KPMG
cutting through complexity

INFORMATIKAI KOCKÁZATKEZELÉSI SZOLGÁLTATÁSOK

BCM-körkép 2012

Tanulmány az üzletfolytonosság-tervezés magyarországi helyzetéről
Fókuszban az üzletihatás-elemzés

kpmg.hu

Gaidosch Tamás
partner
T: +36 1 887 7139
E: tamas.gaidosch@kpmg.hu

Tisztelt Olvasó!

2011-ben a KPMG országos felméréssel értékelte, hogy a vezető magyarországi vállalatok és közintézmények hogyan kezelik az üzletfolytonosság (Business Continuity Management – BCM) kérdéskörét, milyen a szervezetek érettsége e területen. Mivel e témakörben Magyarországon még nem volt hagyománya a hasonló felméréseknek, célunk akkor egy átfogó körkép megalkotása volt. Az eredmények ismeretében láttuk az igényt a fókuszált kutatásokra is, ezért elhatároztuk, hogy 2012-ben az üzletfolytonosság-tervezés egy kulcsfontosságú területét, az üzletihatás-elemzést (Business Impact Analysis – BIA) vizsgáljuk közelebbről. Az idei felmérésünk is hasonlóan nagy érdeklődésre tartott számot, és úgy véljük, ugyanolyan izgalmas eredményekkel szolgál valamennyi hazai BCM-, IT- és kockázatkezelési szakember számára. Célunk továbbra is az, hogy ily módon is hozzájárulhassunk a hazai BCM-keretrendszerek fejlődéséhez.

Üdvözlettel:

Gaidosch Tamás

Tartalomjegyzék

Ha most csak egy oldalra van idő

Az első valóban széles körű hazai BCM-felmérés a tavalyi év során számos tanulságos megállapítással szolgált a BCM-keretrendszerek minőségéről, illetve e kockázatkezelési gyakorlat elterjedtségéről. Bár korábban is szándékunk volt egy rendszeres felmérés megvalósítása, az első felmérés sikere további motivációt adott a folytatáshoz. Így a 2012-es felmérésünk megmutatja a változásokat, a BCM-érettség elmúlt évben történt fejlődését, de ezúttal az üzletfolytonosság-tervezés kulcsfontosságú területére, az üzletihatás-elemzésre is nagy hangsúlyt helyeztünk. Fókuszált, 25 kérdésből álló online felmérésünket 77 szervezet töltötte ki, amelyek jellemzően ismét a pénzügyi társaságok közül kerültek ki, de szép számmal képviseltette magát az informatikai és telekommunikációs, az energia és a járműipari szektor is.

Ha az eredményeket összevetjük a tavalyi adatokkal, örömteli változás, hogy a résztvevők jóval nagyobb aránya, immáron kétharmada (2011-ben 31 százalék) rendelkezik kész BCM-keretrendszerrel. A részleteket tekintve azonban továbbra sem rózsás a helyzet: nem jellemző a BCM-specifikus szabványok szerinti tanúsítás, vagy a dedikált BCM-költségvetés, valamint a BCM-keretrendszerrel rendelkezők 60 százaléka szkeptikus a rendszer működőképességét illetően. Mi okozhatja ezt a bizonytalanságot? Egyrészt a résztvevők fele szerencsére még nem használta terveit, így nem is volt módjuk meggyőződni azok működőképességéről, másrészt a terveket nem is auditáltatták, így a bizonytalanságot az is okozhatja, hogy nincs független szakértői véleményük a rendszerről.

A résztvevők közül a BCM-mel már rendelkezők 25 százaléka nem készítette el üzletihatás-elemzését. Ők vajon mire alapozták terveiket? Ráadásul a BIA-val nem rendelkezők 41 százaléka gondolja úgy, hogy stabil és működőképes BCM-mel rendelkezik. Ez vajon lehetséges BIA nélkül is?

A válaszok részletes elemzése során örömmel konstatáltuk, hogy az üzletihatás-elemzések jellemzően folyamat-alapúak (75 százalék), és a többség a BIA elvégzése során a folyamatok különböző kiesési hatásaira, a kritikus erőforrások azonosítására és a folyamatok maximálisan megengedett kiesési idejére is figyelt. Azonosítottunk azonban olyan általános módszertani hibát, illetve az elfogadott legjobb gyakorlat követésének hiányát, ami jelentősen gátolhatja a precíz hatáselemzés elvégzését. Így például a maximálisan megengedhető adatvesztés mértékének meghatározására (Recovery Point Objective – RPO) vagy a BIA és a szolgáltatásiszint-megállapodások összhangjára igen kevesen ügyeltek.

Továbbra is bízunk benne, hogy felmérésünk kérdései és eredményei arra ösztönzik a résztvevőket, hogy tökéletesítsék BCM-keretrendszerüket, és ezáltal a következő felmérés során még pozitívabb képet adhatunk a hazai üzletfolytonosság-tervezési gyakorlatról.

If you only have time to read one page

After we completed the first comprehensive survey on the maturity and penetration of Business Continuity Management (BCM) systems in Hungary we discovered a number of thought provoking findings. Though we were already interested in establishing a regular survey, the success of our first initiative increased our interest substantially. With our 2012 survey we aimed at revealing the changes since last year and the development of BCM maturity levels. However, we also put a great emphasis on one of the key fields in BCM: the Business Impact Analysis (BIA). We created an online survey consisting of 25 questions that focus on this topic. Our survey was answered by 77 organisations. As previously, the majority of respondents are in the financial and insurance world, but there were numerous participants from the IT and telecommunications sectors as well as the energy and automotive industries.

When we compare the results with last year we are pleased to see a much larger portion of respondents (in 2011, 131 percent; in 2012, 66 percent) reporting to have a complete BCM framework. But, a deeper analysis casts a shadow on the results: it is unusual to certify against a BCM specific standard or to have a dedicated BCM budget. Furthermore, those having a BCM framework in place are not confident on its ability to work. What could cause this uncertainty? As half of the respondents have never used their BCPs, and the plans have not even been audited, there were no means to make sure the BCM indeed works in practice.

Fact: 25 percent of those respondents having a BCM framework in place did not prepare a BIA. What could serve then as a basis for their BCPs? Also, 41 percent of those having no BIA in place believe that their BCM framework is ready and works well. How is that possible without a BIA?

Looking more into the details, we were pleased to see that most BIAs are process-based (75 percent), and during the analysis the majority of organisations paid attention to different impacts of process outages, identification of critical resources and Maximum Tolerable Period of Disruption (MTPD). On the other hand, we identified some methodological flaws as well as ignorance of best practices that would be key for delivering a precise analysis. For instance, very few respondents considered defining the Recovery Point Objectives (RPO) or the harmonisation of the service level agreements and BIA.

We are confident that our initiative will have a motivational effect on organisations as our survey's questions and results encourage the participants to further improve their BCM frameworks. As a result, we expect that our next survey will reveal a significant improvement in the overall BCM practice within Hungary.

