ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel

Információbiztonsági stratégia és vezetés

Oroszi Eszter Diána

Nemzeti Közszolgálati Egyetem

Budapest, 2014

Tartalomjegyzék

Bevezetés

Napjainkban minden vállalat egyik legnagyobb üzleti értéke az információ – üzleti titkok, ügyféladatok, üzleti tervek, fejlesztésekkel és projektekkel kapcsolatos belső információk. A legtöbb szervezetnél az információ, és az arra épülő tudásbázis az egyik legfontosabb vagyonelemnek tekinthető, mely nélkül az üzleti tevékenységük végzése csak nehezen biztosítható, vagy teljes mértékben tudás alapon működő vállalatok esetében (például tanácsadó tevékenység folytatása során) akár teljesen el is lehetetlenül. Mindebből kifolyólag mind a saját, belső információk, mind az ügyfél adatok bizalmasságának, sértetlenségének és/vagy rendelkezésre állásának sérülése jelentős anyagi, reputációs, működési és egyéb a szervezet-specifikus károkkal járhat, valamint törvényi kötelezettségnek való nem-megfelelőséget és ezzel járó bírságot, szankciókat is vonhat maga után. A leírtak alapján elmondható, hogy a szervezetek szempontjából az információbiztonságot egyre kritikusabb tényezőként kell tekinteni, és be kell építeni mind az üzleti, mind a működési és egyéb funkcionális stratégiákba. Az információbiztonsági követelményeknek, intézkedéseknek támogatniuk kell az üzleti folyamatokat, annak érdekében, hogy az üzleti stratégiában megfogalmazott célok megvalósuljanak a biztonsági szempontból is megfelelő működés megteremtése és az adatvagyon védelmének biztosítása által.

Annak érdekében, hogy a vállalati adatvagyon elemhez ne történjen jogosulatlan hozzáférés, vagyis az információ bizalmassága, sértetlensége és rendelkezésre állása biztosított legyen, gondoskodni kell azok megfelelő szintű védelméről. A tapasztalatok alapján elmondható azonban, hogy sok esetben a vállalatok által bevezetett védelmi intézkedések elsősorban inkább csak az informatikai rendszerekre, ügyviteli alkalmazásokra fókuszáltan kerülnek bevezetésre, nem pedig magára az információra. Ez a megközelítés azonban nem támogatja az információbiztonság teljes körű megvalósítását, a védelmi intézkedéseknek, kialakított kontrolloknak ki kell terjedniük az adatok kezelésére, feldolgozására, átadására és tárolására is, mely magában foglalja többek között a fizikai biztonságot, humán erőforrás biztonságát, hozzáférés menedzsmentet, jogosultságkezelést, az üzletfolytonos működés biztosítását, és egyéb, a későbbiekben részletezett kapcsolódó területeket.

Hasonlóan gyakori tapasztalat, hogy a bevezetett védelmi intézkedések és kontrollok egymástól függetlenül, elszigetelten kerülnek bevezetésre, mely azonban nem támogatja a működés hatékonyságát. Ennek elkerülése és a hatékony működtetés megvalósítása érdekében fontos mind a technológiai, mind az adminisztratív információbiztonsági intézkedések

összehangolása, egymással összefüggő, komplex rendszerben történő tervezése, kialakítása, működtetése. Mindezek megvalósítása érdekében célszerű, ha a szervezet egy összetett információbiztonsági irányítási rendszer bevezetésével támogatja a védelmi intézkedések és kontrollok kialakítását és hatékony alkalmazását. Az információbiztonsági irányítási rendszer alappillére az információbiztonsági politika, illetve egy megfelelő információbiztonsági stratégia kidolgozása, valamint az annak megvalósítását támogató és végrehajtó szervezet felállítása, a megfelelő irányítás, vezetés biztosítása, valamint a rendszer hatékony működésének folyamatos monitorozása, visszamérése.

Az információbiztonsági irányítási rendszer

Az információbiztonsági politika az információbiztonsági irányítási rendszer egyik alappillére, magas szintű dokumentuma, a felső vezetés információbiztonság iránti elkötelezettségét nyilvánítja ki. Felülvizsgálatára, esetleges módosítására 5-10 évente kerül sor. Az információbiztonsági irányítási rendszer elemeinek megvalósításának tervezését, az információbiztonsági célokat az információbiztonsági stratégia dokumentuma tartalmazza.

Jelen dokumentum célja annak bemutatása, hogy hogyan kell kialakítani, és mit kell tartalmaznia az információbiztonsági stratégiának, milyen támogató eszközök, irányítási, vezetési lehetőségek állnak rendelkezésre annak menedzselésére, és milyen visszamérési, ellenőrzési módszerek beépítése szükséges azok működési teljesítményének méréséhez, hatékonyságának fokozásához.

A dokumentum felépítését tekintve a következő fő témakörökre épül:

- Az információbiztonsági irányítási rendszer célja
- Az információbiztonsági stratégia kialakítása
- Az információbiztonsági irányítási rendszer irányítása, a stratégia megvalósítása
- Az információbiztonsági irányítási rendszer működésének ellenőrzése, visszamérése

Információbiztonsági irányítási rendszer

1. Az információbiztonsági irányítási rendszer célja

Az üzleti célokat az üzleti stratégia, és a hozzá kapcsolódó területi, funkcionális stratégiák határozzák meg. Ezek egyike az információbiztonsági stratégia, mely az információbiztonsági irányítási rendszer kialakítását, valamint hatékony és eredményes működtetését tűzi ki célul, valamint támogatja a megvalósítás során. Mielőtt azonban az információbiztonsági stratégia kidolgozásának lehetőségeit vizsgálnánk, tekintsük át az információbiztonsági rendszer működtetésének indokoltságát és jelentőségét.

Az üzleti célok általában a következő főbb követelményeket határozzák meg, és bontják le az egyes funkcionális stratégiákban:

Megfelelő minőségű termékfejlesztés és szolgáltatásnyújtás

Új tevékenységi területek feltérképezése, kidolgozása

Folyamatos szolgáltatásnyújtás, megbízhatóság biztosítása

Folyamatos fejlesztés, innováció

Ügyféligények kielégítése

Ügyfél-elégedettség növelése

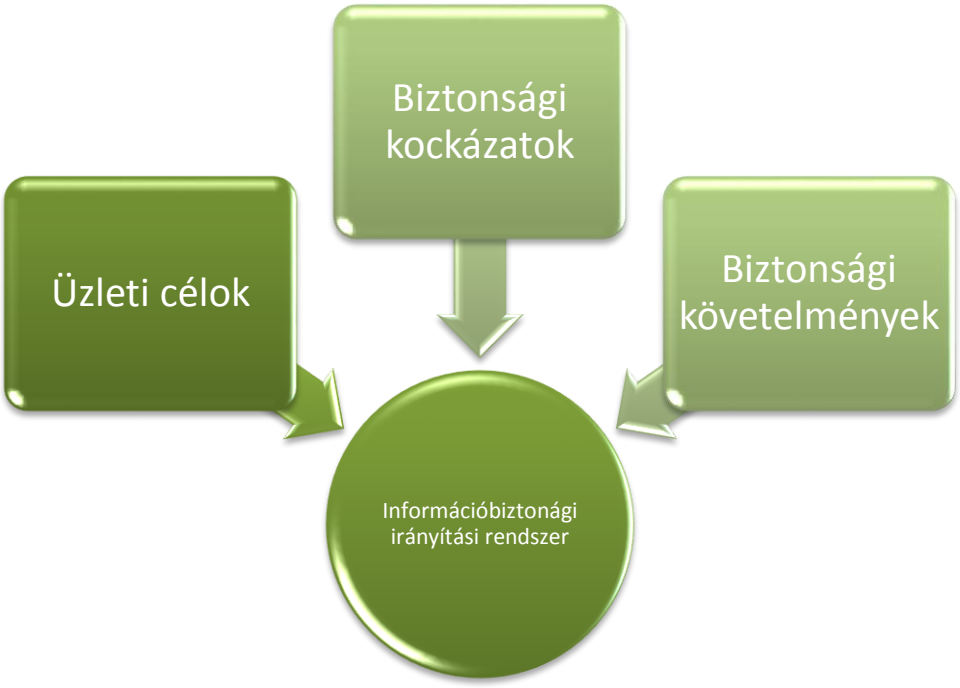
Új ügyfelek felkutatása, szerzése

Törvényi kötelezettségeknek való elégtétel

Mindezek mellett egyre hangsúlyosabb szerepet kap az ezek biztosítását támogató, információbiztonsági szempontból is megfelelő működés támogatása. A szervezetek legtöbbje már felismerte az információbiztonság jelentőségét, és bevezetett információbiztonsági védelmi intézkedéseket, azonban ezek nem minden esetben működnek egy egységes rendszerben, elszigetelt menedzsmentjük pedig gyakran nem járul hozzá az eredményes és hatékony működtetésükhöz. A védelmi intézkedések és kontrollok komplex átlátása,

egymással összhangban történő kialakítása és fenntartása információbiztonsági irányítási rendszer bevezetésével és működtetésével valósítható meg leghatékonyabban.

Az információbiztonsági irányítási rendszer bevezetésének célja a szervezet által használt kritikus információk és információs rendszerek azonosítása, azok információbiztonsági kockázatainak felmérése, ezek alapján biztonsági követelmények meghatározása és kockázatarányos védelmi intézkedések bevezetése és folyamatok kialakítása, valamint azok összhangjának megteremtése és eredményes, hatékony működésének irányítása. Ezen célok eléréséhez a rendszer tervezésekor információt kell gyűjteni az üzleti célokról, a szervezetet érintő biztonsági kockázatokról, valamint az ezek alapján meghatározott biztonsági követelményekről, biztonsági igény-szintről.



Az információbiztonsági rendszer kialakításához szükséges információk

Ezen kívül az információbiztonsági irányítási rendszer kialakításának előnyei a szervezet számára:

- üzleti célok elérésének, teljesítésének támogatása,
- törvényi kötelezettségeknek való elégtétel biztosítása,
- külső (például csoportszintű) követelményeknek való megfelelés biztosítása,
- szervezeti, funkcionális és információbiztonsági célok összehangolása,
- üzleti funkciók, tevékenységek támogatása,
- információbiztonsági követelmények meghatározása és megvalósításának támogatása,

- kritikus információk és támogató információs rendszerek azonosítása,
- az azonosított információk és rendszerek bizalmasságát, sértetlenségét, illetve rendelkezésre állását befolyásoló tényezők, kockázatok azonosítása és elemzése,
- a kockázatkezelési lehetőségek azonosítása,
- a kockázatelemzés eredménye alapján kockázatarányos és költséghatékony védelem kialakítása és folyamatos fenntartása,
- védelmi intézkedések és kontrollok komplex rendszerben történő kezelése, összehangolása, működési hatékonyságuk növelése és kontrollja,
- erőforrások kihasználtságának monitorozása, optimalizálása,
- biztonsági incidensek, rendkívüli események kezelésének támogatása, azonnali reakció biztosítása,
- információbiztonsági szemlélet fokozása, biztonságtudatossági szint növelése a szervezeten belül,
- folyamatos visszamérés, fejlesztés biztosítása,
- pozitív megítélés, üzleti előny szerzése, ügyfél-elégedettség növelése,
- külső (például ISO/IEC 27001:2013 szabvány szerinti) tanúsítvány megszerzésének lehetősége, mely nagymértékben hozzájárul az ügyfelek bizalmának növeléséhez és üzleti előny szerzéséhez is.

Mindezek alapján az információbiztonsági irányítási rendszer 6 fő célját különböztethetjük meg (CISM Review Manual, 2014):

- *Információbiztonsági és az üzleti célok összehangolása*: Az információbiztonság jelentőségének felismerésével és rendszer szintű támogatásával a biztonsági követelmények beépülnek az üzleti tevékenységekbe, a biztonsági intézkedések üzleti folyamatokhoz kerülnek igazításra, megteremtésre kerül az egyes funkcionális stratégiák közötti összhang. Ennek hatására az információbiztonsági kontrollok nem a „szükséges rossz” intézkedések, korlátozó tényezők kategóriáját képviselik, hanem úgy kerülnek azonosításra, mint az üzleti célok elérésének támogató eszközei, lehetőségei.
- *Kockázatmenedzsment*: Annak érdekében, hogy az információbiztonsági kockázatok megfelelően kerüljenek kezelésre, illetve csökkentésre, első lépésként célszerű, ha a szervezet tisztában van a rá vonatkozó, releváns kockázatokkal. A kockázatok felmérését és értékelését követően ki tudja alakítani a kockázatkezelési stratégiát, és annak megfelelően tud dönteni az azonosított kockázatok kezeléséről. Ehhez

elengedhetetlen, hogy azonosításra kerüljenek a szervezetre vonatkozó potenciális fenyegetések, és azok a sérülékenységek, melyek az azonosított fenyegetések által kihasználhatóak. A kockázatok felmérésével meghatározható a szervezet kockázati profilja, azonosíthatóak a kitettségek és azok bekövetkezésének hatásai, valamint az ezek alapján bevezetésre kerülő védelmi intézkedések és kontrollok megvalósításával elfogadható mértékre csökkenthetőek a maradvány kockázatok (a felső vezetés által elfogadott, a kockázatcsökkentő védelmi intézkedések bevezetése után fennmaradó, a továbbiakban nem, vagy nem költséghatékonyan csökkenthető, ezáltal felvállaltnak tekintendő minimális kockázatok).

- *Értékteremtés*: A rendszer kialakításával az információbiztonsági intézkedések az üzleti célok megvalósítását támogatják, hozzájárulnak az egész szervezetet lefedő, folyamatos fejlődési lehetőségek megteremtéséhez.
- *Erőforrás optimalizálás*: A rendszer szintű szemlélet támogatja a szükséges erőforrások beszerzését, allokálását, megfelelő és hatékony használatát, a szervezeti tudásbázis folyamatos bővítését és rendelkezésre állását, valamint az információbiztonsági folyamatok, eljárások dokumentálását.
- *Teljesítmén mérés*: Az információbiztonsági rendszer elemeinek folyamatos monitorozása, valamint a visszamérés és értékelés lehetőségének megteremtése támogatja a kitűzött célok elérését, valamint az eltérések azonosítását és javítását, fejlesztését, ezáltal a hatékonyság növelését.
- *Integráció*: Az információbiztonsági folyamatok a működési folyamatokba integrálhatóan kerülnek kialakításra, mely hozzájárul mind az egyes szakterületi funkciók, működési folyamatok, mind az információbiztonsági intézkedések eredményes és hatékony működéséhez.

2. Az információbiztonsági rendszer kialakítása

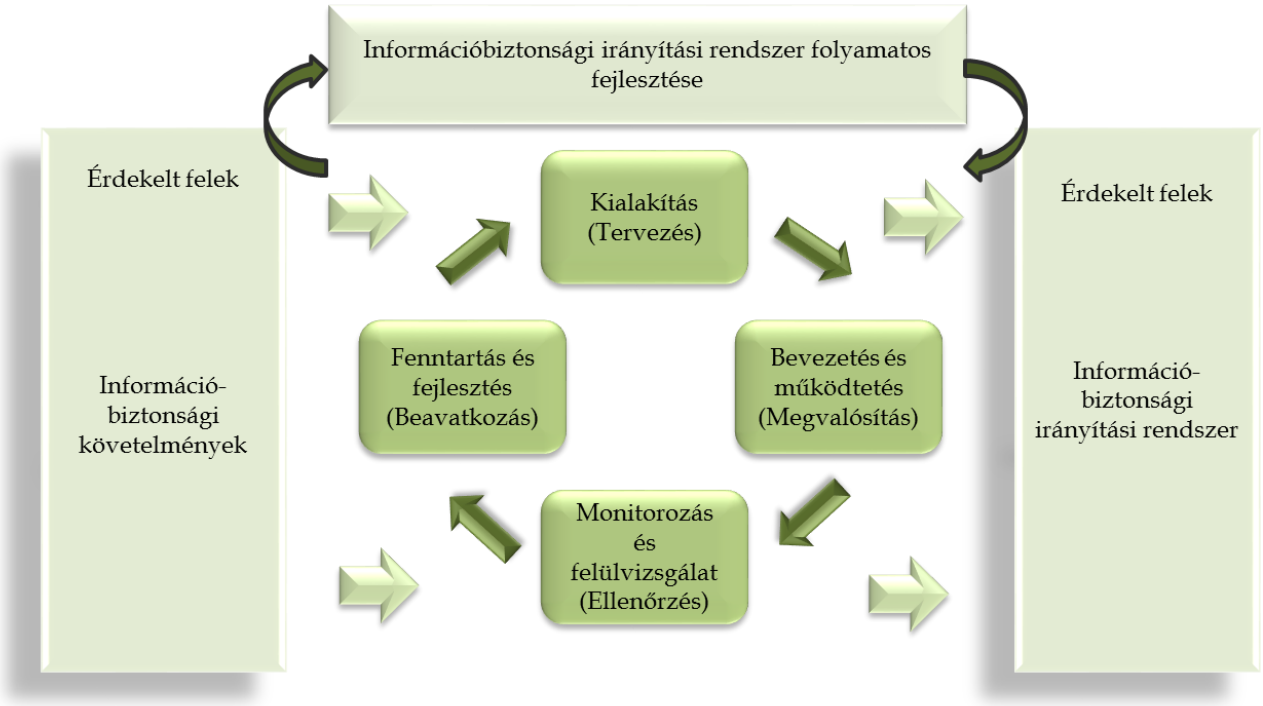
Bármilyen rendszer tervezéséről legyen szó, többféle tervezési modell, támogató eszköz közül választhatunk, ezek közül a legismertebbek:

- Gap analízis
- Balanced Scorecard
- PDCA modell
- SWOT analízis
- Játékelmélet

- Storyboard
- Szcenário tervezés

Az alkalmazandó modellt, keretrendszert minden esetben a szervezet igényeinek, sajátosságainak, képességeinek megfelelően kell kiválasztani – tevékenységtől, kultúrától, infrastruktúrától, valamint természetesen a megvalósítandó céloktól függően eltérő modellek alkalmazása lehet indokolt.

Mivel a keretrendszer a stratégia és a rendszer kialakításának alapja, ezért nagyon fontos a megfelelő kiválasztása. Az információbiztonsági irányítási rendszer stratégiai tervezésének, kialakításának és működtetésének megvalósítása a ISO/IEC 27001:2013 szabványban is bemutatott PDCA (Plan-Do-Check-Act) modellnek megfelelően célszerű, és jelen dokumentumban is ez kerül bemutatásra.



