020 (en) Risk management — Guidelines on using ISO 31000 in management systems, https://www.iso.org/obp/ui/fr/#iso:std:iso:iwa:31:ed-1:v1:en
[10] COSO. (2004). *Enterprise Risk Management – Integrated Framework*
[11] ISACA. (2012). *CObIT5. A Business Framework for the Governance and Management of Enterprise IT.*
[12] NIST Special Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations
[13] Fogarasi, A., & Szűcs. E. (2021). A szabványos irányítási rendszerek fejlődése, integrációja, *Biztonságtudományi Szemle, 3*(2), pp. 1-13
[14] Michelberger, P. (2018). *Információ-, folyamat- és vállalatbiztonság*, Óbudai Egyetem, Keleti Károly Gazdasági Kar
[15] De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations*, Springer Nature Switzerland AG.
[16] ISO/IEC 15504-2:2003(en)
Information technology — Process assessment — Part 2: Performing an assessment, https://www.iso.org/obp/ui/#iso:std:iso-iec:15504:-2:ed-1:v1:en
[17] Iványos, J., Roóz, J., & Messnarz, R. (2010). *Governance Capability Assessment. Using ISO/IEC 15504 for Internal Finacial Controls and IT management*. Proceedings of the MONTIFIC Project at the Conference of "The Current Financial Crisis and Competences to Address Problems on the European Market", pp.17-47., https://www.researchgate.net/publication/294428037_Governance_Capability_Assessment_Using_ISOIEC_15504_for_Internal_Financial_Controls_and_IT_Management
[18] ISACA. (2009). *The RiskIT Framework*, https://www.hci- itil.com/ITIL_v3/docs/RiskIT_FW_30June2010_Research.pdf
[19] Csordás, E. (2012). Fogalmi és értelmezési zavarok a kockázati mátrixok és kockázati térképek körül, *Hitelintézeti Szemle*, https://www.bankszovetseg.hu/Content/Hitelintezeti/254-271-csordas1.pdf
[20] Farkas, Sz., & Szabó, J. (2010). *A vállalati kockázatkezelés kézikönyve.* Dialog Campus
[21] Conrad, E., Misenar, S., Feldman, J. (2016). Chapter 2 - Domain 1: Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity), In Conrad, E., Misenar, S., & Feldman, J. (Eds.), *CISSP Study Guide* (3rd Edition, pp. 11-79). Syngress, https://doi.org/10.1016/B978-0-12-802437-9.00002-3

[22] Fennelly, L.J., & Perry, M. A. (2017). Assessing Risk and Vulnerabilities. in Fennelly, L.J., Perry, M. A. (Eds.). *Physical Security: 150 Things You Should Know* (2nd ed.)
[23] Peterson, K. E. (2010). Security Risk Management. *International Foundation for Protection Officers (IFPO): The Professional Protection Officer: Security Strategies, Tactics and Trends,* (2nd ed.), Butterworth-Heinemann, https://doi.org/10.1016/C2009-0-19898-7
[24] Purpura, P. P. (2013). Resilience, Risk Management, Business Continuity, and Emergency Management. *Security and Loss Prevention* (6th ed.)
[25] Kemendi, A. (2021). E-commerce safety and security in the industry 4.0 era, *National Security Review*, *2021(*1), https://www.knbsz.gov.hu/hu/letoltes/szsz/2021_1_NSR.pdf
[26] Takácsné György, K. (2017). Kihívások, esélyek, alternatívák (és a nem-növekedés tóriája – „degrowth"), in Takács, I. (Ed.), *Az együttműködési attitűdök gazdasági társadalmi hatótényezői az északmagyarországi régióban működő kkv-kban*. http://real.mtak.hu/54108/1/Tanulmanykotet_OTKA_K109026_u.pdf
[27] Takácsné György, K. & Benedek, A. (2016). Bizalmon alapuló együttműködés vizsgálata a kis- és középvállalatok körében, In Csiszárik-Kocsir, A. (Ed.), *Vállalkozásfejlesztés a XXI. században VI.*, pp. 379-390, Óbuda University, Keleti Faculty of Business and Management. http://kgk.uni-obuda.hu/sites/default/files/27_Benedek-Takacsne.pdf
[28] Ni, H., Chen, A., & Chen, N. (2010). Some extensions on risk matrix approach, *Safety Science*, *48*(10), pp. 1269-1278, https://doi.org/10.1016/j.ssci.2010.04.005, https://www.sciencedirect.com/science/article/pii/S0925753510001049
[29] MIL-STD-882E. System Safety. Department of Defense (USA). Standard Practice.
[30] Rao, S. R. (2014). Perspective SOX Controls - Driving Transformation of the Order-to-Cash Value Chain, Infosys Limited External Document, https://www.infosysbpm.com/offerings/functions/sales-fulfillment/white-papers/Documents/SOX-controls.pdf
[31] Reason, J. (1999). The 'Swiss Cheese' model
[32] Reason, J. (2000). Human error: models and management, *BMJ*, *320*(7237): 768–770. https://doi.org/10.1136/bmj.320.7237.768, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117770/
[33] Michelberger, P. & Kemendi, A. (2020). DATA, INFORMATION AND IT SECURITY - SOFTWARE SUPPORT FOR SECURITY ACTIVITIES, *PROBLEMS OF MANAGEMENT IN THE 21ST CENTURY, 15* (2), pp. 108-124. https://www.scientia-socialis.lt/pmc/files/pdf/108-124.Michelberger_Vol.15-2_pmc.pdf