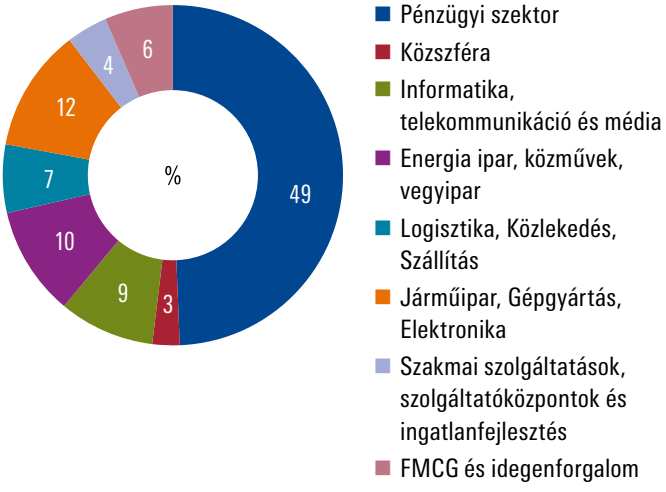
Miért és hogyan készítettük?

A BCM olyan nélkülözhetetlen eleme a kockázatkezelési szakemberek eszköztárának, melynek segítségével a szervezetek megelőzhetik vagy hatékonyabban kezelhetik a váratlan eseményeket, incidenseket. Milyen eseményekre és kockázatokra kell felkészülni? Mekkora károkat okozhatnak ezek? Mely kritikus folyamatok és szolgáltatások folytonosságát kell feltétlenül biztosítani?

E kérdésekre egy átfogó és részletes üzletihatás-elemzés adhatja meg a választ. Hogy kiderítsük, a gyakorlatban milyen érettségi szintet értek el a hazai szervezetek az üzletihatás-elemzés tekintetében, felmérést készítettünk 2012. május és július között. Ismét számos magánvállalatot és állami szervezetet kértünk fel, hogy csatlakozzanak a kutatásunkhoz, és töltsék ki online kérdőívünket.
A megkeresésünkre végül 77 szervezet – jellemzően közép- és nagyvállalat – válaszolt az alábbi iparágakból:

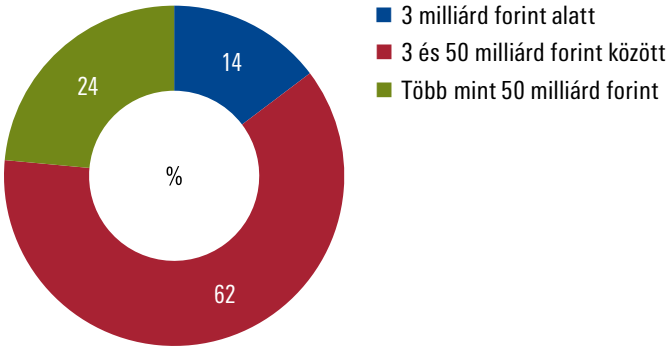
- energiaipar, közművek, vegyipar;
- FMCG és idegenforgalom;
- informatika, telekommunikáció és média;
- járműipar, gépgyártás, elektronika;
- közszféra;
- logisztika, közlekedés, szállítás;
- pénzügyi szektor;
- szakmai szolgáltatások, szolgáltató-központok és ingatlanfejlesztés;

A felmérésben részt vevők szektoriális eloszlása



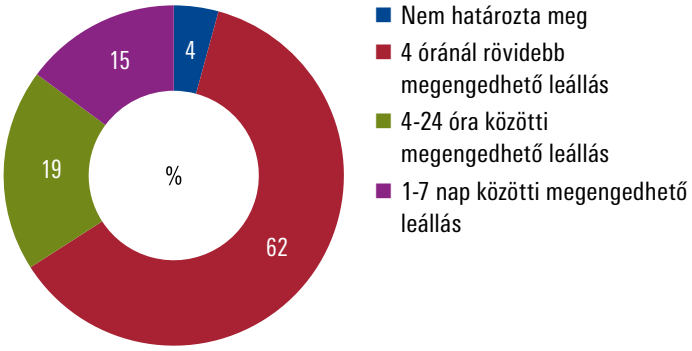
A résztvevők majdnem fele 500 fő feletti létszámú nagyvállalat, és közel negyedük éves árbevétele 50 milliárd forint feletti.

A felmérésben részt vevők eloszlása árbevétel szerint



A résztvevők közül üzletihatás-elemzést 38-an készítettek BCM-programjuk keretében, ami csupán a válaszadók fele. Ők azonban jellemzően időkritikus tevékenységekkel rendelkeznek, 62 százalékuk folyamatait jellemzően 4 órán belül helyre kell állítani, és összesen 80 százalékuk folytat 1 napon belül helyreállítandó tevékenységet.

A felmérésben részt vevők tevékenységeinek időkritikussága



Akik nem kívántak részt venni a felmérésben, ismét jellemzően az információ bizalmasságára hivatkoztak.

Köszönjük a résztvevők hozzájárulását! Reméljük, nemcsak ők, hanem valamennyi üzletfolytonosság-tervezéssel, informatikával vagy kockázatkezeléssel foglalkozó szakember is hasznosnak találja felmérésünk eredményeit.

A 2011-es év folyamán a KPMG átfogó, országos felméréssel értékelte, hogy a vezető hazai vállalatok és közintézmények hogyan kezelik az üzletfolytonosság kérdéskörét. 2012-ben az üzletihatás-elemzésre fókuszálva megismételtük a felmérést, és szeretnénk ezzel hagyományt teremteni.

Előszó gyanánt – Miért fontos a BIA?

Tavalyi felmérésünk előszavában Jakab Péter, az MKB bankbiztonsági igazgatója így fogalmazott: *„Egy hitelintézet komplex módon értelmezett biztonságáért felelős vezetőjeként bizton állítom: a hitelintézetek termékei és szolgáltatásai szinte kivétel nélkül számos üzleti folyamat, illetve különféle emberi és technikai erőforrás rendelkezésre állását, összhangját igénylik."*

De vajon melyek ezek az üzleti folyamatok, emberi és technikai erőforrások, továbbá milyen rendelkezésre állási kritériumok vonatkoznak rájuk, és milyen összhang szükséges közöttük az említett termékek és szolgáltatások zavartalan biztosításához? Úgy hisszük, az üzletfolytonossági keretrendszer és tervek kidolgozásakor ez az első, és talán nem túlzás azt állítani, hogy az egyik legfontosabb kérdés, amely rendszerint felmerül. Tapasztalataink alapján a szervezetek egy része úgy véli, hogy ezen kritikus szolgáltatásokat és folyamatokat, valamint a támogató erőforrásokat könnyen és gyorsan képes azonosítani, akár egy rövid workshop alkalmával. Vajon ők rendelkeznek elegendő információval a kritikus folyamatok és erőforrások pontos és teljes körű azonosításához? Rendelkeznek a szervezet minden területére vonatkozóan olyan operatív szintű rálátással, hogy képesek legyenek ezeket nemcsak megnevezni, hanem a rendelkezésre állási kritériumokat, a megengedett kiesési időket, a folyamatok és erőforrások közötti összetett függőségeket is meghatározni? Vajon képesek a rendelkezésre állást fenyegető kockázatok és a jelenlegi üzletfolytonossági képességek pontos azonosítására?