A PDCA modell

A PDCA modell egyes fázisai a következőek (ISO/IEC 27001:2013):

- *Kialakítás (Tervezés)*: A szervezet céljaihoz és üzleti stratégiájához alkalmazkodó információbiztonsági stratégia és információbiztonsági politika kialakítása, definiálása, stratégiai lépések meghatározása, ütemezése és erőforrások allokálása a megvalósításhoz.
- *Bevezetés és működtetés (Megvalósítás)*: A stratégiában meghatározott célok eléréséhez szükséges folyamatok, védelmi intézkedések, kontrollok megvalósítása és működtetése.

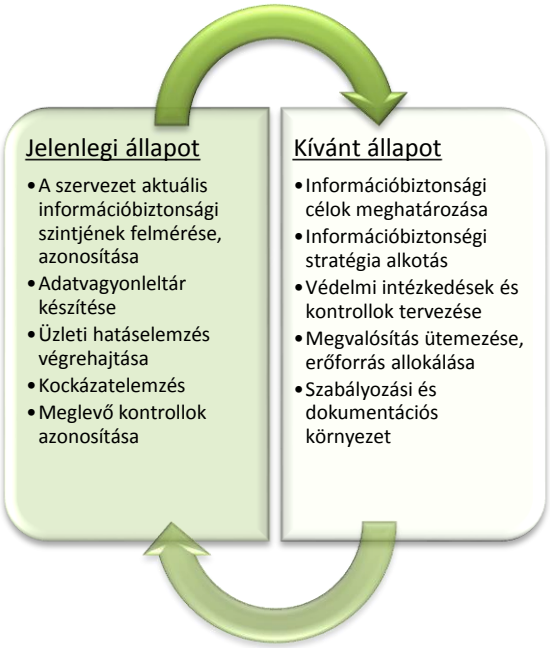
- *Monitorozás és vizsgálat (Ellenőrzés)*: A rendszer rendszeres, előre meghatározott időközönkénti felülvizsgálata és karbantartása, mely magában foglalja a kialakított folyamatok, védelmi intézkedések és kontrollok, valamint az azokat támogató erőforrások megfelelő működtetésének, kihasználtságának folyamatos monitorozását, mérőszámok definiálását a ráfordítások visszaméréséhez és a teljesítmény értékeléséhez.
- *Fenntartás és fejlesztés (Beavatkozás)*: A felülvizsgálatok, illetve a monitorozás és visszamérés során tapasztalt eltérések, nem-megfelelőségek vagy fejlesztési javaslatok alapján a rendszer folyamatos fejlesztése helyesbítő, javító vagy megelőző intézkedések végrehajtásával.

(Megjegyzés: Amennyiben az információbiztonsági irányítási rendszer az ISO/IEC 27001:2013 szabvány szerint kerül kialakításra és tanúsításra, abban az esetben az a már esetlegesen bevezetett ISO 9001 minőségirányítási rendszerbe integrálható és együttesen működtethető, tanúsítható, valamint auditálható. Az így kialakított keretrendszer lehetővé teszi, hogy az ISO/IEC 27001:2013 követelmények is implementálhatóak legyenek a már kialakított és működő dokumentációs rendszerben, ezzel biztosítva a redundancia elkerülését, minimalizálását.)

Az információbiztonsági irányítási rendszer kialakítása, működtetése és rendszeres felülvizsgálata a szervezet felső vezetésének felelőssége. A szervezet az információbiztonság irányítására információbiztonsági felelőst (Chief Information Security Officer - CISO) nevez ki, illetve kijelöli az információbiztonsági irányítási szervezet tagjait, akinek feladatai és felelősségei a munkaköri leírásában rögzítésre kerülnek. Az információbiztonsági irányítási rendszer szervezetének felépítését, a kapcsolódó feladatokat, hatásköröket és felelősségeket Az információbiztonsági irányítás szervezeti felépítése alfejezet mutatja be.

Az információbiztonsági irányítási rendszer kialakításának célja, hogy a jelenlegi állapot, információbiztonsági érettség felmérése, azonosítása után meghatározza az információbiztonsági érettség elérni kívánt szintjét (kívánt állapot), és ehhez definiálja a stratégiai célokat, erőforrásokat, feladatokat, felelősségeket, valamint támogassa ezek megvalósítását, folyamatos rendelkezésre állását. Ez a rendszer egyik alap dokumentumában, az információbiztonsági stratégiában kerül rögzítésre. Tekintve, hogy a biztonság nem egy termék, hanem egy folyamat, az információbiztonsági irányítási rendszer kialakítása és működtetése sem egy egyszeri projekt, hanem folyamatos működtetést, rendszeres felülvizsgálatot, karbantartást igényel, melynek során a változások követése, a rendszer folyamatos fejlesztése biztosított. Ennek érdekében szükséges az információbiztonsági

stratégiában foglalt célok megvalósításának nyomon követése, folyamatos monitorozása, valamint az információbiztonsági irányítási rendszer jelenlegi állapotának, illetve az aktuális stratégiának a rendszeres időközönkénti felülvizsgálata, szükség esetén módosítása.



Az információbiztonsági rendszer megvalósítása és fejlesztése

Az információbiztonsági irányítási rendszer bevezetésének főbb lépéseit az alábbi ábra szemlélteti, az egyes lépések megvalósítása és szerepét az információbiztonsági stratégia tartalmazza, mely *Az információbiztonsági stratégia kialakítása* fejezetben kerül bemutatásra.

Az információbiztonsági irányítási rendszer kialakításának lépései

3. Az információbiztonsági irányítási rendszer elemei

Az információbiztonsági irányítási rendszer tervezésének kereteit a célok, felelősök, folyamatok, erőforrások, valamint az ütemezés alkotják. Ezek alapján az információbiztonsági irányítási rendszer az alábbi elemekre bontható:

- *Információbiztonsági politika*, mely tartalmazza a felső vezetés információbiztonság iránti elköteleződését, támogatását.
- *Információbiztonsági stratégia*, mely megteremti az üzleti és más funkcionális célokkal való összehangolást, az információbiztonsági célok megvalósításához szükséges erőforrások biztosítását, allokálását.
- *Információbiztonsági irányítási folyamatok*, melyek támogatják a stratégiában foglaltak megvalósítását az azokat támogató erőforrások alkalmazásával.
- *Információbiztonsági szabályzatok és eljárások*, melyek rögzítik a stratégiában meghatározott követelményeket, illetve dokumentálják a folyamatokat.
- *Szabványok és ajánlások*, melyek útmutatást adnak az információbiztonsági rendszer kialakításához, követelmények meghatározásához, védelmi intézkedések bevezetéséhez.
- *Információbiztonsági irányítási szervezet*, mely támogatja az információbiztonság hatékony menedzselését, illetve meghozza a stratégiai döntéseket.
- *Visszamérési, ellenőrzési rendszer*, mely biztosítja a rendszeres visszacsatolást és a megfelelőség biztosítását az előre definiált, jól meghatározott mutatók segítségével.

A felsoroltak közül az egyik legfontosabb elem az információbiztonsági stratégia, mely az információbiztonsági rendszer kialakításának és működtetésének teljes életciklusán átível, illetve minden további elemének megvalósítását, alkalmazását magában foglalja.

Az információbiztonsági irányítási rendszer működtetése során kiemelten fontos, hogy annak céljai és az ezek megvalósításához kapcsolódó erőforrások és felelősségek az információbiztonsági stratégiában egyértelműen meghatározásra és dokumentálásra kerüljenek. Jóváhagyott információbiztonsági stratégia nélkül a rendszer megvalósítása nem, vagy nem teljes körűen, illetve nem megfelelően lehetséges. Az információbiztonsági stratégia kialakítása azonban nem csak a felső vezetés és az információbiztonsági vezető feladata, hanem szoros együttműködést igényel az üzleti és szakterületek vezetőivel, a folyamatgazdákkal is.

A dokumentum további részében az információbiztonsági célok meghatározását, a stratégia kialakítását tekintjük át.

Az információbiztonsági stratégia

1. A stratégia fogalma, célja

A stratégia a célok meghatározásának és megvalósításának eszköze. Általában hosszabb távú terv a szervezeti célok elérésének megvalósításához. Fogalma alatt a szervezeti, üzleti vagy funkcionális célok, és az azok eléréséhez szükséges erőforrások (humán erőforrások, eljárások, eszközök) meghatározását, rendelkezésre állásának, illetve összehangolt működésének biztosítását is értjük. Meghatározható úgy is, mint döntések mintája a szervezetben, melyek azonosítják és meghatározzák a szervezet hosszú-, közép- és rövidtávú céljait, az azokhoz kapcsolódó folyamatokat, vezérelveket, szabályokat és eljárásokat, valamint alacsonyabb szintű terveket dolgoznak ki ezek megvalósítása érdekében.

A stratégiaalkotás egy folyamatos tevékenység, folyamat. A megfelelő stratégia nem csak a meghatározott követelményeknek felel meg, hanem a szervezeti kultúrához is illeszkedik, melynek biztosítása egy kritikus sikertényezője a stratégiában foglaltak sikeres megvalósításának.

A stratégiaalkotás célja, hogy meghatározza a szervezet céljait, felmérje a jelenlegi helyzetet, annak alapján meghatározza azokat a lépéseket, feladatokat, melyek a célok eléréséhez, a kívánt állapot eléréséhez szükségesek, és irányítsa, támogassa azok megvalósítását.

A stratégia elemei

A stratégia alkotás célja ezek alapján a következő pontokba szedhető:

- szervezeti, üzleti vagy funkcionális, működési célok definiálása,
- közép- és hosszú távú célok megkülönböztetése,
- a célok megvalósításához szükséges eszközök, keretek, feltételek megteremtése,
- a célok megvalósításához szükséges pénzügyi erőforrások allokálása, költségek becslése, ráfordítások nyomon követése,
- erőforrások biztosítása,
- a különböző stratégiák átfedéseinek azonosítása, egymáshoz igazítása, összehangolása,
- a stratégia megvalósítását támogató architektúra, szabályzati környezet, eljárások kialakítása,
- mutatók definiálása, melyek segítségével a stratégia megvalósításának sikeressége mérhető, a hibák, eltérések azonosíthatóak a stratégia rendszeres felülvizsgálata során,
- folyamatos monitorozás, riportok és visszamérési lehetőségek biztosítása a stratégiában meghatározott célok megvalósításának nyomon követésére és a mielőbbi beavatkozás lehetőségének megteremtésére,
- változások követése, a stratégia rendkívüli felülvizsgálata és módosítása szervezeti vagy külső változások esetén.

A leírtakból kifolyólag a stratégia jellemzői az alábbiak:

- a szervezet vagy terület jelenlegi állapotából a kívánt, cél állapotába történő elmozdulás lépéseit definiálja,
- rendszeresen aktualizált, naprakész,
- hosszabb távú célokat tartalmaz (3-5 év)
- a célokat magasabb szinten határozza meg, a pontos kivitelezést, megvalósítást nem rögzíti, azokat a kapcsolódó alacsonyabb szintű tervekben határozza meg,
- a célokat a szervezet más stratégiáival összhangban tűzi ki, támogatja más funkciók hatékony működését, az üzleti célok elérését,
- definiálja a felelősöket, hatásköröket, rendelkezésre álló erőforrásokat, költségkeretet,
- definiálja a visszaméréshez szükséges mutatószámokat és célértékeket, megfelelőségi kritériumokat,
- kiindulási alapot nyújt a stratégiában foglalt célokhoz kapcsolódó intézkedési tervek elkészítéséhez,
- rögzített, dokumentált,

- a felső vezetés által jóváhagyott,
- az érintettek felé megfelelően kommunikált,
- számon kérhető.

A stratégia alkotás csak abban az esetben támogatja a szervezet céljainak pontos meghatározását és megvalósítását, amennyiben a legjobb gyakorlatnak megfelelően és a szervezetre szabottan került kialakításra. Az a stratégia, mely nem teljes körűen, vagy nem a szervezet képességeihez mérten kerül definiálásra, nem vagy nem megfelelően támogatja, sőt akár akadályozhatja is a kitűzött célok megvalósítását. (Például egy nem megfelelően kialakított és átgondolt informatikai stratégia alapján egy olyan rendszer került bevezetésre, mely a meglevő rendszerekkel nem teljes mértékben kompatibilis, így többlet fejlesztést igényel, és a működő rendszerek hatékonyságát pedig nem növeli.)

Mindezekből kifolyólag az információbiztonsági stratégia csak abban az esetben lesz sikeresen megvalósítható, ha a felső vezetés, döntéshozók bevonásra kerülnek és támogatják annak kialakítását, végrehajtását, a célok pontosan és érthetően kerülnek megfogalmazásra, valamint priorizálásra, illetve az egymásnak ellent mondó érdekek feloldásra kerülnek.

A megfelelő stratégia siker tényezői (Stackpole, Oksendahl; 2010):

- Egyszerűség
- Elköteleződés
- Alap értékekre történő építés
- Megfelelő kompetenciák, képességek biztosítása
- Kommunikálhatóság
- Megvalósíthatóság

A stratégia alkotás keretrendszerének implementálásához kapcsolódó kritikus sikertényezők a következők (Stackpole, Oksendahl; 2010):

- üzlet-vezérelt stratégiai tervezés módszertan,
- tiszta, érthető célok és egyértelmű tervezés,
- felső vezetés támogatása,
- magas szintű információ-menedzsment képességekkel való rendelkezés,
- minőségi adatforrások alkalmazása,
- a megoldások szervezeti követelményekhez történő igazítása,
- szilárd keretrendszer kialakítása,
- kulcs üzleti-vezérelvek meghatározása és priorizálása mind a teljes szervezet, mind az információbiztonsági terület szintjén (ezek közötti konfliktus kezelése szükséges).

2. A stratégia alkotás előnyei a szervezet számára

A megfelelő stratégiaalkotás az alábbiakban felsorolt előnyöket biztosítja a szervezet számára.

- Üzleti, működési előnyök:
    - Hatékonyság növelése
    - Eredményesség növelése
    - Teljesítmény növekedés
    - Követelmények pontosabb definiálása és könnyebb megértése
    - Területek, funkciók, folyamatok közötti összhang megteremtése
    - Tervezhetőség, ütemezés
- Erőforrásokkal kapcsolatos előnyök:
    - Szabályozottság
    - Nyomon követhetőség, visszamérhetőség
    - Optimalizálás
    - Hatékonyabb allokáció
    - Jobb kihasználtság
    - Megfelelő specifikáció, követelmények
    - Megbízhatóság, rendelkezésre állás növekedése
- Költség ráfordítással kapcsolatos előnyök:
    - Költségek jobb tervezhetősége
    - Ráfordítások nyomon követése
    - Költség optimalizálás
    - Költséghatékonyság növelése
    - Megtakarítások

Az információbiztonsági stratégia kialakításával a szervezet a következőket éri el (CISM Review Manual, 2014):

- Üzleti és információbiztonsági célok összehangolása
- Kockázatmenedzsment hatékonyságának növelése
- Érték teremtés
- Erőforrás optimalizálás
- Teljesítmény mérés
- Folyamatokba történő integráció

3. A stratégia alkotás követelményei

Annak érdekében, hogy a stratégia tényleg az üzleti, illetve funkcionális célokat tartalmazza és azok megvalósítását támogassa, valamint valódi értéket teremtsen a szervezet számára, az abban foglaltaknak meg kell felelniük az alábbi követelményeknek, illetve tartalmazniuk kell a következőket:

- reális, az adott időtávon belül teljesíthető célok,
- holisztikus szemlélet alkalmazása, mely támogatja
    - a biztonsági kockázatok egész szervezetre vonatkozó hatásának azonosítását,
    - a szükséges információbiztonsági követelményeknek jobb megértését,
    - az információbiztonsági működési folyamatokba történő integrálását,
- pontos, bárki számára érthetően definiált célok,
- a rendelkezésre álló erőforrásokra és keretekre építés,
- a törvényi előírásoknak, kötelezettségeknek, egyéb külső követelményeknek való megfelelés biztosítása,
- döntéshozók általi elfogadás, jóváhagyás,
- az érintettek felé történő megfelelő kommunikáció, mely
    - megfelelő időben,
    - megfelelő csatornán keresztül,
    - megfelelő tartalommal,
    - megfelelő nyelvezettel,
    - megfelelő célközönségnek szól,
- a célok megvalósításának, illetve azok eléréséig történő támogatásának biztosítása,
- a visszamérés, monitorozás lehetőségének biztosítása, melynek keretein belül:
    - visszamérhető elemeket, kritikus sikertényezőket és mutatószámokat kell tartalmaznia, melyek alapján meg lehet határozni a megvalósítás eredményességét, valamint ehhez kapcsolódóan,
    - meg kell határozni azt a szintet, mely elérése esetében sikeresnek minősíthető a megvalósítás,
- tartalmazza a riportolási kötelezettségeket, azok
    - gyakoriságát,
    - célközönségét,
    - tartalmát, mutatószámait,

- lehetőséget biztosít a beavatkozásra, amennyiben a stratégia megvalósítása nem a terveknek megfelelően történik, vagy szervezeti, esetleg külső változások miatt újragondolása szükséges.

Ahogyan a követelményekben feltüntetett utolsó pont is előrevetíti, a stratégia megvalósítását több tényező is befolyásolhatja, és bekövetkezésük esetén beavatkozásra van szükség, mely akár a stratégia felülvizsgálatát, módosítását is eredményezheti. Ezek időben történő felismerésére szolgálnak a különféle mutatók, illetve mind a belső, szervezeti változások, mind a környezeti változások folyamatos figyelemmel kísérése. Mindezeket részleteiben „*A stratégiát befolyásoló tényezők*” alfejezet mutatja be.

4. A stratégiák típusai

A szervezet életében többféle stratégiát is megkülönböztethetünk azok tárgya, terjedelme és mélysége szerint. Ezek jellemzően három szintre bonthatóak:

- Szervezeti/vállalati/üzleti stratégia (a továbbiakban üzleti stratégia)
- Üzletági stratégia (amennyiben az adott szervezetnél értelmezhető)
- Funkcionális stratégia (másképp fogalmazva szakterületi stratégia)

A teljesség kedvéért meg kell említeni a stratégiához kapcsolódó, azonban magasabb szintű célkitűzéseket is:

- Vízió
- Misszió

Mindezeket és egymásra épülésüket, a közöttük levő hierarchikus kapcsolatokat az alábbi ábra szemlélteti.

Stratégiai szintek, hierarchia

A **vízió** a szervezet elérni kívánt, jövőbeli állapotát rögzítő, általában konkrét időponthoz nem kötött, magas szintű célkitűzés, iránykijelölés. Ezzel szorosan összhangban, és gyakran egy szinten kerül kialakításra a **misszió**, vagyis a szervezet küldetése, mely a szervezet létezésének célját, értékeit és elveit rögzíti (például érdekcsoportoknak való megfelelés, társadalmi szerepvállalás, szervezeti kultúra és filozófia). Ezek leginkább a tulajdonosok, felsővezetők elképzeléseit, elvárásait tartalmazó célkitűzések, funkcionális, az egyes szakterületekhez kapcsolódó célokat, elvárásokat nem határoznak meg.