TÁBLÁZATOK

MELLÉKLETEK

1. Melléklet: Értékesítési folyamat kockázatai és kontrolltevékenységei

1. Rendelésfelvétel		
Kockázati területek	**Kontroll tevékenység**	**Jógyakorlat**
nem teljes vagy nem pontos rendelési adatok	a hiányzó adatok pótlása, korrigálása	- a rendeléskezelési rendszer a vevő-, ár-, és termék törzsadatokkal összeköttetésben van; - a rendelési nyomtatvány kötelező mezők kitöltése hiányában nem küldhető el; - vevők tájékoztatása a rendelés során a várható feldolgozási időről - érvényes rendelési szám nélkül a rendelés nem kerül feldolgozásra
rendelés duplikált felvétele	a rendszer figyelmeztető üzenetet küld a duplikált rendelésfelvétel megelőzése érdekében	- a rendelések egymást követően számozottak, mely ellenőrzésre is kerül
rendelések feldolgozása a jóváhagyott hitelkereten felül (magasabb vevői kintlévőségek, -és leírások kockázata)	- rendelések automatikus blokkolása, a hitelkeret átlépése esetén - a blokkolt rendelések feloldására jóváhagyási folyamat	- rendelések jóváhagyása a minimális rendelési szabályzat, hitelkeret, termékre-és szolgáltatásra való jogosultság, beszerzés -és készlet rendelkezésre állás, átfutási idő és árazás, ügyfélpolitika szerint - új ügyfél esetén először a törzsadatok létrehozása szükséges, új rendelések ezt követően vehetők fel
magasabb diszkontráták alkalmazása az értékesítési csoport ad hoc kérései szerint	független verifikáció alkalmazása magasabb diszkontráták alkalmazása esetén	sztenderd diszkontráta beállítása, és alkalmazása a rendszerben különböző vevő-, és termék szegmensekre; valamennyi eltérő ráta esetében jóváhagyás szükséges

2. Számlázás		
Kockázati területek	**Kontroll tevékenység**	**Jógyakorlat**
nem, vagy késve generálódik számla a szállítmányokhoz	- szállítmány jóváhagyott kiadása alapján a raktárból, a rendszer automatikusan generálja a számlát azonos dátummal - szállítási dátum nem módosítható megfelelő szintű vezetői jóváhagyás nélkül	- előzetes szállítási értesítés küldése a vevőnek - szállítási konfirmációs dokumentumok scannelni és archiválni - manuális számlák megfelelő jóváhagyással készülhetnek - alacsony összegű készpénztranzakciókat vállalati hitelkártyás, vagy direkt debit-es tranzakcióval helyettesíteni - összevont számlázás a vevőknek - összevont csoportos fizetés lehetősége a vevőknek automatikus pénzallokációval a könyvelésben, ahol lehetséges
nem megfelelő ár, mennyiség, és egyéb információ feltüntetése a számlán	- rendszerbeállítás alapján a számlaadatok ellenőrzése a törzsadatok és a megrendelésadatok alapján. Nem érvényes adatok elutasításra kerülnek vagy egy függő tételeket tartalmazó file-ba, mely később korrigálható	workflow megoldás a vevővel való vitás tételek gyors rendezésére

3. Pénzbeszedés		
Kockázati területek	**Kontroll tevékenység**	**Jógyakorlat**
nincs nyomonkövetés az esedékességet meghaladó vevőkre	- vezető ellenőrzi a koros követeléseket, és összehasonlítja a beérkezett kintlévőségeket a periódus elején nyitott követelésekkel	- fizetési ígéretek rögzítése és nyomon követése,- jelentősebb vevőket ösztönözni arra, hogy fizessenek a termék kézhezvételekor a megrendelő alapján, ahelyett, hogy a számlára várnak, - amennyiben nem a számla teljes összege kerül kiegyenlítésre, azt azonnal eszkalálni kell, - elektronikus átutalási utasításokkal ellátott elektronikus fizetések feltöltése az értékesítési főkönyvbe, amelyek lehetővé teszik az automatikus párosítást
a beérkező pénz nem kapcsolódik az értékesítéshez, vagy nem megfelelő ügyfélszámlára lett könyvelve	- a beérkező pénz ügyfélszámlához rendelése az ügyfélnév, az ügyfélszám, és a számlaszám alapján történik, és csak nyitott számlákkal szemben	- Vevők menedzser felülvizsgálja valamennyi azonosítatlan banki befizetést - amennyiben a beazonosítás nem sikeres, átmenetileg az azonosítatlan/felosztatlan befizetések számlára kerül - a beszedési csoport felelőssége az azonosítatlan/felosztatlan befizetések számla "tisztítása"

4. Visszaküldések		
Kockázati területek	**Kontroll tevékenység**	**Jógyakorlat**
a visszaküldések nincsenek jóváhagyva, vagy azok nem felelnek meg a vállalati szabályzatnak	- a visszaküldött áru fizikai ellenőrzése, felülvizsgálata és a visszáru engedély (RMA - return merchandise authorization) jóváhagyása szükséges	- a jóváhagyási folyamat felgyorsítása valós idejű információk biztosításával a jóváhagyók részére - csak jóváhagyott visszatérítések kerülnek feldolgozásra - magas összegű kérelmek jóváhagyása jóváhagyási limittel rendelkező ügyfélmenedzser által, ill. alacsony összegű kérelmek automatikus jóváhagyása
a készpénzbevételek nem kapcsolódnak az értékesítéshez, vagy nem a megfelelő ügyfélszámlára lettek könyvelve	- a beérkező pénz ügyfélszámlához rendelése az ügyfélnév, az ügyfélszám, és a számlaszám alapján történik, és csak nyitott számlákkal szemben	Rendszer kiépítése a vevői igények és levonások nyilvántartására

Forrás: [30]