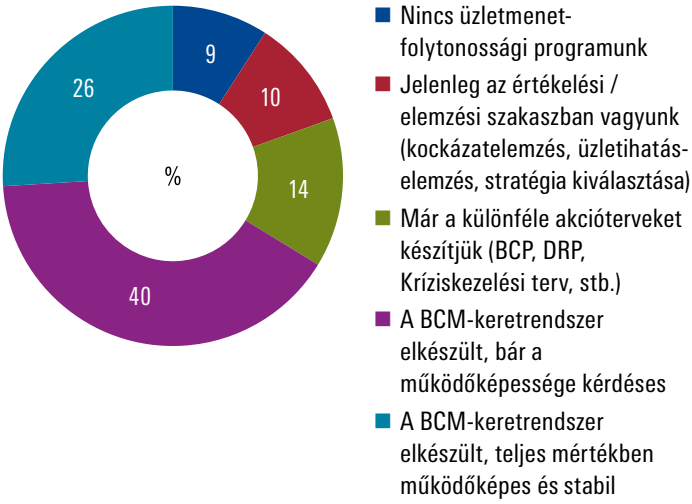
Az üzletfolytonosság fenntartása csak úgy biztosítható, ha részleteiben ismerjük üzleti folyamataink működési sajátosságait, az ezeket támogató erőforrásokat (például informatikai rendszerek, külső szolgáltatók), és az ezek kiesését okozó főbb kockázatokat.

Egy átfogó, alapos és minden részletre kiterjedő üzletihatás-elemzés nélkül aligha. Az üzletihatás-elemzés a kidolgozandó üzletfolytonossági és katasztrófa helyreállítási tervek alapját jelenti. E nélkül, vagy az elemzés felületes kivitelezése esetén nagy a valószínűsége, hogy a kritikus folyamatokat és erőforrásokat, valamint az üzletfolytonossági kockázatokat nem pontosan vagy teljes körűen tárják fel. Ennek pedig az lesz az eredménye, hogy az informatikai infrastruktúra és rendszerek hibatűrő megoldásai nem felelnek meg az üzleti követelményeknek, és az üzletfolytonossági tervek hiányosak lesznek, vagyis nem nyújtanak elégséges megoldást a nem várt események kezelésére.

Mi változott tavaly óta – Átfogó diagnózis

Bár idei kérdőívünk alapvetően az üzletihatás-elemzésre fókuszált, érintettünk néhány, a tavalyi felmérésben is szereplő kérdést, melyek a szervezetek általános BCM-érettségére vonatkoztak. Lássuk, milyen változások történtek tavaly óta. (A tavalyi és idei felmérések eredményeit összehasonlíthatónak gondoljuk, mivel a tavalyi és idei populáció számossága és összetétele között nincsenek jelentős különbségek).

BCM-státusz összefoglaló



A résztvevők 9 százaléka nem alakította ki üzletfolytonossági keretrendszerét, ez gyakorlatilag megegyezik a tavalyi eredménnyel. E választ megjelölők a pénzügyi vagy emberi erőforrások, valamint a felsővezetői támogatás hiányát jelölték meg elsődleges okként. A kérdőívet kitöltők 25 százaléka még csak az üzletfolytonossági terv kialakításánál tart, viszont a fennmaradó kétharmad úgy gondolja, hogy a BCM elkészült. Ez ugyan jelentős pozitív változás az előző évi 35 százalékhoz képest, azonban az üzletfolytonossági keretrendszerrel rendelkezők több mint fele (60 százalék) véli úgy, hogy esetükben a BCM működőképessége kérdéses, azaz ugyan rendelkeznek BCM-mel, de annak minősége és használhatósága nem garantált.

Mi jelenthetne garanciát? Például ha a BCM már a gyakorlatban is megállta a helyét, vagy egy auditnak vetették azt alá. Nos, a válaszadók több mint fele az elmúlt évben nem használta a terveit, és 61 százalékuk még nem auditálta BCM-keretrendszerét (a BCM-üket teljes mértékben működőképesnek és stabilnak ítélők fele szintén nem végzett auditot). Tanúsítvánnyal is csak a válaszadók töredéke rendelkezik, és ők sem BCM-specifikus tanúsítványt szereztek (pl. BS 25999 vagy ISO 22301) hanem ISO 27001-et, amely szabvány csak egy részterületként foglalkozik a BCM-mel.

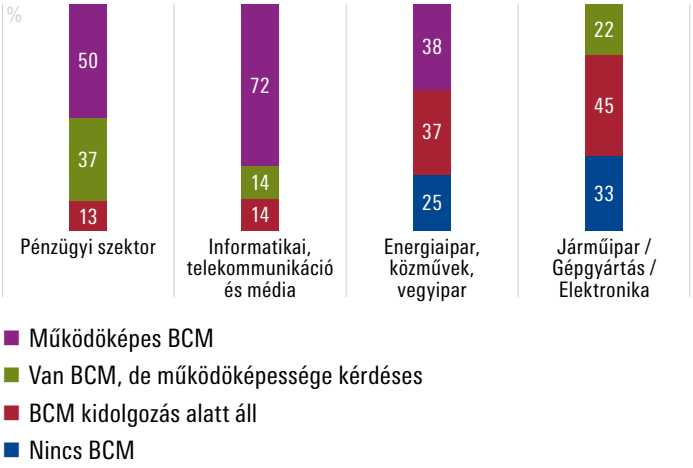
A BCM-státuszok aránya jelentős szórást mutat, ha szektoronként külön vizsgáljuk az eredményeket.

Az erősebben szabályozott pénzügyi szektorban ugyan 87 százalék rendelkezik BCM-mel, de csak a felük véli úgy, a BCM stabil és működőképes.

Az IT-ra szintén erősen támaszkodó informatikai, telekommunikációs társaságok és a média esetében kedvezőbb az arány, több mint kétharmaduk rendelkezik működőképes tervekkel. A termelő vállalatoknál azonban hozzávetőleg 60-80 százalék a kidolgozott BCM-mel nem rendelkezők aránya, pedig az incidenskárok mérséklése mellett az ellátási láncokban betöltött fontos szerepük okán is lenne létjogosultsága a jól kidolgozott üzletfolytonossági terveknek.

A szektorális eredmények értékelésekor idén is számításba kell venni azt, hogy a BCM iránt érdeklődő szervezetek valószínűleg nagyobb arányban vettek részt a felmérésben, kissé felülreprezentáltak, vagyis a valós kép ennél sajnos borúsabb lehet.

Szektoriális BCM-státusz



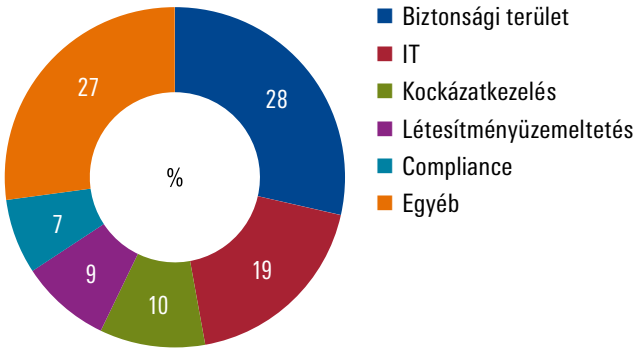
Németh Adrienn
BCM-szakértő
MKB Bank Zrt.