Az **üzleti stratégia** a vízió és misszió megvalósítását szolgáló, konkrét célkitűzéseket és azok megvalósításának eszközeit, módszereit tartalmazó magas szintű dokumentum. Ezt lehet lebontani **üzletági stratégiákra**, melyek az egyes üzletágak specifikus célkitűzéseit, és annak megvalósítását tartalmazzák, illetve **funkcionális stratégiákra**, melyek a teljes szervezetet támogató funkciók, szakterületi, alacsonyabb szintű stratégiákat jelentik.

Ilyen funkcionális stratégiák lehetnek:

Funkcionális stratégiák

A funkcionális stratégiák tekinthetőek a különböző erőforrás csoportok működtetését megvalósító stratégiáknak, így támogató célt szolgálnak a magasabb szintű stratégiák megvalósításához. Mindezek miatt ezen stratégiák kialakítása során kiemelten fontos, hogy azok az üzleti (és üzletági) stratégiákkal, valamint a szervezeti képességekkel összhangban kerüljenek kidolgozásra. Amennyiben a funkcionális stratégiák önállóan, szigetszerűen kerülnek megvalósításra, fennáll a veszélye annak, hogy az adott funkcionális stratégia ugyan megfelelően megvalósításra kerül, azonban nem növeli a többi funkcionális vagy üzleti terület működési hatékonyságát, vagy akár akadályozza is azok megfelelő működését (például az információbiztonsági stratégiában meghatározott célok megvalósításra kerültek, azonban a bevezetett védelmi intézkedések jelentette követelmények nem az üzleti területek képességeinek megfelelően lettek kialakítva, ezáltal fennakadásokat is okozhatnak az üzleti folyamatok működésében, vagy megnehezítik, lassítják azok végrehajtását.). Szintén problémát jelenthet, ha az üzleti és funkcionális stratégiákban definiált célok nem, vagy nem megfelelő időben, nem megfelelő minőségben, vagy nem a megfelelő keretek között (például gazdaságtalan erőforrás-felhasználás, többlet költségek) kerülnek megvalósításra (például, ha az információbiztonsági stratégiát nem hangoljuk össze a kommunikációs terület stratégiájával, és az információbiztonsági relevanciájú szabályzatok kialakításánál figyelmen kívül hagyjuk a rendkívüli események kezelésére vonatkozó szabályait, eljárásait, akkor

előfordul, hogy többlet munkát végzünk, mely ráadásul ellentmondásos információkat is tartalmazhat, mely alkalmazási időszakban jelentős problémákat okozhat).

Az információbiztonsági és egyéb funkcionális stratégiák kapcsolódási pontjaira az alábbi ábra tartalmaz néhány egy-egy példát.

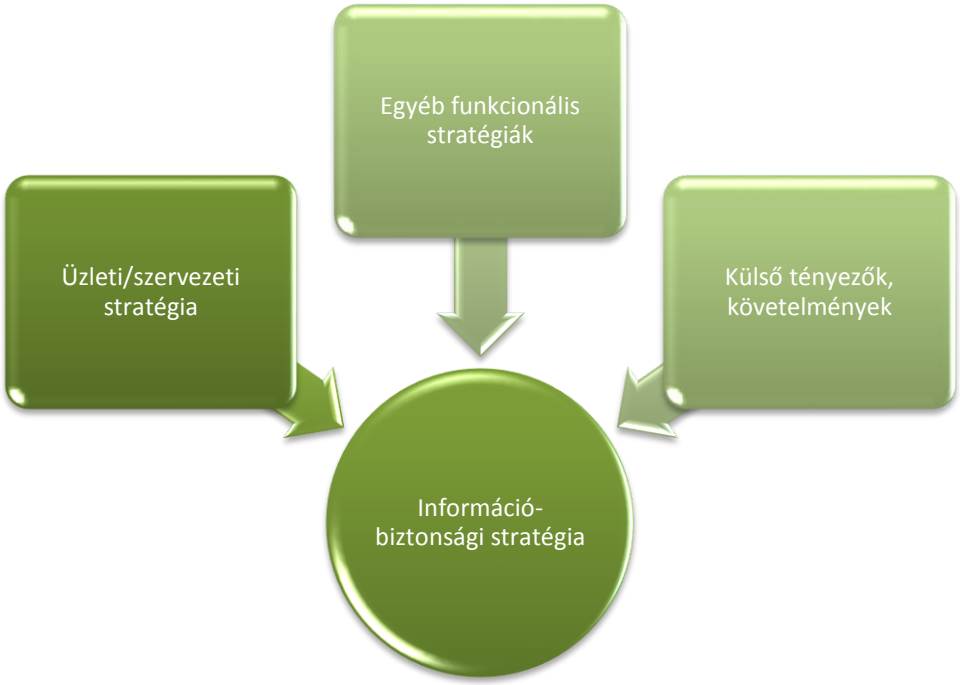
Példák más stratégiákkal való kapcsolódási pontokra

5. Az információbiztonsági stratégia és helye a szervezeti stratégiában

Az informatikai rendszerek alkalmazásának, üzemeltetésének fontosságát manapság már minden szervezet elismerte, hiszen anélkül az üzleti célok elérése lehetetlen. A biztonsági és információbiztonsági funkció azonban sok esetben mind az üzleti célok, mind az informatikai célok, valamint az egyéb támogató funkciók és erőforrásaik mellett az eddigi tapasztalatok alapján gyakran a „szükséges rossz” szerepét tölti be, és sok esetben tévesen egy hátráltató, akadályozó tényezőnek, vagy éppen plusz költségnek tekintik. A legtöbb szervezetnél az információbiztonság leginkább még mindig egy technológia vezérelt, IT központú funkció szerepét tölti be, pedig az információbiztonság a szervezet minden egységét, területét érintő kérdéskör.

Az információbiztonság kapcsolata az üzleti célokkal

Mindezek elkerülésének érdekében az információbiztonsági stratégia is - részben - az üzleti stratégia része kell, hogy legyen, mely alatt az értjük, hogy az üzleti célokkal összhangban kell kialakítani, ezek megvalósítását kell támogatnia, meg kell győzni mind az üzleti területet, mind a kiszolgáló erőforrások üzemeltetőit (jellemzően az informatikai szakterületet), hogy az információbiztonsági célok megvalósítása közös érdekük, és mindegyik fél számára előnyös. Ennek elérése érdekében az információbiztonsági stratégiában meghatározottak az üzleti stratégiából kell, hogy származtathatóak legyenek, azzal szoros összhangban kell állniuk. (Például az üzleti stratégia alapján a szervezet úgy kíván a jogszabályok általi kötelezettségeknek eleget tenni, és ezen túlmenően üzleti előnyre is szert tenni, hogy kiemelten fontosnak tartja és annak megfelelően kezeli az általa nyújtott szolgáltatások biztonságát, az ügyféladatok bizalmas kezelésének megvalósítását, az ezzel kapcsolatos védelmi intézkedések folyamatos fejlesztését és a legújabb technológiák alkalmazását.)



Az információbiztonsági stratégia elhelyezkedése

Mindezek alapján az információbiztonsági stratégia kialakítása során a következő kérdéseket kell feltenni és megválaszolni, kiemelt részletességgel kifejteni az üzleti stratégiával való összhang megteremtése érdekében (Stackpole, Oksendahl; 2010):

- Hogyan tudja az információbiztonság támogatni a szervezeti, üzleti célok megvalósítását?
- Milyen működési és üzleti előnyei származnak a szervezetnek az információbiztonsági irányítási rendszer működtetéséből?
- Hogyan követi az információbiztonsági stratégia a folyamatosan változó követelményeket, iparági trendeket, szervezeti, környezeti és kiemelten a technológiai változásokat?
- Milyen üzleti cél, indok áll ennek megvalósítása mögött?
- Mit szeretne a szervezet elérni az információbiztonság megvalósításával?
- Az információbiztonság hogyan teszi lehetővé, és hogyan támogatja, hogy a szervezet megvalósítsa az üzleti stratégiáját?

Az információbiztonsági stratégia kialakítása után több, alacsonyabb szintű tervre bontható, melyek részletesen „*Az információbiztonság irányítása, a stratégia megvalósítása*” fejezetben kerülnek bemutatásra:

Az információbiztonsági stratégia lebontása

Az információbiztonsági stratégia kialakítása

Az információbiztonsági stratégia kialakításának támogatása, illetve jóváhagyása a felső vezetés felelőssége. Elkészítéséhez össze kell gyűjteni és elemezni kell a szervezet információbiztonsági szintjének jelenlegi állapotból az elérni kívánt állapotba való eljutáshoz szükséges információkat (kiindulási helyzet, rendelkezésre álló erőforrások, lehetséges tevékenységek, azok előnyei, hátrányai, kapcsolódó szabályozások és befolyásoló tényezők, stb.). Ezek alapján meg kell határozni azokat a célokat, tevékenységeket, melyek támogatják a kívánt állapot elérésének megvalósítását, illetve a stratégiában rögzíteni kell az érintett szakterületek által javasolt, az üzlet által elfogadott, illetve a felső vezetés által jóváhagyott információbiztonsági intézkedéseket.

Ebben a fejezetben áttekintjük

- a stratégiaalkotással kapcsolatos feladatokat és felelősségeket,
- a stratégia kialakításához szükséges információkat,
- azok elemzésének és felhasználásának módját,
- a stratégia tartalmi elemeit,
- azok menedzsment szintű elfogadását, valamint
- kommunikálását is.

1. A stratégia kialakításának felelősei

Az információbiztonsági stratégia és az üzleti célok összehangolásával az alábbi csoportoknak vannak a következő feladatai és felelősségei (CISM Review Manual, 2014):

- **Felső vezetés**: stratégiaalkotás támogatása, döntéshozatal
- **Folyamatgazdák**: a biztonsági célok és követelmények üzleti folyamatba történő integrálásának megvalósítása, szakterületi vélemények adás.
- **Információbiztonság irányítási szervezet/bizottság**: az információbiztonsági stratégia kidolgozásának támogatása, felülvizsgálata, annak biztosítása, hogy az üzleti területek és folyamatgazdák támogassák a működési folyamatokba történő integrációt.
- **Információbiztonsági vezető**: az információbiztonsági stratégia kidolgozása, az információbiztonsági program megvalósításának koordinálása, kommunikáció az érintettekkel, folyamatgazdákkal, az üzleti folyamatok és az információbiztonsági célok összekapcsolásának megteremtése.

- **Auditorok**: Információbiztonsági stratégia és rendszer értékelése, felülvizsgálata, javításai, fejlesztési lehetőségek azonosítása.

2. A stratégiaalkotáshoz szükséges információk

A stratégia alkotás alapja az információ. Ezek összegyűjtése során célszerű a rendszer egészét vizsgálni, annak érdekében, hogy jobban megértsük

- kik az információbiztonságban érintett döntéshozók,
- ténylegesen milyen szinten van a szervezet információbiztonsági rendszere jelenleg,
- milyen tényezőket kell figyelembe venni a rendszer kialakítása, fejlesztése során,
- melyek a jelenlegi információbiztonsági trendek,
- milyen jövőbeli hatások várhatóak, melyek befolyásolják az információbiztonságot.

A felsoroltak alapján információra van szükség a jelenlegi helyzetről, kiinduló állapotról, a célokról, a kívánt állapotról, valamint a célok megvalósítását lehetővé tevő eszközökről.

Az információbiztonsági stratégia kialakításához szükséges információk

Ezeket lebontva első körben a szervezet és az információbiztonsági irányítási rendszerre vonatkozó, rendelkezésre álló információkra van szükség, melyek a következők:

- Külső információk
    - Törvényi kötelezettségek és jogszabályi előírások
    - Csoport szintű követelmények
    - Iparági szabványok
    - Piaci környezet
    - Ügyfelek által támasztott követelmények

    - Politikai és társadalmi elvárások
    - Etikai követelmények
    - Technológiai környezet
    - Innováció, trendek
- Belső információk
    - Szervezeti kultúra
    - Szervezeti képességek
    - Rendelkezése álló erőforrások
    - Belső szabályozási környezet
    - Üzleti intelligencia
    - Technológiai környezet
    - Kockázatok
    - Üzleti tényezők

Az üzleti tényezők azok a tényezők, melyek az üzlet előmenetelét támogatják, vagyis olyan külső vagy belső befolyásoló hatások, melyek jelentős hatással bírnak az üzleti folyamatokra, vagy az egész szervezetre.

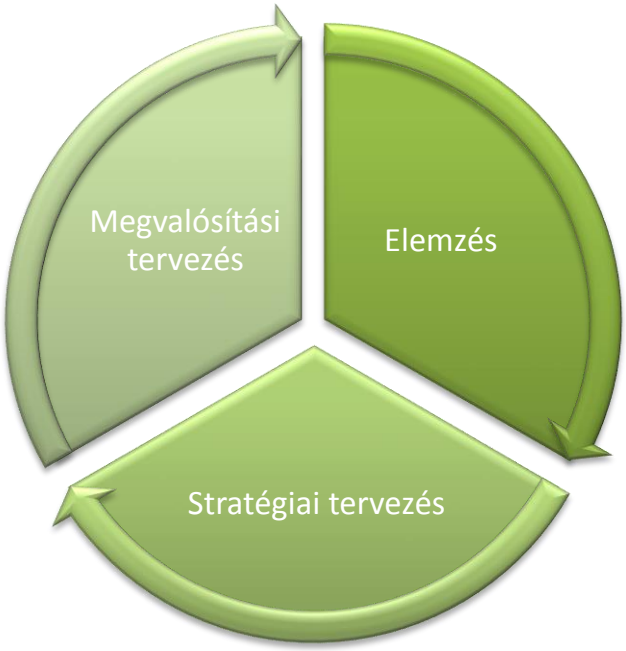
Üzleti tényezőknek tekinthetőek a következők (Stackpole, Oksendahl; 2010):

- Jogszabályok
- Nemzeti vagy nemzetközi szabályozások
- Iparági szabályozás
- Szabványok
- Bizonytalanság
- Márka, hírnév
- IT alkalmazások
- Új technológiák alkalmazásának kockázatai

A gyűjtött információk felhasználására a stratégiaalkotás különböző fázisaiban van szükség, ezek a következő alfejezetben kerülnek bemutatásra.

3. A stratégia alkotás lépései

A szakirodalom a stratégia megalkotásának három fő fázisát különbözteti meg (Stackpole, Oksendahl, 2010):



A stratégia alkotás fő fázisai

Az **elemzés** fázisában az előzőleg összegyűjtött, szükséges információkat, a szervezetre ható mind külső, mind belső hatásokat, követelményeket kell azonosítani, feldolgozni és figyelembe venni.

Az elemzés eredményei alapján kell végrehajtani a **stratégiai tervezés** feladatait, melynek keretein belül definiálni kell az elérni kívánt állapotot, célt és meg kell tervezni a megvalósításához szükséges stratégiát.

A **megvalósítási tervezés** szakaszában pedig a stratégia lebontása történik kisebb tervekre, road-map jellegű megközelítéssel.

A szükséges információk összegyűjtésének és stratégia kialakításának és karbantartásának az alábbi lépéseit különböztethetjük meg általánosságban:

- Először azonosítani kell a szervezetnél alkalmazott stratégiai tervezés folyamatát, és annak megfelelően kell kialakítani az információbiztonsági stratégiát is.
- Azonosítani kell a döntési hatásköröket.
- Meg kell érteni a szervezeti magas szintű célokat (víziót és missziót) és az azokhoz kapcsolódó értékeket, szemléletet, filozófiát.

- Azonosítani és értékelni kell a szervezet külső és belső környezetét, az ezekhez kapcsolódó erősségeket, gyengeségeket, lehetőségeket és veszélyeket. (SWOT analízis, kockázatelemzés)
- Azonosítani kell a szervezeti, üzleti stratégiai célokat.
- Meg kell határozni azokat az információbiztonsági célokat, intézkedéseket, melyek ezek elérését, hatékonyságnövelését támogatni tudják.
- A kitűzött célokat, tervezett információbiztonsági intézkedéseket stratégiai tervben kell rögzíteni, meg kell határozni hozzájuk a szükséges erőforrásokat, kereteket.
- Ki kell fejleszteni egy hatékony megvalósítási folyamatot.
- A stratégiában foglaltakat jóvá kell hagyatni a felső vezetéssel, döntéshozókkal.
- Előre meghatározott időközönként, vagy külső és belső tényezők változásakor felül kell vizsgálni, és szükség esetén módosítani kell a stratégiát.

Ezek különböző al-fázisait különböztethetjük meg:

- Elemzés
    - Jelenlegi helyzet felmérése
    - Elérni kívánt állapot azonosítása
- Stratégiai tervezés
    - Elérni kívánt állapot definiálása
    - Célok meghatározása
- Megvalósítási tervezés
    - Tervekre bontás

A stratégia kialakítása

Ennek alapján mennyiben például a stratégiai célkitűzés az, hogy a vállalat az üzleti előny megszerzéséhez, illetve információbiztonsági irányítási rendszerének hatékony működtetéséhez szeretné megszerezni az ISO/IEC 27001:2013 tanúsítványt. Ennek megvalósításához először is meg kell állapítani, hogy jelenleg milyen szinten van az információbiztonsági irányítási rendszer kialakítva az ISO/IEC 27001:2013 szabvány követelményeinek megfelelően, milyen intézkedéseket és milyen hatékonysággal alkalmazunk (jelenlegi helyzet felmérése). Következő lépésként azonosítani kell, hogy milyen hiányosságok, eltérések vannak az információbiztonsági irányítási rendszerünkben a szabványban foglaltakhoz képest (elérni kívánt állapot azonosítása), majd az azonosított hiányosságok és eltérések alapján meg kell határozni, hogy miket kell megvalósítani, fejleszteni, annak érdekében, hogy realizálható legyen a cél elérése (elérni kívánt állapot definiálása). Ezek után meg kell határozni, hogyan szeretnénk ezeket a fejlesztéseket megvalósítani, az aktuális védelmi intézkedéseket módosítani, illetve milyen új védelmi intézkedéseket szeretnénk bevezetni, milyen erőforrások szükségesek ezek megvalósításához, illetve hogyan szeretnénk ezek megvalósítását ütemezni és nyomon követni, visszamérni (célok meghatározása). Miután ezek a célok jóváhagyásra kerülnek, következhet a célok alacsonyabb szintű tervekre bontása. Ezek a tervek tartalmazzák a feladatok részletes leírását, felelőseit, visszamérésük és monitorozásuk követelményeit. Jellemzően ezek nem a stratégia

dokumentumában kerülnek rögzítésre, viszont szoros kapcsolatban állnak azzal és együtt alkalmazandóak (tervekre bontás).
Amennyiben a stratégiában foglalt célok, részcélok megvalósításra kerülnek, azok eredményességének visszamérése szükséges, valamint a stratégia felülvizsgálata, és indokolt esetben módosítása javasolt.