„Annak érdekében, hogy a BCM-el kapcsolatos teendők ne sikkadjanak el, és a BCM-ünk stabil, működőképes és naprakész maradhasson, a kríziskezelés központi felelősei, koordinátorai mellett legalább olyan fontosnak tartjuk, hogy az üzleti és háttér területeknek is legyenek a vezetők által kijelölt és támogatott BCM-felelősei (és helyettesei), akik az adott szakterület alternatív folyamatainak, BCM-dokumentumainak naprakészen tartásáért felelnek."

A kidolgozott és a kialakítás alatt álló BCM-mel rendelkezők túlnyomó többsége (80 százaléka) nem rendelkezik dedikált BCM-költségvetéssel. Véleményünk szerint ez is jelzi a BCM-re szánt csekély figyelmet, és összecseng a tavalyi eredményekkel, ahol a legtöbb válaszadó eseti alapon határozta meg a BCM-re fordítandó költségkeretet. A BCM-re szánt költségek a felmérés alapján leginkább az informatikát, a biztonságért felelős részleget vagy az érintett üzleti területet terhelik.

Örömmel tapasztaltuk, hogy a válaszadók között a BCM-ért felelős területek arányát tekintve 33 százalékról 19 százalékra csökkent az IT dominanciája. Az IT mellett továbbra is jellemzően a biztonságért felelős terület kezében van a BCM-irányítás (29 százalék), mely mellett a kockázatkezelés, a létesítményüzemeltetés és a compliance szerepel még nagyobb arányban; ez, a létesítményüzemeltetés kivételével, amely főként a termelő vállalatoknál gyakorlat, pozitív változás. Sajnos a válaszadók 27 százalékánál továbbra sincs kijelölt, a BCM-ért felelős terület, vagy az más, kevésbé operatív vagy releváns üzleti területen található, mint például a pénzügy, a minőségügy, a belső ellenőrzés vagy a szervezés.

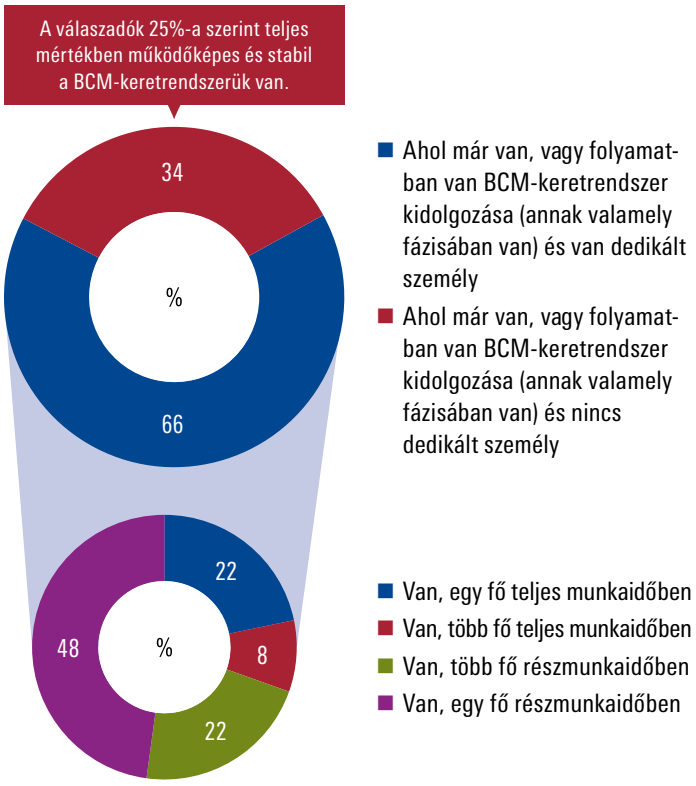
A BCM-ért felelős terület



Dedikált felelős terület hiányában dedikált költségvetés sincs, így egy esetleges incidens költsége jellemzően az IT-t vagy az érintett területet terheli.

Megvizsgáltuk azt is, hogy a BCM-mel már rendelkező vagy azt éppen kialakító szervezeteknél van-e a BCM-ért dedikáltan felelős személy. A válaszadók mintegy 66 százalékánál van dedikált felelős, bár többségében (70 százalékuk esetén) csak részmunkaidőben foglalkozik a feladattal. Komoly problémát látunk abban, hogy egyrészt a felmérésben részt vevők 34 százalékánál nincs BCM-ért felelős szakember, másrészt ennek ellenére negyedük mégis úgy gondolta, hogy teljes mértékben működőképes és stabil a BCM-keretrendszere. Vajon megoldható ez megfelelően kialakított felelősségek nélkül?

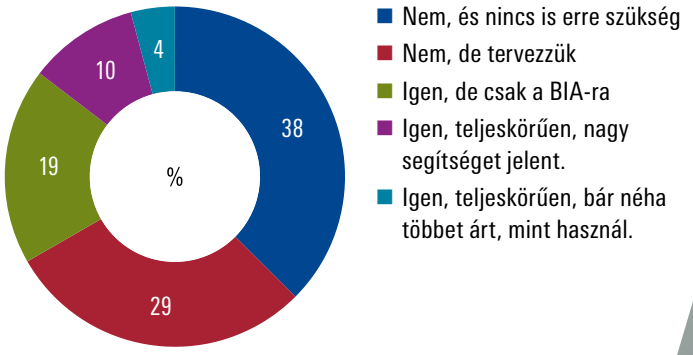
Dedikált BCM-felelős



Ismét igyekeztünk megtudni, a társaságok figyelembe veszik-e, hogy üzleti partnereik rendelkeznek-e BCM-mel. A helyzet alapvetően nem változott, a válaszadók 42 százaléka továbbra sem fordít figyelmet partnerei BCM-keretrendszereire, és további 30 százalékuk is csak informálisan veszi ezt figyelembe. A partnereik BCM-keretrendszereire is ügyelő szervezetek kétharmada a pénzügyi szférából került ki.

A BCM-et támogató szoftver használatát tekintve sem változott gyökeresen a helyzet, továbbra is a válaszadók mintegy 14 százaléka használ a BCM-et teljes körűen támogató szoftvert, melyet 19 százalékuk az üzletihatás-elemzésre támogatására használ, ugyanakkor továbbra sem jelent előnyt a szoftveres támogatás a válaszadók közel 40 százaléka számára. A kép annyiban pozitívabb, hogy 10 százalékkal, 29 százalékra nőtt a szoftver bevezetését tervező szervezetek aránya.

BCM-szoftver használat



Giesz István
Informatikai vezérigazgató-helyettes, GIRO Zrt.

„Az üzleti partnerek kiválasztásánál figyelembe vesszük, hogy rendelkeznek-e rendszeresen auditált és tesztelt BCM-el, ugyanis biztosítva kell lennünk afelől, hogy egy nem várt esemény bekövetkezésekor is képesek lesznek a szerződésben meghatározott szolgáltatást nyújtani.”