Jelenlegi helyzet felmérése

Az információbiztonsági stratégia elkészítésének alapja a jelenlegi helyzet feltárása, melynek során előállnak a stratégiaalkotáshoz szükséges információk.
A következő információk szükségesek az információbiztonsági stratégia kialakításához:

- Az információbiztonság jelenlegi szintje, aktuális állapota
- Jelenlegi információbiztonsági követelmények, valamint amennyiben rendelkezésre áll, aktuális stratégia
- Üzleti hatáselemzés eredménye, azonosított kritikus folyamatok és erőforrások listája (amennyiben rendelkezésre áll)
- Kockázatelemzés eredménye, azonosított sérülékenységek és fenyegetések, ezekből származó kockázatok (amennyiben rendelkezésre áll)
- Jelenleg bevezetett információbiztonsági kontrollok, védelmi intézkedések, ezek megvalósításával elért maradvány kockázatok
- Jelenlegi biztonságtudatossági szint, biztonsági kultúra

Az információbiztonsági stratégia megalkotásának két fő segédeszköze az üzleti hatáselemzés, illetve a kockázatelemzés eredménye – ezek elkészítését és rendszeres felülvizsgálatát mindenképpen tartalmaznia kell a stratégiának, valamint a stratégiai célokat ezek alapján javasolt meghatározni.

Üzleti hatáselemzés

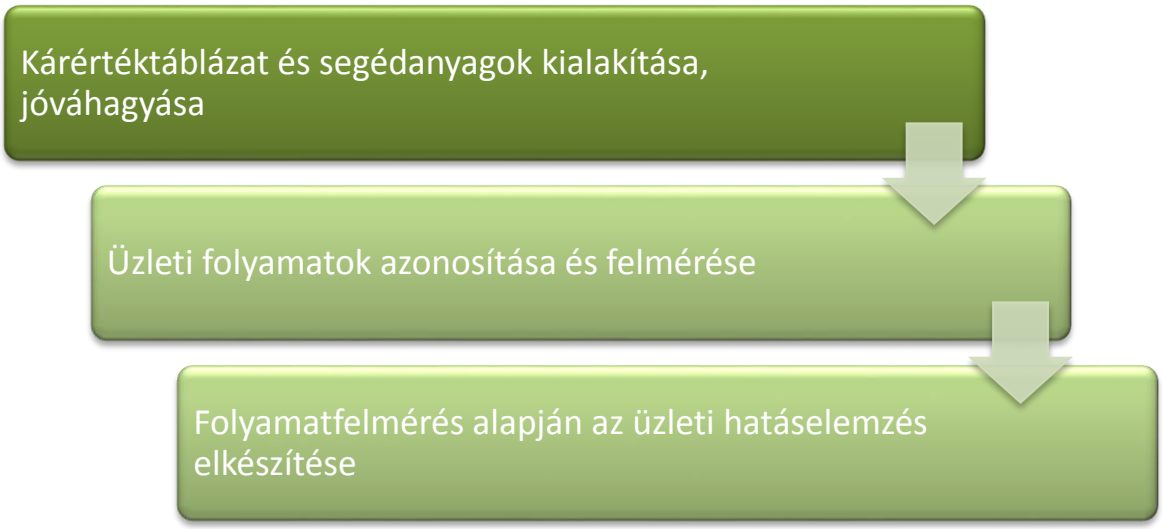
Az üzleti hatáselemzés célja annak meghatározása, hogy melyek a szervezet kritikus üzleti folyamatai, azok milyen kritikus támogató erőforrásoktól, más folyamatoktól függnek, továbbá azt vizsgálja, hogy egy váratlanul bekövetkező, nem kívánt esemény milyen negatív hatással van ezekre az üzleti folyamatokra, kiesésük esetén milyen jellegű és mértékű kárral kell számolnia a szervezetnek.
A kiesési hatások mértékének ismeretében határozhatóak meg a szervezet kritikus folyamatai.
A hatáselemzés elkészítéséhez a folyamatgazda, illetve az általa kijelölt személyek

szolgáltatnak adatokat, az adott folyamat leállása esetén várható kárkövetkezményeket a gyakorlati tapasztalatok, a korábbi trendek, illetve becslések alapján határozzák meg. Ezek egy előre kialakított kárérték táblázat alapján kerülnek megállapításra, mely a szervezet által meghatározott, és a felső vezetés által jóváhagyott segéd-dokumentum.

A kárérték táblázat tartalmazza a szervezetnél értelmezett:

- kártípusokat
- kiesési hatások mértékének skáláját

Elkészítésének lépései jellemzően a következők:



Üzleti hatáselemzés készítése

A folyamat részletes lépései:

- Szervezetre szabott kárérték táblázat elkészítése és jóváhagyatása a felső vezetéssel
- Folyamatok felmérése
    - Szabályozó dokumentumok, eljárások vizsgálata
    - Folyamatfelmérő kérdőívek alkalmazása
        - Folyamat alapadatainak felmérése
        - Felelősök azonosítása
        - Erőforrások azonosítása
    - Interjú a folyamatgazdákkal
        - Üzleti területek és folyamataik, azok részletes lépéseinek megismerése
        - Folyamatban alkalmazott erőforrások és folyamat-függések azonosítása
        - Folyamat maximális kiesési idejének meghatározása
        - Folyamat kiesése esetén felmerülő károk, kiesési hatások azonosítása (kárérték táblázat segítségével)

        - A káresemény kiváltó okainak elemzése nem tartozik jelen felmérés hatókörébe!
- Üzleti hatáselemzés elkészítése
    - Interjúk eredményeinek feldolgozása
    - Eredmények rögzítése (például erre a célra kialakított Excel táblázatban, üzleti hatáselemzés készítését támogató alkalmazásban, üzletfolytonossági rendszert támogató szoftverrel)
    - Kritikus üzleti folyamatok azonosítása
    - Kritikus erőforrások azonosítása
    - Maximális kiesési idők azonosítása
    - Folyamatok priorizálása

Az üzleti hatáselemzés általában az alábbi kártípusok esetleges bekövetkezését vizsgálja:

- anyagi kár (közvetlen vagy közvetett)
- jogi kár
- reputációs kár
- működési kár
- társadalmi kár,
- egyéb, az adott szervezetre vonatkozóan értelmezhető kártípus

A hatáselemzés részét képezi a megengedett maximális kiesési idő meghatározása is, azaz annak az időtartamnak a meghatározása, melyben a folyamat leállása még tolerálható. A hatáselemzésnél azt vizsgáljuk, hogy a megengedett maximális kiesési időn túli leállás mekkora kárt okoz.

Ezek mellett vizsgálni kell a kritikus időszakokat, vagyis azokat a dátumokat, időpontokat, amelyek esetén a megengedett kiesési idők rövidebbek lehetnek. Ilyen kritikus időszak lehet például egy törvényi kötelezettség teljesítéséhez kapcsolódó dátum (illetve a feladat végrehajtásához szükséges időtartam, ezáltal meghatározott időszak), napszak, melyben egy adott feladatot végre kell hajtani (például napi riport leadása minden nap 16:00-ig).

A maximális kiesési idő megadásánál jellemzően az alábbi értékeket vesszük alapul, de ezeket is a szervezetre lehet és kell is szabni:

- 30 perc
- 1 óra
- 2 óra
- 4 óra

- 1 nap
- 1-3 nap
- 3-5 nap
- 5-7 nap
- 7 nap felett.

Ezeken az értékeken kívül természetesen figyelembe kell venni az egyes üzleti területek által esetlegesen pontosabban meghatározott kiesési időket (például 2,5 óra, 6 óra, stb.)

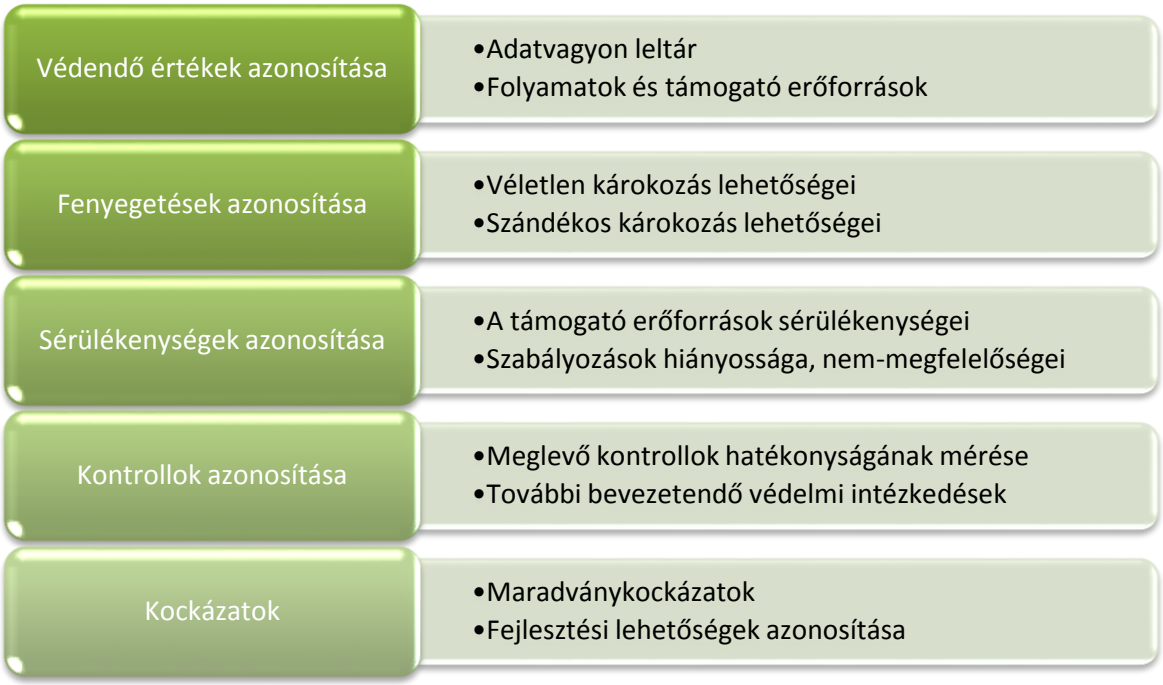
A hatáselemzés eredményei alapján a folyamatok általában három kategóriába sorolhatók:

- kritikus,
- közepesen kritikus,
- nem kritikus folyamatok.

A folyamatok kritikussági besorolását annak alapján kell meghatározni, hogy milyen mértékű a kiesési hatása. Kritikusnak minősül általában a „jelentős" vagy „kritikus" hatás, közepesen kritikusnak a „mérsékelt" hatás, a nem kritikus folyamatok pedig általában az „elhanyagolható" vagy „minimális" kiesési hatással rendelkezők.

Kockázatelemzés

Az információbiztonsági stratégia legfontosabb kérdése: mi a cél, mit szeretnénk elérni? A kérdés megválaszolásához a legfontosabb információ, hogy tulajdonképpen mi is a védendő érték a vállalat számára, milyen sérülékenységeik vannak az azokat tároló, kezelő, továbbító erőforrásoknak, azokat milyen fenyegetések használhatják ki, mitől kell megvédeni, hogyan kell megvalósítani a védelmet, illetve hogyan kell meggyőződni arról, hogy a védelem megfelelően és hatékonyan működik.



Kockázatok azonosítása

Az információbiztonsági irányítási rendszer bevezetésének és az információbiztonsági stratégia kialakításának elsődleges alapja az információbiztonsági kockázatelemzés elkészítése, mely tartalmazza a szervezetnél azonosított, aktuális információbiztonsági kockázatokat. A stratégiát, illetve a későbbiekben bevezetendő védelmi intézkedéseket és eljárásokat célszerűen ezeknek megfelelően kell kialakítani.

A kockázatelemzés végrehajtásával és az erre épülő stratégiaalkotással a szervezet tisztábban látja a szervezetet érintő, potenciális kockázatokat, pontosabban meg tudja állapítani és hatékonyabban tudja tervezni és allokálni az ezek kezelésére irányuló védelmi intézkedések költségeit, a stratégiában megfogalmazott célokat, intézkedéseket gyorsabban és eredményesebben be tudja építeni a folyamatokba, szolgáltatásokba és termékekbe, valamint az infrastruktúrába. (Stackpole, Oksendahl; 2010)

A kockázatelemzés során azonosított kockázatok kezelésének módjáról a menedzsment hozza meg a döntést, mely lehet:

- Az azonosított kockázat(ok) elutasítása
- Az azonosított kockázat(ok) felvállalása
- Védelmi intézkedések vezetése az azonosított kockázat(ok) bekövetkezési valószínűségének, vagy bekövetkezés esetén okozott hatásának csökkentésére. A bevezetendő védelmi intézkedések lehetnek:
    - Megelőző (preventív) védelmi intézkedések

- Észlelő (detektív) védelmi intézkedések
- Javító (korrektív) védelmi intézkedések

A kockázatelemzés elkészítésének lépései az alábbiak:

Kockázat menedzsment módszertan kidolgozása

A kockázatok azonosításának és felmérésének első lépése egy kockázat menedzsment módszertan elkészítése, mely a Szervezetre szabva tartalmazza a kockázatelemzés végrehajtásának lépéseit és részletes leírását, valamint rögzíti az alkalmazott segédleteket, úgy mint:

- releváns bekövetkezési gyakoriságok,
- a felmérés során alkalmazott kárérték-táblázat (bekövetkezési hatások),
- kockázati szint meghatározás.

A kárérték táblázat kialakítása során meg kell határozni a szervezetre vonatkozó:

- Kártípusokat (közvetlen anyagi kár, közvetett anyagi kár, jogsértés, reputációs kár, személyi sérülés, egyéb értelmezhető kártípus)
- Kárérték skálát (1-5, 1-6 stb. értékekkel, valamint a kárértékekhez tartozó leírással kártípusonként)

Mivel ezen dokumentum képezi a felmérés alapját, az ebben szereplő paraméterek módosítása a módszertan véglegesítéséig lehetséges, a megvalósítás során az adott projektben nincs rá mód, hiszen az a már elkészült felmérések újraértékelését vonná maga után.

Adatvagyonleltár készítés

A kockázatelemzés elkészítésének alapja, hogy a szervezet azonosítsa az üzleti folyamatai által használt adatvagyon elemeket, valamint az azokhoz kapcsolódó erőforrásokat. Ezek azonosításának módja az adatvagyonleltár elkészítése, melynek során a folyamatgazdákkal folytatott interjúk keretein belül fel kell mérni és rögzíteni kell a szervezet:

- adatvagyon elemeit, a folyamatok által használt információkat,
- azok megjelenési formáját, adathordozóját és tárolási helyét (papír alapon vagy elektronikusan tárolva, szabadon hozzáférhetően vagy elzárt helyen),
- az azokat feldolgozó informatikai rendszereket (IT erőforrások),
- az azokhoz hozzáférési jogosultsággal rendelkező munkakörök megnevezését (humán erőforrások), illetve a hozzáférési jogosultságot (írás, olvasás, törlés),
- az adatgazdát.

Az egyes adatvagyon elemeket biztonsági osztályba (nyilvános, belső használatú, bizalmas, szigorúan bizalmas, stb.) kell sorolni, melynek adatbiztonsági osztályait és besorolási elveit a Szervezetnél kialakításra kerülő Adatvédelmi és adatkezelési szabályzat, valamint az információbiztonsági előírások is kell, hogy tartalmazzák.

Kockázatelemzés

A kockázatelemzés során fel kell tárni az előző lépésben azonosított információkat és a hozzájuk kapcsolódó erőforrásokat érintő kockázatokat, vagyis a releváns fenyegetéseket, azok bekövetkezési gyakoriságát, továbbá a bekövetkezés során – legrosszabb esetet feltételezve - keletkezett kár mértékét és típusát (hatást), valamint a fenyegetések bekövetkezéséhez vezető sérülékenységeket. Az elemzés során a kockázatokat három szempontot kell vizsgálni, annak megfelelően, hogy az adatok

- bizalmassága,
- sértetlensége,
- rendelkezésre állása

sérül. Az értékelés során figyelembe kell venni a szervezetnél jelenleg hatályban levő védelmi intézkedéseket is, melyek célja a kockázatok bekövetkezési valószínűségének és/vagy hatásának a csökkentése.

A kockázatelemzésben az azonosított kockázatok mellett javaslat készül a kockázatok kezelésére irányuló védelmi intézkedésekre, melyek bevezetéséről, alkalmazásáról a felső vezetés hozza meg a döntést. Azon kockázatok, melyek csökkentésére a felső vezetés nem tervezi védelmi intézkedés bevezetését, felvállalt kockázatnak tekintendőek, ezekről a felső vezetés hozza meg a döntést, illetve hagyja azokat írásban jóvá.

Azon kockázatok esetén, melyek valamilyen védelmi intézkedés bevezetésével vagy tervezésével kezelésre kerülnek, azonosításra kerülnek a védelmi intézkedések bevezetése után fennmaradó, a továbbiakban már nem csökkenthető kockázatok, és rögzítésre kerülnek a maradványkockázatok listáján. A maradványkockázatok elfogadásáról a felső vezetés hozza meg a döntést, és írásban nyilatkozik azok felvállalásáról.

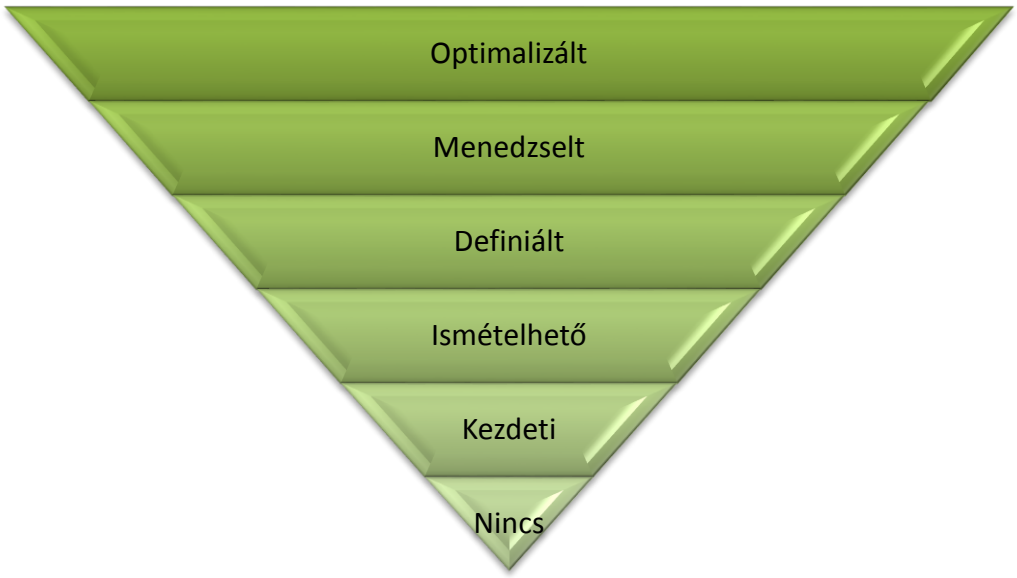
A kockázatok kezelésének módja és eszközei a kockázatkezelési stratégiában kerülnek meghatározásra, melynek dokumentuma a kockázatok változásával folyamatosan felülvizsgálatra és frissítésre, aktualizálásra kerül.