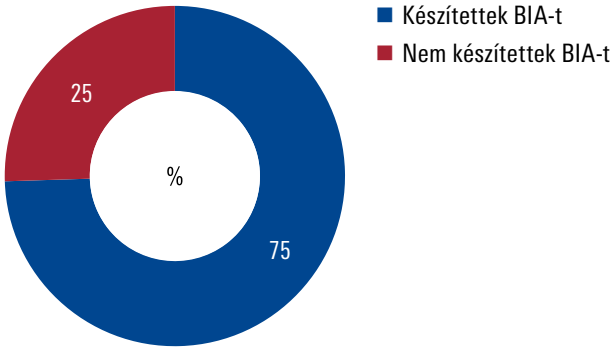
Rendben vannak-e az alapok? – Milyen üzletihatás-elemzéssel rendelkeznek a hazai szervezetek?

A rendelkezésre állás elvesztéséből fakadó kockázatokat megfelelően kezelő és hatásosan működő üzletfolytonossági terveknek szilárd alapokra kell épülniük. Ezt az alapot egy átfogó és részletekbe menő üzletihatás-elemzés tudja megteremteni. Idei felmérésünkben igyekeztünk feltárni, hogy a résztvevő magyarországi szervezetek végeztek-e üzletihatás-elemzést az üzletfolytonossági tervek készítése előtt, illetve milyen megközelítéssel és módszer használatával tették azt.

BIA nélkül mit érek én…

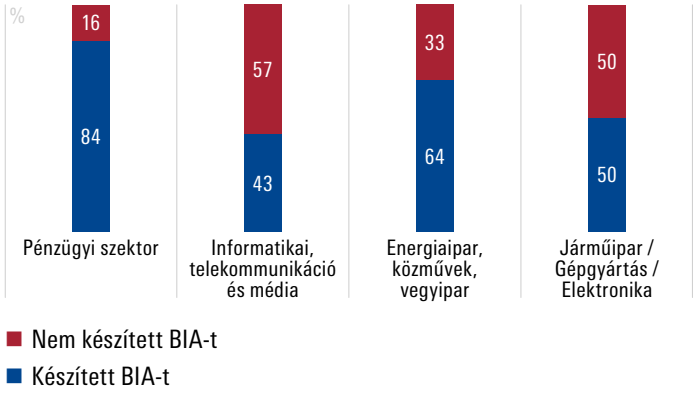
Mint azt korábban is említettük, a résztvevők kis része még egyátalán nem alakította ki üzletfolytonossági keretrendszerét, így nyilván ők üzletihatás-elemzést, BIA-t sem készítettek. Emellett azonban azt tártuk fel, hogy a BCM-mel már rendelkezők 25 százaléka sem készítette el üzletihatás-elemzését.

Mennyien készítettek BIA-t?



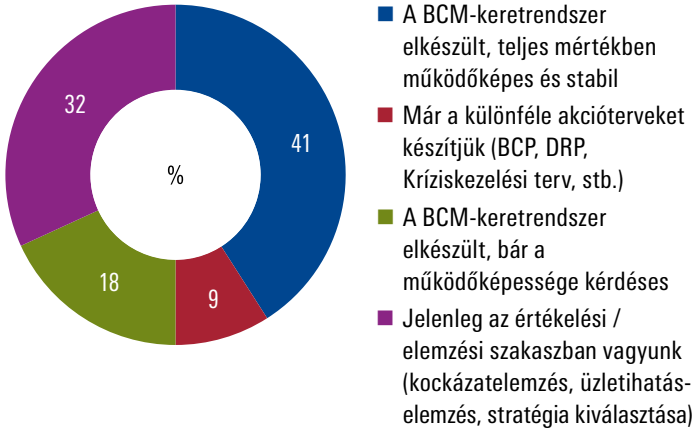
Ha iparáganként vizsgáljuk az üzletihatás-elemzések státuszát, megállapíthatjuk, hogy a pénzügyi szektorban tevékenykedő szervezetek igen magas hányada (84 százalék) dolgozta ki a BIA-t, és az energia/közművek/vegyipar szektor esetében is közel kétharmad az arány.

BIA-készítés szektoriális eloszlása



Az alábbi ábrán összefoglaltuk, hogy azok a résztvevők, akik nem rendelkeznek BIA-val a BCM-készültség mely fokán állnak.

BIA-val nem rendelkezők BCM-státusza

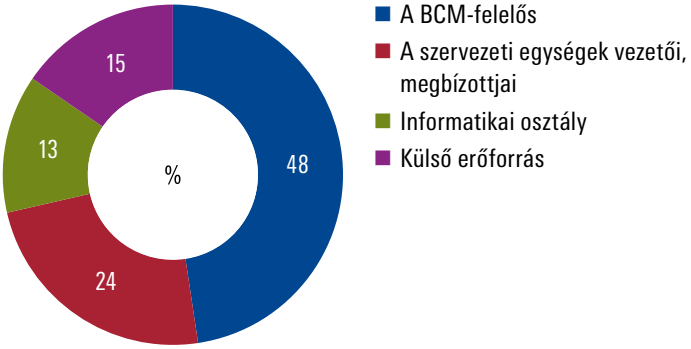


Kézenfekvő, hogy a BCM-keretrendszerrel nem rendelkezők BIA-t sem készítettek, valamint azok sem, akik még a BCM kialakításának az értékelési, elemzési szakaszában vannak. Azonban, ha őket nem számítjuk, még mindig 50 százalék azok aránya, akik BIA nélkül készítik a terveiket, vagy már anélkül dolgozták ki BCM-keretrendszerüket. Ráadásul a BIA-val nem rendelkezők 41 százaléka gondolja úgy, hogy stabil és működőképes BCM-mel rendelkezik. Véleményünk szerint azonban e BCM-ek minősége kérdéses, hiszen ők vajon mi alapján dolgozták ki a üzletmenet-folytonossági (BCP) és katasztrófa-helyreállítási terveiket (DRP), mely folyamatok vagy erőforrások kiesésére készültek fel?

Egy átfogó, alapos és minden részletre kiterjedő üzletihatás-elemzés nélkül nagy a valószínűsége, hogy a kritikus folyamatokat és erőforrásokat, valamint az üzletfolytonossági kockázatokat nem pontosan vagy teljes körűen tárják fel, melynek eredményeként az informatikai infrastruktúra és informatikai rendszerek hibatűrő megoldásai nem nyújtanak elégséges védelmet nem várt események bekövetkezése esetén, és ezáltal nem felelnek meg az üzleti elvárásoknak.

Ki készíti?

Ki készítette a BIA-t?



Felmérésünkből világosan kiderül, hogy amennyiben az adott szervezet készített üzletihatás-elemzést, úgy a résztvevők közel fele azt egy belső BCM-felelősre bízta, aki nagyrészt interjúk, kisebb részben pedig kérdőíves módszer segítségével gyűjtötte össze, majd elemezte az adatokat. Ugyancsak helyesnek ítélhető az a megközelítés, amikor külső erőforrás, tanácsadó segítségével és vezetésével készül el a BIA, mivel ebben az esetben is egy kézben összpontosul a begyűjtött információ, így az egyenszilárdság és az összehasonlíthatóság jobban biztosítható az elemzés során. Megállapítható azonban, hogy az egyes szervezetek ritkán vesznek igénybe külső partnert az üzletihatás-elemzés elvégzésére, bár a tanácsadóknál felgyülemlett tapasztalat nagyban segítheti és gyorsíthatja a folyamatot.

A válaszadók 24 százaléka esetén az egyes szervezeti egységek vezetői készítették a BIA-t, amely bár az elosztott munkavégzésből következően gyorsítja a folyamatot, egyúttal növeli az eredmények inkonzisztenciájának kockázatát. A fennmaradó 13 százalék esetében az informatikai osztály végezte az üzletihatás-elemzést, amely eljárás esetén felmerül a kérdés, hogy az üzleti hatásokat vajon sikerült-e pontosan felmérniük, illetve mennyire elfogulatlanul sikerült meghatározni az informatikai erőforrásokkal szemben támasztott rendelkezésre állási követelményeket.

Az elkészült BIA eredményeit jellemzően a felső vezetés hagyja jóvá, és a megkérdezett szervezetek körülbelül egyforma arányban a részlegvezetőkkel és az informatikai osztállyal is egyeztetik azokat.

Ássunk a mélyére!

Ebben az évben felmérésünk elkészítésénél arra helyeztük a legnagyobb hangsúlyt, hogy részletesen felfedjük, ki milyen megközelítéssel készítette el az üzletihatás-elemzést, milyen céljai és elvárásai voltak, és milyen szempontokat vett figyelembe a kritikus folyamatok és erőforrások azonosítása érdekében.

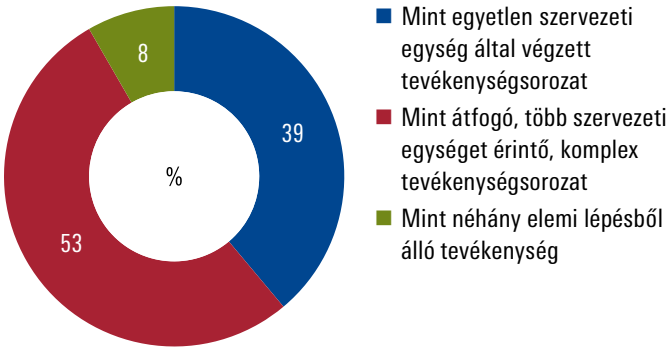
Elsőként megvizsgáltuk, hogy a válaszadók mire alapozták az elemzést.

Mi volt a BIA alapja?

Világosan láthatjuk, hogy a résztvevők túlnyomó többsége (75 százaléka) üzletihatás-elemzését szervezete folyamataira, tevékenységeire alapozza, és folyamatalapú BIA-t készít(ett). Az általános elfogadott megközelítés, valamint a témában iránymutató ISO 22301:2012 szabvány (amely a BS 25999-re alapul) szerint is a szervezet folyamatai, tevékenységei jelentik a BIA alapját, ezek kiesésének hatásait vizsgálja az elemzés. Néhányan a szervezet szolgáltatásaiból/termékeiből indultak ki, és mivel ezek előállítását az egyes üzleti folyamatok biztosítják, valószínűleg ők is jó úton jártak. Hasonlóan azok, akik a szervezeti egységekből indultak ki, bár itt már kétséges, hogy sikerült-e azonosítani a szervezeti egységek egyes tevékenységeit, ugyanis egy adott szervezeti egységen belül is létezhetnek magasabb prioritású és kevésbé kritikus tevékenységek, amelyek megkülönböztetése a BIA alapvető célja kell, hogy legyen. Néhány válaszadó a szervezet erőforrásaira alapozta a BIA-t, amely szintén megfelelő megoldás lehet, ha sikerül az erőforrás helyreállítási kritériumainak pontos meghatározása, és később a tervezés során az erőforrás kiesése esetén alkalmazandó helyettesítési folyamat részletes, optimálisan folyamatonkénti kialakítása.

Ugyan a válaszadók nagy része folyamatalapú BIA-t készített, tapasztalataink szerint jelentős eltérés mutatkozik abban, hogy ki mit ért üzleti folyamat alatt, ezért ezt is igyekeztünk felderíteni.

Mit értettek üzleti folyamat alatt a résztvevők?



„A folyamatok maximálisan megengedett kiesési idejének meghatározásánál figyelembe vettük a kritikus időszakokat is, hiszen ilyenkor a tolerálható kiesési idő kevesebb, mint a normál időszakban.”

Nagy Erika – business continuity manager, biztonsági szenior menedzser, Magyar Telekom Nyrt.

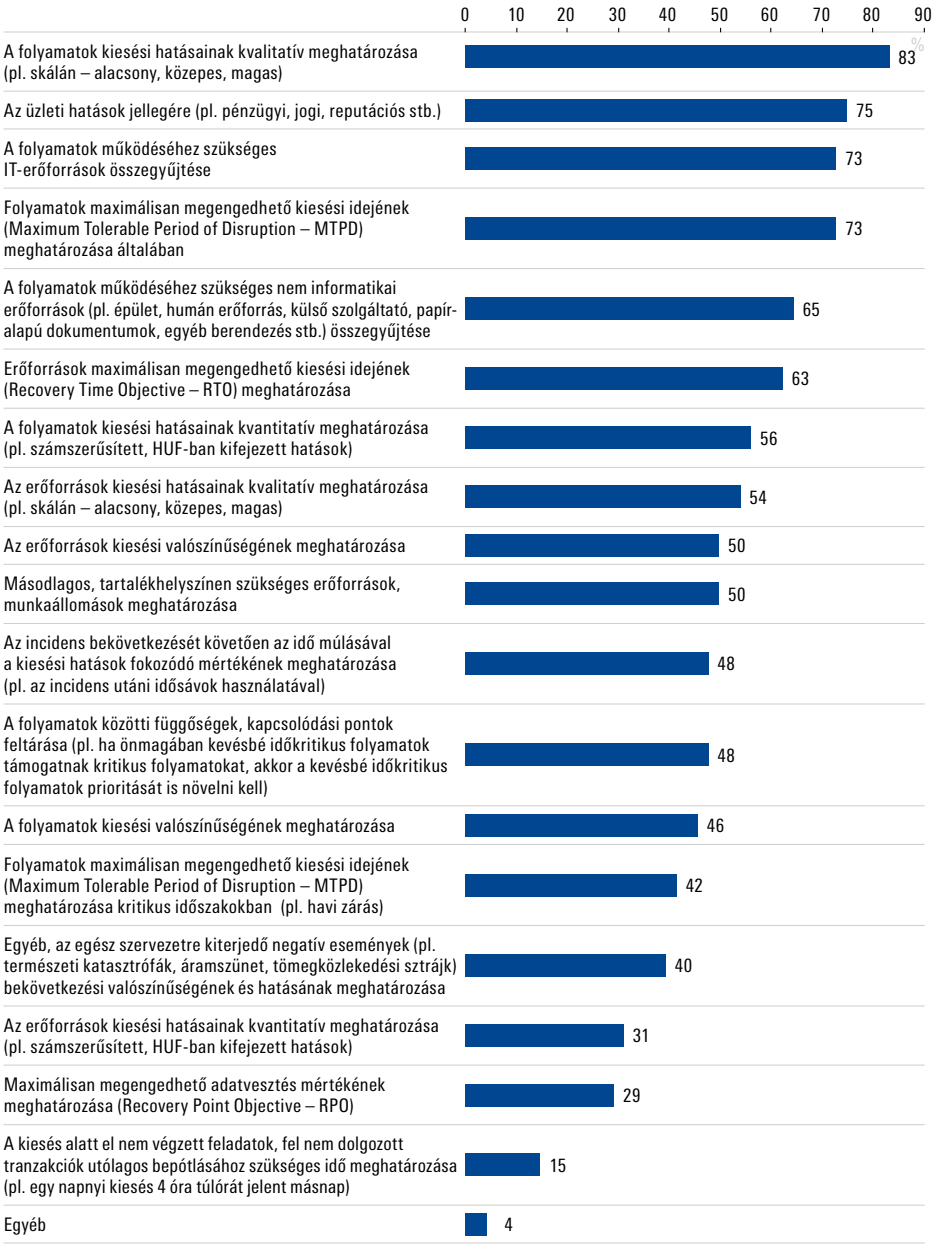
Azok a résztvevők, akik folyamatalapú BIA-t készítettek, többségükben (53 százalék) a folyamatot úgy értelmezik, mint egy átfogó, több szervezeti egységet is érintő, komplex tevékenységsorozatot. Erre jó példa lehet a pénzügyi szférából a hitelezés, amely magában foglalja a hitelkérelmek befogadásától és feldolgozásától kezdve, a hitelbíráláton keresztül a folyósításig és akár a követeléskezelésig tartó komplex, számos szervezeti egységen átívelő folyamatot; vagy a beszerzés, amely az igény felmerülésétől, a szállítók tendereztetésén és kiválasztásán keresztül, a bevételezésig és pénzügyi teljesítésig számos alfolyamatot felölel. E megközelítés ugyan összefüggéseiben vizsgálja a szervezet értékteremtő folyamatait, azonban az egyes alfolyamatok kritikussága általában eltérő, és ezeket a különbözőségeket ez a szemlélet elmoshatja, így a BIA kevésbé pontos.