Elérni kívánt állapot definiálása

Az elérni kívánt állapot definiálása során a célul kitűzött információbiztonsági érettség szintjét kell meghatározni a következő információk felhasználásával:

- Szervezeti követelmények
- Az üzleti folyamatok követelményei
- Egyéb funkcionális stratégiák
- Törvényi előírások, kötelezettségek
- Csoportszintű követelmények
- Szabványokban, ajánlásokban meghatározott követelmények, javaslatok
- Benchmarking tapasztalatai
- A megvalósítás és működtetésének ellenőrzési, visszamérési követelményei, mutatószámok
- Felső vezetés által jóváhagyott elfogadott kockázatkezelési stratégia, kockázati szint, elfogadott maradványkockázatok

A kívánt állapotot érettségi szint modellekkel is definiálhatjuk, melyek közül jelen dokumentumban a Capability Maturity Model (CMM) elemeit tekintjük át. (CISM Review Manual, 2014) A modell 5 szintjét különbözteti meg az egyes egymásra épülő érettségi szintnek:



CMM modell

1. *Kezdeti*: kialakítatlan, ad-hoc, nem megismételhető folyamatok.
2. *Ismételhető*: a folyamatok kialakításra kerültek, és a gyakorlatban működnek, azonban nem dokumentáltak.
3. *Definiált*: a folyamatok lépései rögzítésre, dokumentálásra kerültek.
4. *Menedzselt*: a folyamatok végrehajtása kontrollált, mérőszámok és mutatók kerültek meghatározásra a visszaméréshez, értékeléshez.
5. *Optimalizált*: a folyamatok a visszamérés, értékelés alapján fejlesztésre kerülnek.

A kívánt állapot meghatározásához nyújtanak hasznos segítséget a COBIT 5 vezérelvei is, melyek a következők:

- Tulajdonosi és felsővezetői érdekek és az információbiztonsági igények, követelmények egyeztetése.
- A szervezet teljes mértékű lefedése, vagyis az információbiztonsági rendszernek a szervezet minden funkciójára, folyamatára, erőforrására ki kell terjednie.
- Egy keretrendszer kiválasztása (szabvány, legjobb gyakorlat) és annak alkalmazása a tervezés és megvalósítás során.
- Teljeskörűségre, a rendszer egészének vizsgálatára vonatkozó holisztikus megközelítés alkalmazása..
- A vezető (governance) és az irányító (management) funkció elkülönítése, vagyis a döntéshozatal és a végrehajtás irányításának szétválasztása.

Célok meghatározása és elérésük eszközei

A kívánt állapot definiálása után meg kell határozni az annak elérését támogató célokat, vagyis azokat az információbiztonsági intézkedéseket és kontrollokat, melyek a kívánt biztonsági szint elérését lehetővé teszik.

A megvalósítás lehetséges eszközei az alábbiakat foglalják magukban:

- Védendő értékek és védelmi igényszintjük meghatározása a kockázatarányos védelem megvalósításához
- Jóváhagyott alkalmazható védelmi intézkedések és kontrollok, fejlesztési lehetőségek
    - fizikai biztonsági intézkedések
    - logikai védelmi intézkedések
    - adminisztratív kontrollok
- felső vezetés által jóváhagyott költség- és időráfordítás
- támogató erőforrások biztosítása, megfelelő erőforrás allokálás
- feladatok és felelősségek dokumentálása

4. Az információbiztonsági stratégia tartalma

Ahogyan bemutatásra került, az információbiztonsági stratégia célja, hogy meghatározza az információbiztonsági szint, irányítási rendszer elérendő, kívánt állapotát az üzleti és az információbiztonsági célok kitűzésével, összehangolásával. A stratégia dokumentuma ennek megvalósításának alapja, ez tartalmazza az információbiztonsági irányítási rendszer, védelmi intézkedések megvalósításának magas szintű tervét, annak érdekében, hogy implementálásra kerüljön, illetve elérje a kitűzött célokat.

A stratégia dokumentuma a következőket tartalmazza (Stackpole, Oksendahl; 2010):

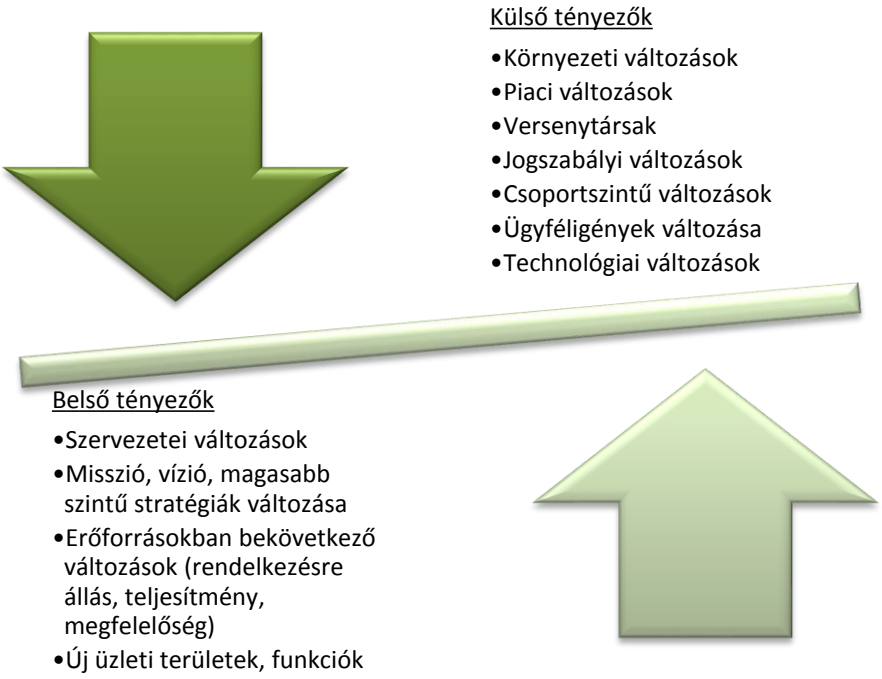
- az információbiztonság fogalma, meghatározása (mit ért alatta a szervezet)
- az információbiztonsági követelmények magas szintű megfogalmazása (milyen szintre szeretne eljutni a szervezet)
- az információbiztonság jelentőségének kifejtését
- az információbiztonsági követelmények megvalósításának üzleti előnyeit, hogyan támogatja az üzleti célokat és hogyan került összehangolásra a szervezeti és más funkcionális stratégiákkal
- elsődlegesen az üzleti célokhoz illesztett információbiztonsági célokat (például ügyféladatok bizalmas kezelése)
- a hatékonyan működő információbiztonsági irányítási rendszer hasznát, jelentőségét a szervezet számára
- az információbiztonsági keretrendszer leírása, az információbiztonság szervezetbe, folyamatokba történő integrálásának terve
- annak bemutatása, hogy az információbiztonsági célok hogyan kerülnek teljesítésre
- a végrehajtásban felelősök, döntéshozók és közreműködők meghatározása
- a célok teljesülésének mérési és értékelési rendszere
- a szervezetre jellemző kockázatok rövid bemutatása és a kockázatelemzés eredményének rövid áttekintése (kiemelve a főbb kockázatokat)
- kockázatkezelési stratégia és a szervezet kockázatvállalási, tűrési képessége
- az azonosított, ismert információbiztonsági problémák és kezelési lehetőségeiknek leírása
- az információbiztonsági irányítási rendszer hatékony működését akadályozó jelenlegi tényezők

- információbiztonsági trendek bemutatása, illetve azok hatása és alkalmazhatósága a szervezetre vonatkozóan
- outsourcing, kiszervezés stratégia (mit érdemes kiszervezni, illetve mit célszerű házon belül tartani)
- megvalósítási terv
- kommunikációs terv
- a szervezet biztonságtudatossági fejlesztésének, információbiztonsági oktatásának stratégiája
- a stratégiai tervben megfogalmazottak megvalósításának nyomon követésére, eredményének visszamérésére szolgáló mutatók és kulcs teljesítmény mutatók meghatározása, célértékek definiálása
- a stratégia rendszeres felülvizsgálatának, ütemezésének meghatározása, követelményei
- a stratégiai tervek karbantartásának, frissítésének dokumentált folyamatának meghatározása

5. A stratégiára ható, befolyásoló tényezők

A stratégia kialakítására és megvalósítására ható tényezők közül megkülönböztethetünk külső és belső tényezőket. A külső tényezőkre, mint például a jogszabályi változásokra, ügyfél igények módosulására, új versenytársak megjelenésére a szervezetnek nincsen ráhatása, hanem követnie kell ezeket a változásokat, alkalmazkodnia kell ezekhez, és a stratégiáját is ezeknek megfelelően kell átértékelnie, szükség esetén módosítania. Kiemelten fontos mindezek miatt a nyomonkövethetőség, folyamatos változáskövetés biztosítása (például rendszeres jogszabálykövetés, ügyfél igények felmérése, piacelemzés, kutatás-fejlesztés). Informatikai és biztonsági szempontból elsősorban az innovációk, új technológiai megoldások folyamatos megjelenése és gyors változása jelenti a kihívást mind az üzleti, mind az információbiztonsági stratégia kialakításakor és felülvizsgálatakor.

A belső tényezők már könnyebben azonosíthatóak és kezelhetőek, hiszen megfelelő mutatók alkalmazásával általában jobban előre jelezhetőek és tervezhetőek. Funkcionális stratégiák szempontjából a változások többnyire magasabb szintű stratégiák módosulásából, vagy feltárt nem-megfelelőségekből, hiányosságokból, a tervezés pontatlanságainak azonosításából generálódnak.



A stratégiára ható tényezők

A külső vagy belső tényezők által indukált bekövetkezett változások a következő tényezők átgondolását indokolhatják a stratégiában:

- Stratégiai célok átgondolása (Tényleg ez a megfelelő irány az üzleti célok elérésének támogatására?)
- Bevont erőforrások átgondolása (Tényleg ezek az erőforrások, és ezekkel a paraméterekkel szükségesek a célok eléréséhez? A megfelelő erőforrásokkal dolgozunk?)
- Erőforrás allokálás átgondolása (A megfelelő erőforrások a megfelelő helyen és időben kerülnek bevonásra? Megfelelően használjuk az erőforrásokat?)
- Ütemezés átgondolása (A célokat megvalósító terveket, lépéseket a megfelelő prioritásokkal, megfelelő időben és tartható határidőkkel hajtjuk végre? Miből származnak/származhatnak csúszások?)

6. A stratégia jóváhagyása, döntés a megvalósításról

A stratégiában meghatározott célok csak jóváhagyás után bonthatóak alacsonyabb szintű tervekre a megvalósítás megkezdése érdekében. A stratégiában meghatározott célok megvalósításáról a felső vezetésnek kell meghoznia a döntést.

A döntés során figyelembe vett szempontok:

- megvalósíthatóság

- rendelkezésre álló és szükséges erőforrások
- költség ráfordítások, költség-haszon elemzés
- ütemezés, határidők
- megvalósítási alternatívák
- más stratégiákkal, tervekkel való összhang, kapcsolat
- prioritások

Amennyiben a felső vezetés nem hagyja jóvá a kitűzött célokat, illetve az azok elérését támogató eszközöket, a stratégia felülvizsgálata, újragondolása és módosítása szükséges.

7. A stratégia kommunikálása

A jóváhagyott stratégia alapján alacsonyabb szintű terveket kell készíteni a megvalósítás részleteinek kidolgozásához. Ehhez elengedhetetlen, hogy a stratégiában foglaltak megfelelő időben és megfelelő tartalommal kommunikálásra kerüljenek az érintett személyek felé.
A stratégia kommunikálása során a következő tényezőket kell figyelembe venni (Stackpole, Oksendahl; 2010):

- Kommunikációs stratégia kialakítása:
    - Kommunikáció céljának pontos, objektív definiálása
    - Tartalom és célközönség meghatározása
    - Időzítés és gyakoriság meghatározása
    - Kommunikációs stílus, nyelvezet
    - Kommunikációs csatornák meghatározása
    - Kérdések, visszajelzések kezelése
- Kommunikációs csatornák sajátosságai
    - Korlátozások (például e-mail csatolmány maximális mérete)
    - Elérhetőség
    - Interakció
    - Több csatorna egyidejű alkalmazása
- Tartalom közvetítő technika
    - Szervezeti kultúrához illesztés
    - Célközönségnek szánt nyelvezet
    - Érthetőség

8. Az információbiztonsági stratégia kialakításának nehézségei, kihívásai

Az információbiztonsági stratégia kialakításakor nehézséget jelent, hogy mind az információbiztonság szervezetben elfoglalt szerepével, funkciójával, mind pedig általában a stratégiaalkotással ellenérzések, tévhitek, negatív tapasztalatok megléte jellemző.

A stratégiákkal kapcsolatos tévhitek (Stackpole, Oksendahl; 2010):

- A stratégiai tervezésnek nincsen jelentősége, hiszen az abban foglaltak nem a valós tevékenységeket rögzítik, hanem csak magas szinten közelítik meg a felső vezetés által meghatározott vagy jóváhagyott követelményeket. Pedig enélkül a rész-célok, megvalósítandó tervek kitűzése és megvalósítása kevésbé hatékonyan, vagy akár csak vaktában történik.
- A stratégiaalkotás csak egy éves rendszerességű feladat, és az elkészített dokumentum csak a „fiók alján pihen" a felülvizsgálatig. Valójában a stratégia célja, hogy az érintettek szemléletmódján, hozzáállásán változtasson, és annak segítségével támogassa a célok megvalósulását.
- Gyakori tévhit, hogy a stratégiaalkotásban csak a szervezet felső vezetése érintett. Habár a stratégiaalkotás valóban menedzsment szintű hatáskör, azonban kialakításában és megvalósításában minden munkavállaló érintett.
- A múltbeli trendek elemzése megfelelő bemenő adatokat szolgáltat a jövőre vonatkozó stratégia kidolgozásához. Megfelelő stratégia kialakítása azonban csak abban az esetben lehetséges, ha a szervezet a jövő lehetőségeit vizsgálja, és nem a múltból indul ki. Ez a szemlélet támogatja a stratégia iránti elköteleződést is.
- Folyamatos kontroll, felügyelet alatt állunk. Valójában a stratégia nem annak az eszköze, hogy a felső vezetés vagy a felelősök érvényesítsék az akaratukat, hanem hogy együttműködjenek a stratégiában foglaltak megvalósításában résztvevő munkavállalókkal.
- A változásnak rendbontó hatása van.

Az információbiztonsággal kapcsolatos tévhitek (Stackpole, Oksendahl; 2010):

- Az információbiztonság nem támogatja, hanem inkább hátráltatja, akadályozza az üzleti folyamatokat.
- A biztonság megoldások csak fekete-fehérek lehetnek, arany középút nem létezik.

- A biztonsággal foglalkozó munkatársak mindegyike arrogáns és főnöknek képzeli magát.
- A biztonság nem érti a szervezeti célokat, üzleti tevékenységet.
- A biztonság egy STOP táblával szemléltethető a legjobban – csak a tiltás jellemző rá.
- A biztonság alatt az őröket, fegyvereket, beléptető rendszereket értjük.
- Az információbiztonság nyers és nehezen érthető.
- A biztonságért felelős munkatársak nem fogadják szívesen a változásokat.
- A biztonság rugalmatlan.

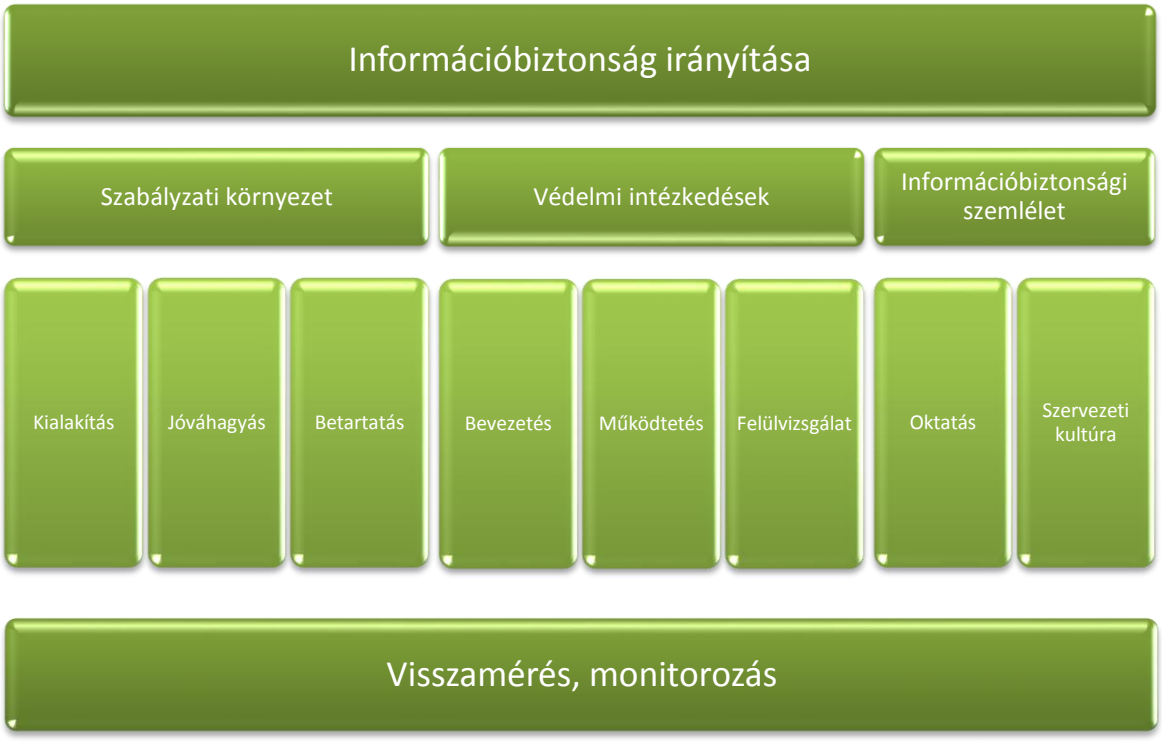
Ezen tényezők kezelése és tisztázása után valós kihívást jelentenek a következők:

- A szervezeti és üzleti célok megfelelő megértése,
- Olyan rugalmas biztonsági architektúra tervezése, mely megfelelően tudja kezelni, követni a környezeti változásokat
- Integrált megközelítés alkalmazása a lokális megoldások helyett
- A sikeres megvalósításhoz, skálázhatósághoz és kihasználtsághoz megfelelően össze kell kapcsolni a vállalati stratégiát, illetve a mutatókat
- Szisztematikus megközelítés alkalmazása
- Költségek menedzselése, megfelelő finanszírozás
- Hatékony kockázat menedzsment támogatása
- Annak a szemléletnek a megváltoztatása, hogy az információbiztonság csak akadályozó tényezője az üzleti célok elérésének.
- A stratégiában megfogalmazottak célközönségnek megfelelő, hatékony kommunikálása.