Szintén jelentős számú válaszadó (39 százalék) úgy értelmezi a folyamatot, mint egy adott szervezeti egység által végzett tevékenységsorozatot. Ez a megközelítés egyrészt a felmérést is segíti és egyszerűsíti, további előnye, hogy jobban elkülöníthetőek a folyamatok, és ezáltal precízebben meghatározható az egyes folyamatok kritikussága, a folyamatok közötti függőségek és kapcsolódások pedig a vizsgálat során feltárhatók.

A résztvevők csupán kis hányada értelmezi a folyamatot néhány elemi lépésből álló tevékenységként. A tapasztalatok szerint az ilyen szintű részletesség esetén a befektetett munka hozadéka már kérdéses, és a folyamatok közötti összefüggések feltárása is igen bonyolult kapcsolati hálót eredményez.

Egyik legfontosabb kérdésünk a BIA-módszertana kapcsán arra vonatkozott, hogy a BIA milyen aspektusokra terjed ki – itt a résztvevők a 19 válaszlehetőségből többet is megjelölhettek attól függően, hogy az ő szervezetüknél az üzletihatás-elemzés mennyire alkalmaz komplex megközelítést.

BIA készítés során figyelembe vett tényezők



„A BIA elkészítésekor társaságunk üzleti folyamatait vettük alapul, mivel az volt a célunk, hogy pontosan azonosítsuk egyes események bekövetkezése milyen nemkívánatos hatást gyakorol értékteremtő folyamatainkra.”

Ferenczné Földvári Katalin – Kockázati tanácsadó, BC manager K&H Bank Zrt.

Az eredményekből a következő főbb tanulságokat vonhatjuk le:

- A válaszadók legnagyobb többsége (83 százalék) a folyamatok kiesési hatására fókuszált a BIA során. Tette ezt alapvetően kvalitatív megközelítéssel, míg a hatások számszerűsített meghatározására a résztvevők nagyjából fele (56 százalék) fordított figyelmet. Azonban az incidens bekövetkezését követően az idő múlásával a kiesési hatások fokozódó mértékének meghatározását csak a résztvevők közel fele (48 százalék) tartotta fontosnak.
- A válaszadók pontosan háromnegyede (75 százalék) határozta meg az üzleti hatások jellegét is (például pénzügyi, jogi vagy hírnév-jellegű hatás).
- A folyamatok közötti függőségek feltárására csak a válaszadók közel fele (48 százalék) fordított figyelmet.
- A folyamatokhoz szükséges erőforrásokat is jellemzően összegyűjtötték a válaszadók, bár itt elsősorban az informatikai erőforrásokra koncentráltak (73 százalék), és némileg kisebb mértékben az egyéb erőforrásokra (65 százalék).
- A folyamatok maximálisan megengedett kiesési idejét (Maximum Tolerable Period of Disruption - MTPD) is meghatározta a válaszadók többsége (73 százalék), bár arra, hogy az MTPD értékét kritikus időszakok tekintetében külön is meghatározza, csak a válaszadók 42 százaléka ügyelt.
- Az MTPD-ből következő, az erőforrásokhoz tartozó helyreállítási idő célkitűzést (Recovery Time Objective - RTO) már kevesebben, csak a válaszadók 63 százaléka határozta meg, pedig ez kulcsfontosságú alkotóeleme a megfelelő BCM-stratégia és -tervek megalkotásának.
- A maximálisan megengedhető adatvesztés mértékét (Recovery Point Objective - RPO) már csak a válaszadók 29 százaléka határozta meg, míg a kiesés alatt el nem végzett feladatok, fel nem dolgozott tranzakciók utólagos bepótlásához szükséges időt csupán a válaszadók 15 százaléka veszi figyelembe.
- Úgy tűnik, sokan csak a kisebb kiterjedésű folytonossági eseményekre készülnek fel, ugyanis az egész szervezetre kiterjedő negatív események (például természeti katasztrófák, áramszünet, tömegközlekedési sztrájk) bekövetkezési valószínűségét és hatását pusztán a válaszadók 40 százaléka határozta meg. Az ilyen események kezelésére nélkülözhetetlen másodlagos, tartalékhelyszínen szükséges erőforrásigények meghatározását is csak a válaszadók fele érezte fontosnak.
- A BIA eredményei nyomán meghatározhatóak az egyes folyamatok és erőforrások folytonossági és rendelkezésre állási idő kritériumai, mégis a BIA eredményei csak a válaszadók 10 százalékánál vannak összhangban a szolgáltatásiszint-megállapodásokkal (SLA). Vajon a többiek esetében csak az összhang, vagy az SLA-k is hiányoznak?
- Az eredményeket szektoronként elemezve látható, hogy a pénzügyi szektor élen jár az elemzés komplexitását illetően, ezt követik a logisztika/közlekedés/szállítás, és az informatikai, telekommunikáció és média iparágakban tevékenykedő szervezetek, míg legkevésbé a közszféra végez összetett BIA-elemzéseket.

Összefoglalóan elmondható, hogy ugyan a résztvevők által elvégzett üzletihatás-elemzések kiterjednek a legalapvetőbb aspektusokra (mint például a folyamatok kiesési hatásainak és támogató erőforrások körének, valamint a maximálisan megengedett kiesési idők meghatározására), de csak kevesen foglalkoznak az olyan - szintén kritikus - elemzésekkel, mint a folyamatok közötti kapcsolódások feltárása, az egész szervezetre kiterjedő negatív események elemzése, vagy az RPO-k meghatározása. Pedig egy részletes és minden aspektusra kiterjedő elemzés hiányában nem lehetséges a pontos hatáselemzés elkészítése, melynek következtében előfordulhat, hogy a társaságok nem a megfelelő folyamatok és erőforrások kiesésének kezelésére fókuszálják amúgy is szűkös pénzügyi és emberi erőforrásaikat.

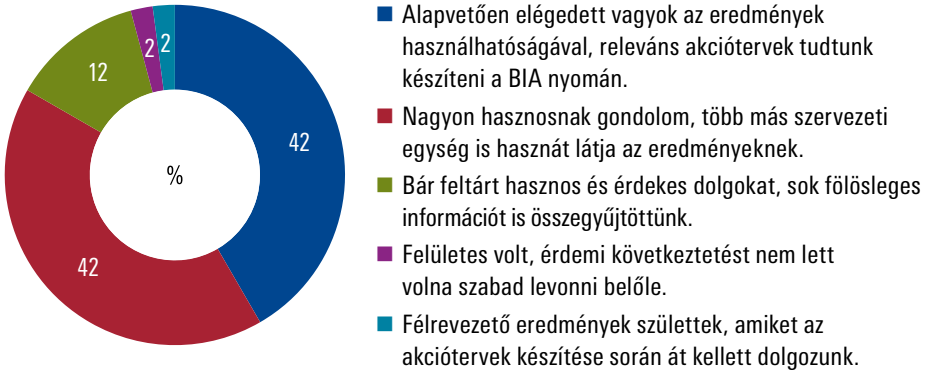
„Egyes átfogó BCM- események (például tömegközlekedési sztrájk, természeti katasztrófák) jellemzően a szervezet egészére kihatnak, így a BCM keretein belül ezeknek a komplex problémáknak a kezelésével is foglalkoztunk. A kockázatok alapján úgy ítéltük meg, hogy az ilyen események kezelése gyakran csak tartalékhelyszínek biztosításával oldható meg."

Nagy Sándor – IT biztonsági vezető, Banco Popolare Hungary Zrt.

Szeretjük? És gondozzuk is?

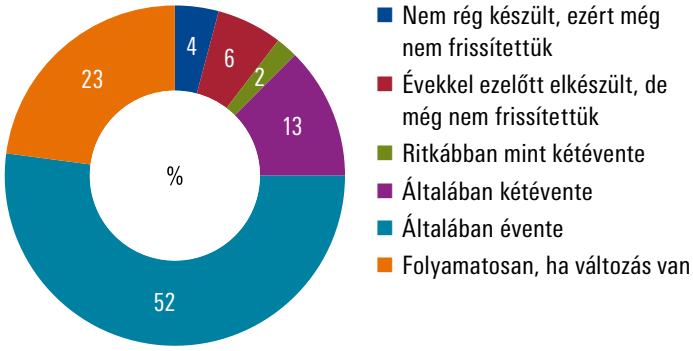
Mint az korábbi elemzésünkből kiderült, a felmérésben résztvevők fele készített üzletihatás-elemzést. Túlnyomó többségük elégedett volt a BIA eredményeivel, és hasznosnak találta azt. Úgy vélték, a BIA megfelelő alapot jelentett az üzletfolytonossági tervek kidolgozásához. A válaszadók 12 százaléka már kevésbé volt elégedett, szerintük sok felesleges információt is összegyűjtöttek.
Ez esetben a BCM-keretrendszer integritása kérdéses, vagy csupán még nem eléggé kiforrott, hiszen nem célszerű olyan adatokat begyűjteni, amelyet aztán nem használunk fel.

Elégedettség a BIA eredményeivel



A BCM naprakészségének biztosítása kulcsfontosságú, így értelemszerűen ennek kiindulási alapját, a BIA-t is rendszeresen frissíteni kell. Az üzletihatás-elemzés aktualizálására vonatkozó kérdésünkre a válaszadók fele az évenkénti frissítési gyakoriságot jelölte meg, míg 13 százalékuk szintén rendszeresen, de csak kétévente frissíti a BIA-t. A válaszadók 23 százaléka a változásokhoz köti a BIA aktualizálását, és azokkal párhuzamosan végzi el a frissítést. Biztató, hogy csak a résztvevők kis része (mintegy 8 százalék) nem tartja karban üzletihatás-elemzését, vagy teszi ezt két évnél ritkábban.

A BIA frissítési gyakorisága



Csincsák Tünde
Risk & Business Continuity Manager, Vodafone Magyarország Zrt.

„Az üzletihatás-elemzésünket évente minimum egyszer, de jelentősebb változások esetén is felülvizsgáljuk, és szükség esetén aktualizáljuk."

A KPMG-ről

A KPMG Magyarország vezető szakmai szolgáltató társasága (a BBJ kiadványa, a Listák könyve szerint). A 152 országban 145 000 szakembert foglalkoztató KPMG-hálózat magyarországi tagvállalatainál 600 munkatárs dolgozik – a KPMG Hungária Kft. könyvvizsgálati, míg a KPMG Tanácsadó Kft. széles körű adó- és üzleti tanácsadási szolgáltatásokat kínál magyar és multinacionális társaságok, kormányzati szervek és külföldi befektetők számára.

Globális stratégiánk jelmondata, a „Cutting Through Complexity" összegzi küldetésünket: célunk, hogy az egyre összetettebb üzleti, gazdasági környezetben tiszta, érthető válaszokkal és megoldásokkal támogassuk ügyfeleinket.

Iparág-specifikus szolgáltatásokat kínálunk a pénzügyi szolgáltatások, a telekommunikáció, az energia- és közműszolgáltatások, a kormányzat, az infrastruktúra, az ingatlanpiac és a turizmus terén. Tanácsadóink nemzetközi kompetenciával rendelkeznek az energia- és közüzemi szektorban, a turizmus- és sportfejlesztés, valamint a regionális és osztott szolgáltató központok fejlesztése és üzemeltetése terén. Budapesten működik a KPMG adóügyviteli központja is.

Informatikai kockázatkezelési szolgáltatásokkal foglalkozó tanácsadóink az informatikai környezet és rendszerek biztonságossá tételében, a hatásos kontrollok és a jogszabályi megfelelőség megteremtésében nyújtanak támogatást. Segítünk ügyfeleinknek, hogy azonosítsák és értékeljék információbiztonsági kockázataikat, amelyek jelentős hatással lehetnek a biztonságos és folyamatos működésre, ezáltal a társaság bevételtermelő képességére. Szakértőink támogatják olyan információbiztonsági kontrollok kialakítását és bevezetését, amelyek megfelelnek a jogszabályoknak és a nemzetközi szabványoknak egyaránt.

A kiadvány készítésében közreműködtek:

Bagdi Ágnes

Horváth Andrea

Molnár István

Kapcsolat

Gaidosch Tamás
partner
T: +36 1 887 7139
E: tamas.gaidosch@kpmg.hu

Molnár István
szenior menedzser
T: +36 1 887 7445
E: istvan.molnar@kpmg.hu

kpmg.hu