Az információbiztonság irányítása, a stratégia megvalósítása

Az információbiztonsági stratégiában foglaltak megvalósítása az információbiztonsági irányítási rendszer irányításának keretein belül valósul meg, lényegében ez biztosítja a rendszer működésének alapját, kereteit. A stratégia megvalósításával ugyan más tantárgyak is részletesen foglalkoznak, emiatt más jegyzetekkel átfedések tapasztalhatóak, jelen fejezetben a stratégia megvalósítása kifejezetten az információbiztonsági stratégiára fókuszáltan kerül bemutatásra.

Az információbiztonság irányításának elemei három fő csoportra bonthatóak, melyeket az alábbi ábra szemléltet, és bemutatásra kerülnek ezen fejezetben. Ezek visszamérésének, monitorozásának követelményei és módszerei pedig a következő fejezetben kerülnek bemutatásra.



Az információbiztonsági irányítási rendszer elemei

Mielőtt azonban a három fő csoportot áttekintenénk, a stratégia megvalósításához elengedhetetlen két tényezőt mutatom be: a szükséges tervek elkészítésének feltételeit, valamint a stratégia megvalósítását támogató, információbiztonsági szervezet felépítését.

1. Tervezés, a stratégia lebontása

A stratégiában meghatározott magas szintű célok teljesítésének feltétele, hogy azok alacsonyabb szintű részcélokra, akciótervekre kerüljenek lebontásra. Ezek a tervek részletesen tartalmazzák a stratégiában foglalt célkitűzések megvalósításához szükséges

- feladatokat, lépéseket,
- erőforrásokat, melyek lehetnek
    - technológiai erőforrás, eszköz,
    - humán erőforrás,
    - pénzeszközök, költségvetés,
- felelősöket,
- határidőket, mérföldköveket, valamint
- ütemezést, projekttervet.

Mindezek pontos meghatározásához elengedhetetlen egy gap analízis, eltérés elemzés készítése, mely teljes mélységében felfedi, hogy a stratégiában definiált célok eléréséhez mi áll jelenleg rendelkezésre (eszközök, erőforrások, szabályzatok), milyen hiányosságok és eltérések vannak, melyeket pótolni, módosítani, fejleszteni kell annak érdekében, hogy a célok megvalósíthatóak legyenek. Ezen eltérésekre, hiányosságokra kell a részleteiben lebontott tervet kidolgozni.

A gap analízis elkészítésének több módszere is lehet (például a korábbiakban is bemutatott CMM megközelítés), legtöbbjük a következő területek értékelésével tárja fel az eltéréseket (CISM Review Manual, 2014):

- az információbiztonsági stratégiát a felső vezetés elfogadja és támogatja
- az információbiztonsági stratégia egyértelműen összekapcsolható az üzleti célokkal
- az információbiztonsági szabályzatok teljesek, és összhangban vannak a stratégiával
- a szabályzati környezet karbantartására megfelelő szabványok, eljárások állnak rendelkezésre
- a folyamatok teljesek és dokumentáltak
- a feladatok és felelősségek pontosan, egyértelműen definiáltak
- a szervezeti struktúra támogatja az információbiztonsági irányítási rendszer működését, menedzsmentjét, a belső konfliktusok kezelése biztosított
- az információs vagyon felmérésre került, az adatvagyon elemek biztonsági osztályba sorolása megtörtént

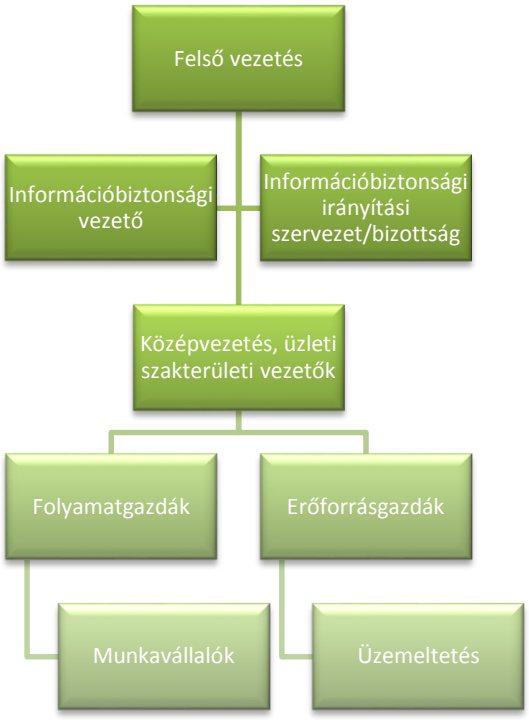
- hatékony kontrollok kerültek kialakításra, bevezetésre, és rendszeres karbantartásuk biztosított
- hatékony visszamérési, monitorozási folyamat került kialakításra, megfelelő mutatószámok kerültek definiálásra
- a megfelelőséget biztosító és a szankciókat definiáló folyamatok megfelelően kerültek kialakításra
- az üzletfolytonossági és a katasztrófa-elhárítási tervek megfelelően kerültek kialakításra és tesztelésre
- a változáskezelés folyamatában az információbiztonsági jóváhagyások megfelelően megtörténnek
- hatékony kockázatmenedzsment, a kockázatok azonosításra, értékelésre, kommunikálásra és kezelésre kerültek
- minden felhasználó a számára megfelelő mélységű és releváns információkat tartalmazó információbiztonsági oktatáson, biztonságtudatossági tréningen vesz részt rendszeresen
- a rendszer vagy szolgáltatás fejlesztések, megrendelések, bevezetések információbiztonsági szemlélete fokozódik
- az információbiztonsági szemlélet a szervezeti kultúra részévé válik, minden munkavállaló érdekelt lesz a támogatásában
- a kapcsolódó törvényi és jogszabályi előírások megfelelően értelmezettek és alkalmazottak
- az információbiztonsági követelmények a külső partnerekre, kiszervezett szolgáltatásokra is kikényszerítésre kerülnek
- a nem-megfelelőségek, eltérések, incidensek időben észlelésre, azonosításra és kezelésre kerülnek

Az azonosított eltérések, hiányosságok feltárása után célirányos tervek kerülnek kialakításra, melyek az adott terület fejlesztésének módját és eszközeit határozzák meg a korábban leírt tartalmat definiálva.

2. Az információbiztonság szervezeti felépítése

A stratégiában foglalt célok, illetve az azok alapján meghatározott intézkedési tervek megvalósítása csak abban az esetben valósul meg hatékonyan, amennyiben a szervezeti felépítés, a felső- és középvezetői szint megfelelően támogatja az információbiztonsági irányítási rendszer működését.

Ennek biztosítása érdekében minden szervezetnél meg kell határozni az információbiztonság szervezetét. Ennek felépítése szervezetenként eltérő, a szervezet jellege, működése jelentős mértékben befolyásolja ennek felállítását, ezért minden szervezetnek saját magára testre kell szabnia és meg kell határoznia az információbiztonság szervezetének felépítését. Példaként egy általános sémát azonban következő ábra szemléletet:



Az információbiztonsági irányítási szervezet általános felépítése

Természetesen a fent definiált pozíciók és csoportok megnevezései is szervezetenként eltérőek lehetnek.

A következőkben ezen példa mentén végighaladva kerülnek bemutatásra az egyes résztvevők feladatai és felelősségei, döntési és javaslattételi hatáskörül az információbiztonsági irányítási rendszer vonatkozásában.

Felső vezetés

Mivel az információbiztonsági irányítási rendszer menedzselése a szervezet irányításának részét képezi, ennek stratégiai irányítása szintén a felső vezetés hatáskörébe tartozik. A felső vezetés felelőssége annak biztosítása, hogy az információbiztonsági kockázatok felmérése és kezelése megfelelően megtörténjen, a maradványkockázatok elfogadásra kerüljenek, a stratégia kialakítása és elfogadása megtörténjen, valamint a vállalati információk és erőforrások megfelelően és felelősségteljesen kerüljenek felhasználásra, továbbá az információbiztonsági irányítási rendszer az egész szervezetre vonatkozóan kiterjesztésre kerüljön és minden felhasználói réteg érintett legyen – a rá szabott mértékben - az információbiztonsági rendszer működtetésében. A vezetőség felelőssége a rendszer megfelelő és hatékony működtetése, az információbiztonsági intézkedésekkel kapcsolatos stratégiai döntéshozatal, illetve a szükséges engedélyek, jóváhagyások megtétele.

A felső vezetés szerepe és feladata az információbiztonság támogatásában a következő (CISM Review Manual, 2014):

- Információbiztonsági stratégia és szabályzatok kialakításának támogatása, az elkészült dokumentumok jóváhagyása, elfogadása.
- Védelmi intézkedések kialakításának támogatása, a szükséges erőforrások és hatáskörök biztosítása az információbiztonsági rendszer kialakításához, kontrollok bevezetéséhez és működtetéséhez.
- A szakterületi vezetők, folyamatgazdák tájékoztatása az információbiztonság fontosságáról, az őket érintő ezzel kapcsolatos feladatokról és felelősségekről, kritikus üzleti folyamatok felmérésének, meghatározásának támogatása.
- Az üzleti célok és az információbiztonság összehangolása, a biztonság integrálása a működési folyamatokba, mely megvalósításának egyik eleme, hogy a felsővezetői értekezleten rendszeres napirendi pont az információbiztonság kérdésköre, az információbiztonsági irányítási rendszer működése is.
- Az információbiztonsági szabályzatokban foglaltak betartatása, illetve betartásának ellenőrzése, a szabályzatokban foglaltaknak megfelelő működés folyamatos monitorozása.
- Az információbiztonsági irányítási rendszer magas szintű átlátása és kontrollálása.
- Az egész szervezetre vonatkozó, annak minden munkavállalóját érintő biztonságtudatossági oktatás, program végrehajtásának támogatása.

- Az információbiztonsági szemlélet fokozása, a szervezeti kultúrába történő illesztésében való közreműködés. Ennek legjobb módja a példamutatás a szabályzatokban foglalt eljárások betartásához.

Annak érdekében, hogy a felső vezetés felismerje az információbiztonsági rendszer működtetésének fontosságát, az ezzel kapcsolatos feladatait és felelősségeit, megfelelően megalapozott döntéseket hozzon a stratégiaalkotás és megvalósítás során, hatékonyan kommunikálja az érintettek felé a célokat és az ezzel kapcsolatos kötelezettségeiket, illetve támogassa az információbiztonsági kontrollok és védelmi intézkedések működtetését, valamint hozzáigazítsa az információbiztonsági követelményeket az üzleti célokhoz, a rendszer bevezetése előtt elengedhetetlen egy menedzsment szintű, vezetői fókuszú oktatás.

Az információbiztonsági és üzleti célok összehangolásához, stratégiaalkotáshoz és döntéshozatalhoz elengedhetetlen a következők ismerete (CISM Review Manual, 2014):

- Információbiztonsági szabályok és eljárások megértése, üzleti célokhoz való kapcsolódási pontjainak azonosítása.
- Információbiztonsággal kapcsolatos törvényi kötelezettségek azonosítása, azoknak való megfelelés biztosítása.
- Költségvetés meghatározása, információbiztonsági program költségelemeinek azonosítása.
- Költség-haszon elemzés (például TCO, ROI alapján).
- Mutatók meghatározása az információbiztonsági irányítási rendszer működési hatékonyságának monitorozására, eltérések, nem-megfelelőségek észlelésére.
- Rendszeres felülvizsgálatok, külső/belső auditok eredményei.

A felső vezetés közreműködése és támogatása nélkül az információbiztonsági irányítási rendszer nem, vagy nem teljes körűen, kevésbé hatékonyan épül be a szervezeti struktúrába, mely által kevesebb a valószínűsége annak is, hogy eléri az információbiztonsági stratégiában kitűzött célokat.

Információbiztonsági irányítási szervezet/bizottság

A felső vezetés támogatására célszerű létrehozni egy, az információbiztonsági irányítási rendszer irányításával megbízott szervezeti egységet, bizottságot. Ezen szervezet tagjai a felső vezetésen kívül jellemzően az érintett középvezetők, az információbiztonsági vezető, illetve egyéb, bevonásra indokolt személyek. Feladatai közé tartozik, hogy kialakítja az információbiztonsági stratégiát, és támogatja az információbiztonság elemeinek,

szemléletének üzleti folyamatokba integrálását. Ezen feladatok közé tartozik továbbá a védelmi intézkedések bevezetésének, kontrollok kialakításának és megfelelő működésének támogatása, valamint szervezettől függően a döntés vagy az ahhoz szükséges javaslattétel biztosítása.

Információbiztonsági vezető

Mivel az információbiztonság irányításának hatékony megvalósítása és a stratégiai célok meghatározása összetett feladat, ezért mindenképpen megfelelő vezetőt, az irányításáért felelős személyt igényel. A tapasztalatok alapján információbiztonsági vezető minden szervezet esetében van, azonban nem mindenhol kerül definiáltan kijelölése, illetve nem mindenhol viseli ez a címet. Általában az informatikai igazgató vagy a biztonsági igazgató van kinevezve, mint információbiztonsági vezető, de megkaphatja ezt a címet az operatív igazgató, vagy akár a vezérigazgató is. Akár definiálásra kerül az információbiztonsági vezető (CISO, Chief Information Security Officer) szerepköre, illetve betöltésre kerül a pozíciója, akár nem, az információbiztonsági irányítási rendszerrel kapcsolatos feladatok irányításával és felelősségével valakit fel kell ruházni.

Amennyiben az információbiztonsági vezető szerepe önálló pozícióként kerül betöltésre, nagyon fontos a megfelelő riportolási kötelezettségek meghatározása – célszerű ezért, ha közvetlenül a vezérigazgató, vagy a felső vezetés alá tartozik, ezáltal elkerülhető ugyanis az ellentétes érdekek és felelősségek ütközése.

Az információbiztonsági vezető feladatai és felelőssége az információbiztonsági irányítási rendszer működtetése során (CISM Review Manual, 2014):

- Információbiztonsági terület irányítása, információbiztonsági folyamatok koordinálása.
- Az információbiztonsági stratégia összeállításának koordinálása, üzleti és működési folyamatokkal történő összehangolása.
- Információbiztonsági projektek vezetése, felügyelete.
- Javaslattétel, illetve bizonyos mértékben döntési jog gyakorlása információbiztonsági kérdésekben.
- Felső vezetés támogatása, javaslattétel az információbiztonságot érintő kérdésekben.
- Koordináció az üzleti hatáselemzés elkészítésében, a folyamatfelmérés és adatvagyonleltár interjúk lefolytatásában.

- Támogatás az üzleti folyamat kritikussági besorolásának megállapításában, jóváhagyásában.
- Kockázatelemzés elkészítése, koordinálása.
- Védelmi intézkedések kialakításának, kontrollok bevezetésének irányítása, folyamatos működésük, fenntartásuk koordinálása.
- Rendszeres külső és belső auditok, a felülvizsgálatok lefolytatása, támogatása.
- Az információbiztonsági irányítási rendszer működésének monitorozása, hatékonyságának mérése, rendszeres riportok készítése a felső vezetés és az információbiztonsági irányítási szervezet/bizottság számára.
- Minden munkavállaló biztonságtudatossági oktatásának biztosítása.
- A biztonsági követelmények kommunikálása és az információbiztonsági szemlélet fokozása a szervezeten belül.
- Információbiztonsági incidensek kezelésének, kivizsgálásának koordinálása, szankciók alkalmazása.

Folyamatgazdák

A folyamatgazdák az általuk irányított üzleti vagy működési folyamat(ok) felelősei. Általában a szakterületi vezetők, vagy a szakterületi vezetők által kijelölt személyek. Az ő felelősségük, hogy az üzleti folyamatok megfelelően kerüljenek üzleti hatás szempontjából priorizálásra, valamint támogassák a kritikus kockázati besorolású folyamatokhoz kapcsolódó védelmi intézkedések, kontrollok bevezetését, fenntartását, illetve hatékony működését, fejlesztését. Mindezek biztosítása érdekében kiemelten fontos, hogy a folyamatgazdák azonosulni tudjanak az információbiztonsági követelményekkel, felismerjék azok fontosságát és előnyeit. Ennek elérésére a legmegfelelőbb egy, a folyamatgazdák igényeire és előismereteire épülő biztonságtudatossági oktatás, valamint az információbiztonsági rendszer egyéb elemeihez kapcsolódó specializált oktatások (például üzletfolytonossági rendszer oktatása).

A folyamatgazdák felelőssége és feladata az információbiztonsági rendszer kialakítása és működtetése során:

- Közreműködés az üzleti hatáselemzés elkészítésében, a folyamatfelmérés és adatvagyonleltár interjúk lefolytatásában.
- Üzleti folyamat kritikussági besorolásának megállapításában, jóváhagyásában való közreműködés, folyamatra vonatkozó kockázatelemzés eredményének jóváhagyása, maradványkockázatok folyamatgazda szintű elfogadása.

- Folyamatra vonatkozó védelmi intézkedések kialakításának, kontrollok bevezetésének aktív támogatása, folyamatos működésükben, fenntartásukban való közreműködés.
- Rendszeres külső és belső auditokon a felülvizsgálatokban, tesztelésben való aktív közreműködés.
- Az információbiztonsági rendszerrel kapcsolatos, észlelt nem-megfelelőségek, fejlesztési lehetőségek jelentése az információbiztonsági vezető felé.
- A hozzájuk tartozó munkatársak biztonságtudatossági oktatásának támogatása, a biztonsági követelmények kommunikálása és az információbiztonsági szemlélet fokozása a csoportjukon belül.

Erőforrásgazdák

Az erőforrásgazdák az üzleti vagy működési folyamatokat támogató erőforrások üzemeltetésének felelősei, akik biztosítják azok megfelelő működését és az igényeknek megfelelő, folyamatos rendelkezésre állását.

A támogató erőforrások lehetnek:

- IT erőforrás, rendszer (például munkaállomás, vállalatirányítási rendszer)
- Infrastruktúra (például irodahelyiség 5 fő részére)
- Humán erőforrás (például az előre meghatározott kompetenciákkal rendelkező ügyintéző)
- Egyéb erőforrás (például speciális eszköz)
- Külső szolgáltató (például távközlési szolgáltató)

Az erőforrásgazdák felelőssége és feladata az információbiztonsági rendszer kialakítása és működtetése során:

- Közreműködés a kockázatelemzés elkészítésében, a támogató kritikus erőforrások azonosításában.
- Az erőforrásokra vonatkozó védelmi intézkedések kialakításában, karbantartásában való aktív közreműködés, az üzleti terület által meghatározott rendelkezésre állási idő és minőség megvalósításának biztosítása.
- Rendszeres külső és belső auditokon a felülvizsgálatokban, tesztelésben való aktív közreműködés.

- Az információbiztonsági rendszerrel és az érintett erőforrásokkal kapcsolatos észlelt nem-megfelelőségek, fejlesztési lehetőségek jelentése az információbiztonsági vezető felé.
- Az üzemeltetési munkatársak biztonságtudatossági oktatásának támogatása, a biztonsági követelmények kommunikálása és az információbiztonsági szemlélet fokozása a csoportjukon belül.

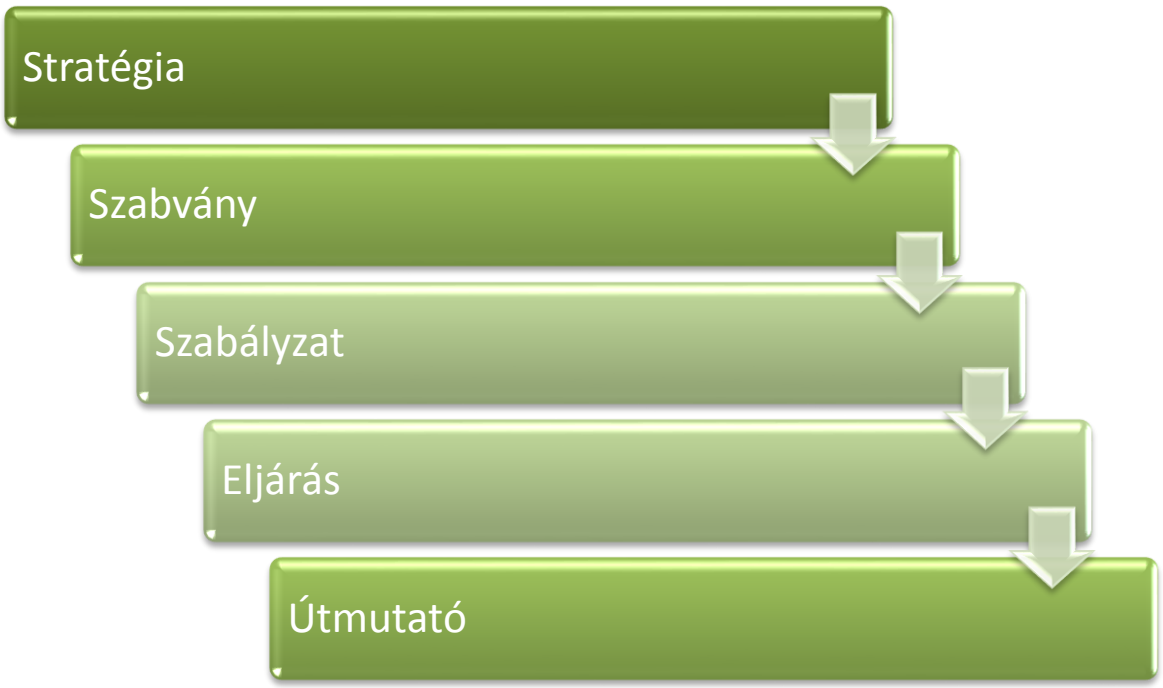
Munkavállalók

Az információbiztonsági irányítási rendszer megfelelő működtetésében minden munkavállalónak közre kell működnie, és a saját felhasználói szintjén hozzá kell járulnia az információbiztonsági rendszer hatékony működéséhez.
A munkavállaló feladatai és felelősségei az információbiztonsági irányítási rendszerrel kapcsolatban:

- Rendszeres időközönként részvétel biztonságtudatossági oktatásokon, tréningeken, valamint új munkaerő esetben a munkába álláskor.
- Szabályzatokban foglaltak megismerése és betartása, napi munkavégzésbe történő beépítése.
- Biztonságtudatos magatartás tanúsítása és más munkavállalók ösztönzése ennek követésére.
- Biztonsági incidensek jelentése a szabályzatokban meghatározottaknak megfelelően.
- Az információbiztonsági rendszerrel kapcsolatban észlelt nem-megfelelőségek, fejlesztési lehetőségek jelentése az információbiztonsági vezető felé.
- A felső vezetés a folyamatgazdák, valamint az információbiztonsági vezető támogatása az információbiztonsági rendszer kialakítása, működtetése során.

3. Szabályzati környezet

Az információbiztonsági irányítási rendszer működtetésének, az információbiztonsági folyamatok irányításának elsődleges elemei a szabályzatok, illetve szabványok, valamint egyéb kapcsolódó, alacsonyabb szintű szabályozó dokumentumok.



Az információbiztonsági irányítási rendszer szabályzati környezetének hierarchiája

Szabvány

A szabványok külső felek, szervezetek által alkotott és kiadott, az adott szakterületre vonatkozó követelményeket meghatározó dokumentumok. Alkalmazásuk az információbiztonsági irányítási rendszer kialakítása s működtetése során nem követelmény, viszont a szabvány alapján a rendszer tanúsítható, mely üzleti előnyt is jelent a szervezet részére. Az információbiztonsági irányítási rendszer esetében az ISO/IEC 27001:2013 a vonatkozó szabvány, mely az információbiztonsági irányítási rendszer kialakításával és működtetésével kapcsolatban határoz meg követelményeket.

A szabvány alkalmazásának előnyei:

- az információbiztonsági irányítási rendszer kialakításának menedzsment eszköze
- meghatározza a rendszer kereteit
- elősegíti a szabályzati környezet kialakítását és védelmi intézkedések, kontrollok definiálását
- támogatja a rendszer folyamatos karbantartását
- biztosítja a monitorozást és visszamérést, a megfelelőség nyomon követését
- lehetővé teszi a külső fél általi auditálást, tanúsítvány megszerzését.

Szabályzat

A szabályzatok magas szintű dokumentumok, melyek definiálják

- a szabályzat célját, hatályát,
- az információbiztonsági követelményeket,
- alkalmazott kontrollokat, védelmi intézkedéseket,
- eljárásokat, utasításokat a követelmények teljesítéséhez,
- megfelelőségi kritériumokat és mutatókat,
- be nem tartásuk következményeit, lehetséges szankciókat.

Például az információbiztonsági szabályzat tartalmazza a biztonsági mentések elkészítésének követelményeit (gyakoriság, mentési mód, mentések tárolása, stb.), azonban nem írja le azok elkészítésének részletes lépéseit.

Információbiztonsági szempontból több releváns szabályzatot is megkülönböztethetünk, melyek készülhetnek egy szabályzatban, vagy akár – amennyiben célszerű - külön dokumentumokban is. Ilyenek például:

- Információbiztonsági szabályzat
- Informatikai felhasználói szabályzat
- Vírusvédelmi szabályzat
- Üzletfolytonossági szabályzat
- Mobil eszközök használatának szabályzata
- Közösségi média alkalmazásának szabályzata

A szabályzatokat a szervezet sajátosságainak, igényeinek megfelelően, más területek, funkciók szabályozó dokumentumaival összhangban kell kialakítani, tárolni, kommunikálni.

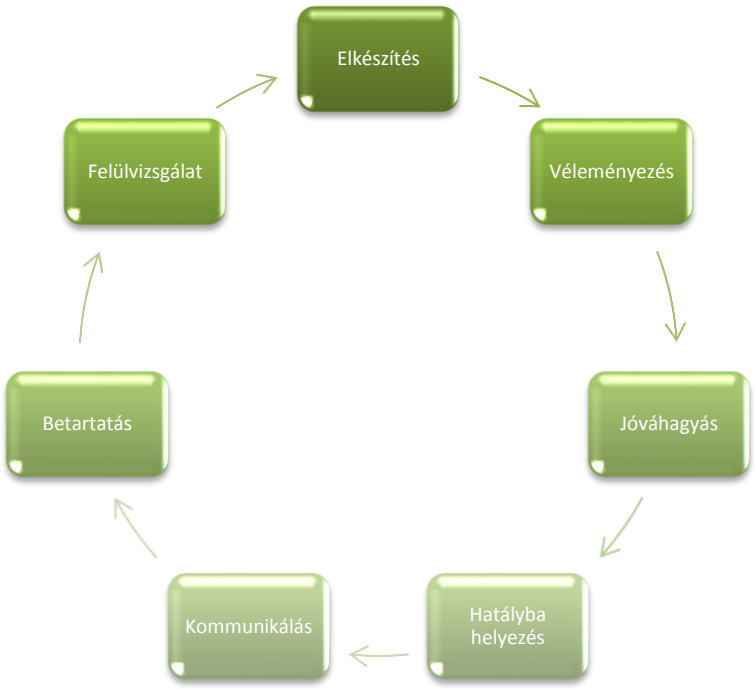
A szabályzatokat a stratégiában megfogalmazottaknak, illetve az alkalmazott szabványban leírtaknak megfelelően kell kialakítani, illetve amennyiben már rendelkezésre állnak, felülvizsgálni, kiegészíteni, módosítani. Tartalmilag egyértelműnek, közvetlenül lekövethetőnek kell lenniük benne a stratégia elemeinek.

Ugyan a szabványok és ajánlások szerint a szabályzatokat a stratégiaalkotást követően, a stratégia jóváhagyása után célszerű kialakítani, a gyakorlati életben azonban ez többnyire nem valósul meg, általában a szabályozó dokumentumok hamarabb előállításra kerülnek, mint a stratégia definiálása, illetve olyan eset is előfordul, hogy a szervezet egyáltalán nem készít stratégiát, és a szabályzatai is pusztán a „fióknak” készülnek, a valós folyamatokkal, eljárásokkal nincsenek összhangban.

A szabályzatok elkészítésével kapcsolatos követelmények (Stackpole, Oksendahl; 2010):

- stratégiában meghatározott célokat szolgálja
- célirányos, pontos
- naprakész, releváns
- könnyen értelmezhető
- egyértelműen megfogalmazott
- teljesíthető követelményeket tartalmaz
- következetes
- ellenőrizhető, visszamérhető

A szabályzatok kiadásának és karbantartásának folyamata a következő:



Szabályzatok életciklusa

A szabályzatok kialakítása, elkészítése az információbiztonsági szakterület és a kapcsolódó szakterületek (például üzemeltetés, fizikai biztonság, humánbiztonság, egyéb területek) feladata az információbiztonsági vezető koordinálása, felügyelete mellett. Az elkészült szabályzatokat az információbiztonsági vezető, illetve a kijelölt szakterületi munkatársak (például az érintett szakterületek vezetői, minőségügy, jogi szakterület) véleményezik. A véleményezés alapján a szabályzatok módosításra kerülnek, illetve elfogadás esetén a felső vezetés dönt azok jóváhagyásáról és hatályba helyezéséről. A szabályzatokat a szervezetnél alkalmazott fórumokon kommunikálni kell az érintettek felé, valamint biztosítani kell azok elérhetőségét. Az érintettek körét aszerint, hogy milyen mélységben kell, illetve lehet

megismerniük a szabályzat tartalmát, célcsoportokra kell bontani. Ilyen célcsoportok lehetnek például:

- felső vezetés, menedzsment
- érintett szakterületek munkavállalói
- csak a szabályzatban foglaltak operatív végrehajtásáért felelős személyek
- minden munkavállaló

A szabályzatok kommunikálásának módszerei az alábbiak lehetnek:

- oktatás
- tájékoztató előadás
- elektronikus levél, hírlevél
- e-learning bemutató
- ezek kombinációja

A szabályzatok tárolása történhet:

- papír alapon
- elektronikus dokumentumként a fájlszerveren
- dokumentum kezelő rendszerben
- intratnetes felületen
- ezek kombinációjaként

A szabályzatok kommunikálása után gondoskodni kell az azokban foglaltak teljesüléséről (például amennyiben egy eszközre vonatkozó előírás szerepel benne, annak teljesülését biztosítani és rendszeresen visszaellenőrizni kell), a szabályok munkavállalók általi betartásáról (adminisztratív intézkedések rendszeres ellenőrzése). Ezen ellenőrzések külső és/vagy belső rendszeres auditok keretein belül történnek meg. Amennyiben a szabályzatok alkalmazásának ellenőrzése során eltérés, hiányosság tapasztalható, annak kivizsgálása az információbiztonsági vezető felelőssége.

A szabályzatokat rendszeres időközönként, legalább évente felül kell vizsgálni, és a felülvizsgálat eredményének megfelelően módosítani, fejleszteni kell. Amennyiben a szervezet életében valamilyen, a szabályzatot érintő változás (például szervezeti változás, incidens, alkalmazott eszközök, technológia változása) következik be, az érintett dokumentumokat soron kívül felül kell vizsgálni, és a változásoknak megfelelően átalakítani, bővíteni.

Eljárás

A szabályzatoknál alacsonyabb szintű, részletesebb dokumentumok, melyek egy adott folyamat leírását dokumentálják. Definiálják az egyes lépéseket, az azokhoz szükséges erőforrásokat és feltételeket, meghatározzák a folyamat várt kimenetelét, valamint az esetleges nem várt eredmények előfordulása esetén végrehajtandó lépéseket. Az eljárások a kapcsolódó követelményeket tartalmazó szabályzattal összhangban kell, hogy kialakításra kerüljenek.

Az előző példánál maradva, eljárás lehet a biztonsági mentések elkészítésének folyamatleírása, mely részletesen, lépésenként leírja a mentések végrehajtását.

Útmutató

Az útmutatók nem szabályozó jellegű dokumentumok, hanem javaslatokat tartalmazó leírások. Ajánlásokat, legjobb gyakorlatokat mutatnak be az egyes információbiztonsági folyamatok kialakításához, melyek különösen hasznos segítséget nyújtanak a különböző eljárások, szabályzatok elkészítéséhez. Tartalmazhatnak példákat, háttér információkat, alkalmazható eszközök bemutatását.

A biztonsági mentések eseténél maradva ilyen útmutató lehet az egyes mentőeszközök dokumentációja, leírása.

4. Védelmi intézkedések

A védelmi intézkedések és kontrollok olyan eszközök, melyek egy adott információbiztonsági kockázat bekövetkezési gyakoriságát vagy hatását csökkentik célirányosan. Ezeket az információbiztonsági stratégiából, illetve a kapcsolódó szabályzatokból kell célirányosan levezetni és kialakítani. A védelmi intézkedések bevezetése jellemzően alacsonyabb szintű tervek alapján, általában éves szintre lebontva, külső vagy belső projektek megvalósítása során történik.

Megkülönböztethetünk informatikai és nem informatikai védelmi intézkedéseket, jellegük alapján pedig három fő csoportba sorolhatjuk a kontrollokat:

- fizikai
- technológiai
- adminisztratív

Természetesen ezeket egymással összehangoltan és átfedően célszerű kialakítani (például a megfelelő jelszavak megválasztásának az alkalmazott rendszeren keresztüli kikényszerítése, mint technológiai védelmi intézkedés mellett szükséges bevezetni olyan adminisztratív jellegű kontrollt is, mint annak szabályzatban történő előírása, hogy a felhasználók nem oszthatják meg a jelszavukat egymással, nem írhatják fel és tárolhatják mások által hozzáférhető helyen). A védelmi intézkedések tervezésénél a maximális biztonság elérése érdekében törekedni kell a többszintű védelem kialakítására, vagyis az egyes védelmi intézkedéseket egymásra építve, úgy kell tervezni, hogy az egyik kontroll sérülése, meghibásodása esetén a következő réteg még megfelelő védelmet nyújtson. (Például, amennyiben a beléptető rendszer meghibásodik, a biztonsági őrök át tudják venni annak szerepét, és ellenőrizni tudják a belépők jogosultságát, megakadályozva ezzel, hogy illetéktelen személyek jussanak be az épületbe, valamint a kritikus helyiségek mechanikus zárral, vagy más jellegű beléptető rendszerrel védettek, így csak külön belépési jogosultsággal lehetséges a belépés.) A védelmi intézkedések szintjeinek számát, mélységét a védendő értékek függvényében kell meghatározni.

Néhány példa lehetséges védelmi intézkedésekre:

- Fizikai biztonság
    - Létesítmény biztonsággal kapcsolatos követelmények:
        - Külső és környezeti fenyegetésekkel szembeni védelem (tűzjelző, elárasztás érzékelő, stb.)
        - Áramkimaradás elleni védelem (generátor, szünetmentes tápellátás biztosítása)
        - Kábelezés biztonsága
        - Biztosítások
    - Fizikai biztonsági zónák meghatározása, és azok biztonsági szintjének megfelelő védelmi intézkedések alkalmazása:
        - Élőerős őrzés-védelem
        - Fizikai hozzáférési kontrollok: beléptető rendszer, zárak, jogosultságok, behatolás érzékelő rendszer alkalmazása
        - Munkakörnyezet biztonsága
        - Külső és környezeti fenyegetésekkel szembeni védelem (Például tűzjelző, elárasztás érzékelő)
        - Nyilvános terek (például tárgyaló biztosítása és kontrolljai)
    - Bevezetett kontrollok és folyamatok dokumentálása
    - Bevezetett kontrollok rendszeres karbantartása és időszakos felülvizsgálata

- Hozzáférés menedzsment
    - Szerepkörök és jogosultságok meghatározása
    - Feladatok elhatárolása
    - Jogosultságok kezelése (felhasználó regisztrálása, jogosultság igénylés, kiadás, módosítás, visszavonás)
    - Hozzáférési jogosultságok rendszeres felülvizsgálata
    - Külső félnek kiadott jogosultságok kezelése (például automatikus lejárat)
    - Kiemelt felhasználók kezelése
    - IDM, jogosultságkezelő rendszer alkalmazásának lehetőségei
    - Jelszókezelés, jelszóhasználattal kapcsolatos követelmények és kontrollok (például biztonságos jelszavak kikényszerítése, lejárat, sikertelen kísérlet utáni zárolás)
    - Tiszta asztal, tiszta képernyő politika
    - Hozzáférés-védelemmel kapcsolatos biztonsági előírások, felhasználók biztonságtudatossági oktatása
- Humán erőforrás biztonsága
    - Felelősségek és szerepkörök rögzítése, szerepkörök szétválasztása
    - Alkalmazottak felvételének követelményei, előzetes ellenőrzések
    - Alkalmazottak elbocsátásakor vagy munkakör változásakor alkalmazott kontrollok, hozzáférési jogosultságok visszavonásával és eszközök visszavételével kapcsolatos követelmények
    - Külső felek, alvállalkozók kezelésére vonatkozó eljárások
    - Titoktartási kötelezettségek
    - Tűz- és munkavédelmi, valamint biztonságtudatossági oktatások, képzések biztosítása
    - Humán erőforrással kapcsolatos kontrollok és folyamatok dokumentálása
    - Bevezetett kontrollok rendszeres felülvizsgálata, oktatásokon elhangzottak visszamérése
- Hálózatbiztonság
    - Alkalmazott hálózati eszközök megfelelő konfigurálása
    - Tűzfalszabályok kezelése
    - Hálózat szegmentálása
    - WiFi hálózatok biztonsága
    - Monitorozás

- Vírusvédelem
    - Vírusvédelmi rendszer üzemeletetése és naprakészen tartása
    - Vírusvédelmi szabályzat
    - Felhasználók biztonságtudatosságának, vírusvédelmi ismereteinek bővítése
    - Egyéb alkalmazható védelmi intézkedések bevezetése (például USB portok letiltása, csak a szervezet tulajdonát képező külső adattárolók csatlakoztatásának engedélyezése, bizonyos weboldalak letiltása)
- Távoli elérés, külső helyszínről történő munkavégzés
    - Megfelelően biztonságos VPN kapcsolaton keresztül történő távoli elérés biztosítása a Szervezet által rendelkezésre bocsátott, a Szervezet által meghatározott eszközökkel.
    - Fizikai biztonsági követelmények rögzítése a külső helyszínre vonatkozóan (például notebook zár használata kötelező, autóban nem hagyható őrizetlenül laptop)
    - Távoli elérés jogosultságok kezelése (ideiglenes vagy állandó jogosultság)
    - Felhasználók biztonságtudatosságának növelése.
- Rendszerfejlesztés, üzemeltetés biztonsága
    - Üzemeltetési szabályzatok, eljárások dokumentálása és karbantartása
    - Szerverek és munkaállomások biztonsági beállításai, megfelelő konfigurálása
    - Változásmenedzsment, módosítások kezelése
    - Kiszervezett szoftverfejlesztés, karbantartás biztonsági követelményei, monitorozása és felügyelete
    - Alkalmazott rendszerek biztonsági auditja, technológiai sérülékenység vizsgálata
    - Érzékeny adatokat kezelő rendszerek izolálása, elhatárolása
    - Éles és teszt környezet elkülönítése, tesztelési előírások és biztonsági követelmények
    - Megfelelő gyakoriságú és típusú biztonsági mentések készítése, biztonsági mentések tárolásárának követelményei
    - Naplózási követelmények
    - Titkosítási követelmények, kulcskezelés
    - Elektronikus levelezés biztonsága, spamszűrés
    - Biztonságos megsemmisítés
    - Adathordozók újrafelhasználása, selejtezése

    - Hordozható eszközök (laptopok, okostelefonok, mobil adattárolók) biztonsági követelményei, beállításai
    - Biztonsági események kezelése: incidensek jelentése, problémamegoldás, HelpDesk tevékenység
- Üzletfolytonossági tervezés
    - Üzleti hatáselemzés készítése, kritikus folyamatok, az azokat támogató kritikus erőforrások és megengedett maximális kiesési idejük meghatározása.
    - Kritikus folyamatok kiesésének áthidalására szolgáló üzletfolytonossági akciótervek. (BCP dokumentáció)
    - Kritikus erőforrások helyreállítására vonatkozó akciótervek. (DRP dokumentáció)
    - Akciótervek tesztelésére vonatkozó előírások, követelmények meghatározása, tesztelés végrehajtása, RTO és RPO teljesülésének ellenőrzése.
    - Akciótervek oktatására vonatkozó előírások, követelmények meghatározása, oktatás megvalósítása.
    - Üzletfolytonossági tervezés rendszeres karbantartásának, felülvizsgálatának követelményei és gyakorisága.

Az információbiztonsági irányítási rendszer működtetése során cél a stratégiában és a tervekben meghatározott védelmi intézkedések és kontrollok bevezetésének koordinálása és támogatása, működtetésük és rendszeres karbantartásuk biztosítása, folyamatos felügyelete. Ennek érdekében az információbiztonsági intézkedések megfelelő működését és működési hatékonyságát folyamatosan monitorozni, ellenőrizni kell, hogy nem-megfelelőség esetén azonnal be lehessen avatkozni a működésbe. A monitorozási és mérési lehetőségek bemutatását a „*Visszamérés, ellenőrzés*” fejezet tartalmazza.

5. Információbiztonsági szemlélet

Az információbiztonsági irányítási rendszer működésének és a stratégia megvalósításának alapfeltétele, hogy az információbiztonsági szemlélet beépüljön a szervezeti kultúrába, és minden munkatárs – felelősségének megfelelően – megismerje a rá vonatkozó, ezzel kapcsolatos feladatokat, és az információbiztonsági követelményeket be tudja építeni és alkalmazni tudja a napi munkavégzése során.

Az információbiztonsági szemlélet fokozásának legalkalmasabb módszere az információbiztonsági oktatás, illetve a biztonságtudatossági tréning. Az oktatás során a résztvevők

- átlátják az információbiztonsági irányítási rendszer céljait,
- felismerik az információbiztonsági rendszerben betöltött szerepüket, helyüket,
- azonosítani tudják az információbiztonsággal kapcsolatos feladataikat,
- megismerik a rájuk vonatkozó szabályzatokat és azok tartalmát,
- megismerik a lehetséges kárkövetkezményeket, szankciókat,
- megismerik az őket érintő fenyegetéseket, veszélyeket,
- elsajátítják a fenyegetésekkel szembeni védekezés lehetőségeit, a kapcsolódó védelmi intézkedések működését,
- megismerik a jelentésköteles biztonsági eseményeket (például incidensek jelentése, nem-megfelelőségek azonosítása),
- az elsajátított ismereteket be tudják építeni napi munkavégzésükbe.

Az oktatás lebonyolítását legalább éves rendszerességgel célszerű megtartani minden munkavállaló részére. Lebonyolítása történhet tantermi keretek között, előadás vagy workshop formájában – a tapasztalatok alapján ez a leghatékonyabb módszer – de akár e-learning rendszeren, vagy hírlevélen keresztül (utóbbi kettő inkább ismétlő jellegű oktatás során alkalmazandó megoldás).

A tananyag összeállításakor fontos, hogy minden esetben a célközönségnek, különböző, előre meghatározott csoportok igényeinek és előismereteinek (például felső vezetés, üzemeltetés ügyfélszolgálat) megfelelően kerüljön összeállításra.

Az oktatás eredménye a tapasztalatok alapján:

- szemléletváltás, az információbiztonság nem teher, hanem a felhasználók saját érdeke
- a kapcsolódó védelmi intézkedések működési hatékonysága nő
- nő a bejelentett biztonsági incidensek, illetve észrevételek száma
- hatékonyabb a változások bejelentése
- kevesebb felesleges szankcionálás válik szükségessé
- az információbiztonsági területtel szemben nő a bizalom
- az információbiztonsági irányítási rendszer támogatottsága nő
- az információbiztonsági és az üzleti célok összehangolása hatékonyabb

6. A stratégia megvalósításának lehetséges buktatói

Az információbiztonsági irányítási rendszer abban az esetben működik megfelelően, ha a stratégiában foglaltakat sikeresen teljesíteni tudja, eléri az abban kitűzött biztonsági célokat. A stratégia kialakításának és megvalósításának azonban vannak olyan „csapdái", melyekbe beleesve fennáll annak a lehetősége is, hogy a stratégia megvalósítása sikertelen eredménnyel zárul. A stratégia megvalósításának ezen buktatói a következők lehetnek (CISM Review Manual, 2014):

- **Túlzott bizalom:** a legtöbben vonakodnak attól, hogy a lehetséges kimenetelek széles tartományát határozzák meg, és inkább előnyben részesítik a pontos, de rossz stratégiát, mint a bizonytalan, de helyes becsléseket, illetve túlságosan bíznak a saját képességeikben.
- **Optimizmus:** az előző pontban bemutatott túlzott magabiztosság optimizmussal kiegészülve katasztrofális hatással is bírhat a stratégiai becslésekre.
- **Lehorgonyzás:** gyakori probléma az első megállapítás, becslés melletti kitartás. Főleg abban az esetben, ha a becslés korábbi, régebbi tapasztalatokon alapul és nem veszi figyelembe a változásokat.
- **Elfogultság:** amikor a stratégia alkotók olyan ismert megközelítés mellett tartanak ki, melyek nem megfelelőek vagy nem hatékonyak.
- **Mások követése:** amikor a stratégia alkotók csak azért és olyan döntést hoznak meg, melyet másoktól látnak mintaként. („Ha ők ezt csinálják, akkor mi is ezt kell tegyük.")
- **Téves egyetértés:** amikor a stratégia alkotók mások véleményét túlbecsülik és ezért elutasítanak, vagy minimálisra vesznek jelentős kockázatokat, melynek következménye egy teljesen működésképtelen stratégia lesz.
- **Egyéni célok kiemelése:** amikor a stratégia inkább az egyéni, adott szervezeti egység vagy vezető céljait tükrözi, nem pedig teljes mértékben a vállalat céljait tartalmazza.
- **Nem megfelelő mérőszámok:** amikor olyan mutatók kerülnek kialakításra, melyek az egyéni célok, elvárások megvalósulását tükrözik, és nem feltétlenül a stratégia megvalósulásának mérésére szolgálnak, illetve nem a vállalat érdekeit veszik alapul.

7. Visszamérés, ellenőrzés

A stratégia megvalósulásának és az információbiztonsági irányítási rendszer megfelelő és hatékony működésének ellenőrzésének két fő módszerét különböztethetjük meg:

- Monitorozás, visszamérés során készített riportok
- Audit, felülvizsgálat során készített jelentések

Az ezek közötti a főbb különbségeket az alábbi táblázat szemlélteti, részletesebben az alábbiakban kerülnek bemutatásra.

Monitorozás, visszamérés	Szempont	Audit, felülvizsgálat
Rendszeres, folyamatos	Rendszeresség	Eseti/rendszeres
Napi, heti, havi	Gyakoriság	Negyedéves, féléves, éves, kétéves, ad-hoc
Szűkebb, célirányos	Hatókör, terjedelem	Tágabb, sokrétűbb
Riport, jelentés	Eredménytermék	Audit jelentés

A monitorozás, visszamérés és az audit, felülvizsgálat közötti főbb különbségek

8. Mutatószámok

A visszamérések, ellenőrzések alapja, hogy legyen valamilyen előre definiált tényező, érték, amelyhez az eredményeket viszonyítani lehet. Ezt a célt szolgálják a mutatószámok, melyek esetében meg kell határozni egy mérhető tulajdonságot, mely alapján az adott tényező megvalósulása, hatékonysága meghatározható, és egy előzetesen elvárt, becsült értékkel összehasonlítható. Információbiztonsági szempontból tipikus mérőszámok például: feltárt sérülékenységek száma, helyreállítási időtartam, a bekövetkezett károk anyagi becslése.

A mutatókkal kapcsolatos kritériumok a következők:

- Érthető, egyértelmű
- Pontos
- Ismételhető
- Összehasonlítható, korábbi vagy más értékekkel
- Előrejelző képességgel bír
- Egyértelműen következnek belőle a szükséges javító intézkedések, beavatkozások
- Eredeti, hiteles, nem manipulálható
- Nem véletlenszerű
- Költség-hatékony

A mutatók közül többfélét különböztethetünk meg (CISM Review Manual, 2014):

- **Információbiztonsági irányítási rendszer hatékonyságának mérési mutatói***:* Az információbiztonsági program elemeinek mérésére a leginkább a CSF, KGI és KPI mutatók a legalkalmasabbak. Ezek nyújtják a legpontosabb és leginkább használható

információkat a folyamat- és szolgáltatás-célok megvalósulásának nyomon követéséhez, illetve a kitűzött célok és mérföldkövek teljesítésének, elérésének ellenőrzéséhez. Ezen mutatók rövid bemutatása:

- **CSF** (critical success factor): kritikus sikertényezők, vagyis azok a szempontok, elemek, melyek megvalósítása mindenképpen szükséges ahhoz, hogy a szervezet elérje a célját. (Például, az információbiztonsági irányítási rendszer működésének egyik kritikus sikertényezője, hogy a munkavállalók elsajátítják az információbiztonsági szemléletet.)
- **KGI** (key goal indicator): kulcs(fontosságú) célmutató, annak a meghatározására és mérésére szolgál, hogy *mit* szeretnénk elérni, mit kell teljesíteni, megvalósítani a kitűzött cél eléréséhez. (Például, annak eléréséhez, hogy a munkavállalók elsajátítsák az információbiztonsági szemléletet, éves rendszerességű információbiztonsági oktatást kell tartani és havi biztonságtudatossági hírlevelet kell számukra küldeni.)
- **KPI** (key performace indicator): kulcs(fontosságú) teljesítmény-mutató, mely annak megállapítására, mérésére szolgál, hogy a bevezetett folyamat *mennyire* megfelelően, hatékonyan működik. (Például, azt, hogy a munkavállalók mennyire sajátították el az információbiztonsági szemléletet, fel lehet mérni az oktatást lezáró vizsga teszttel, Social Engineering audittal, de következtetni lehet rá a bejelentett incidensek számából és jellegéből is.)

- **Stratégia megvalósításának mérési mutatói***:* Az információbiztonsági stratégia tartalmazza annak visszamérési módszereit, mutatóit is, hogy az abban definiált célok elérése, megvalósítása mikor és milyen mértékben teljesült.
- **Kockázatmenedzsment mutatók***:* Az információbiztonsági intézkedéseknek a megfelelő és kockázatarányos védelem kialakítása és fenntartása érdekében a rendszeres kockázatelemzés eredményén kell alapulnia. A kockázatmenedzsment sikerességének biztosításához elengedhetetlen követelmény, hogy az elvárások és a célok jól definiáltak legyenek. A kockázatmenedzsment program mutatóihoz kapcsolódnak például:
  - a szervezete kockázatvállalási hajlandósága
  - elfogadható kockázatok mértékének, szintjének meghatározása
  - kockázatcsökkentő intézkedések száma, hatékonysága az azonosított, jelentős kockázatok kezelésére

- negatív bekövetkezési hatások mértékének csökkentésére irányuló intézkedések száma, hatékonysága
- időszakos kockázat értékelési trendek
- bekövetkezési hatások trendjei
- BCP és DRP akciótervek tesztelésének gyakorisága és eredményei
- üzleti hatáselemzés eredménye

- **Értékteremtési mutatók**: Értékteremtésről akkor beszélhetünk, ha az információbiztonsági beruházások hatékonyan támogatni tudják az üzleti célok megvalósulását. Az információbiztonsági intézkedésekkel kapcsolatos befektetések akkor vannak optimális szinten, ha az információbiztonsági stratégiában meghatározott célok megvalósulnak, és az elfogadható kockázatok szintje minimalizálható. Az ehhez kapcsolódó mutatók magukban foglalhatják:
  - az információbiztonsági intézkedéseket a stratégiában meghatározott célok eléréséhez
  - kockázatarányos védelmi intézkedések bevezetését, vagyis a költségek illeszkednek a védett vagyonelem értékéhez (nem haladják meg azt)
  - az információbiztonsági erőforrásokat, melyek a felmért kockázatoknak és a lehetséges hatásnak megfelelően kerültek allokálásra
  - a védelmi intézkedésekre fordított költségeket, a védelmi intézkedések költséghatékonyságát
  - annak mutatóit, hogy a bevezetett védelmi intézkedések előre meghatározott kontroll célok alapján kerültek kialakításra
  - a szükséges és elégséges védelmi intézkedéseket, melyekkel a kockázatok szintje elfogadható mértékre csökkenthető
  - a bevezetett védelmi intézkedések működési hatékonyságának rendszeresen tesztelését
  - a kialakított kontrollok időszakos felülvizsgálatát és újraértékelését költségek, hatékonyság, illetve megfelelőség szempontjából
  - kontrollok kihasználtságának vizsgálata (a ritkán használt kontrollok nem feltétlenül költség-hatékonyak)
  - bevezetett védelmi intézkedések száma és hatékonyága közötti összefüggés vizsgálatát (kevesebb, de hatékonyabban működő kontroll költség-hatékonyabb lehet, mint több, de kevésbé hatékony)

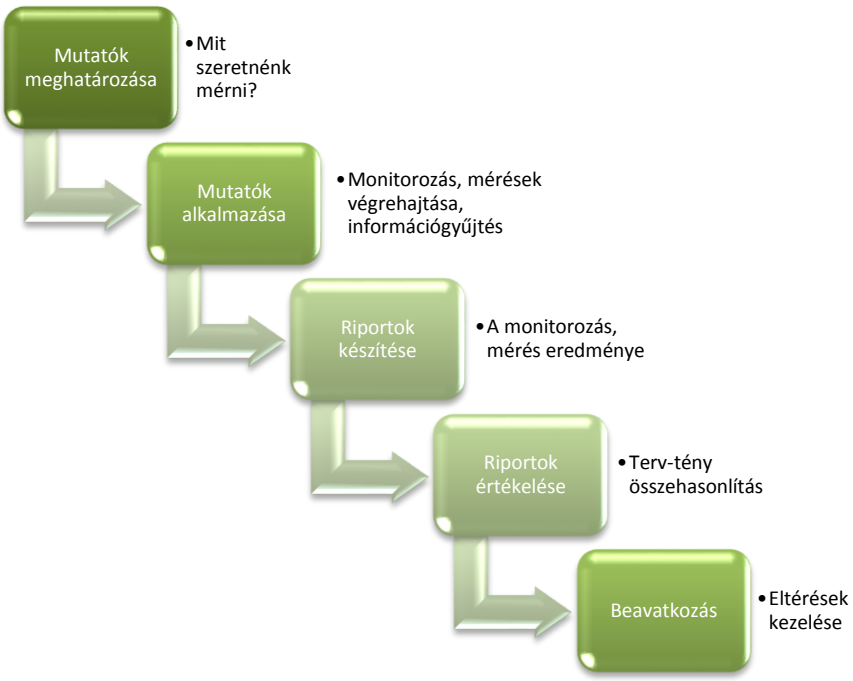
- a védelmi intzékedések működésének és hatékonyságának teszteredményei (a nem megfelelő, vagy nem megfelelően működő kontrollok nem valószínű, hogy költség-hatékonyak)

- **Erőforrás menedzsment mutatók**: A korábbiakban bemutatottak alapján az információbiztonsági intézkedések megvalósításához természetesen szükség van erőforrásokra, melyek lehetnek: humán erőforrások, technológiai megoldások, IT eszközök, infrastrukturális és egyéb erőforrások, valamint az ezekhez kapcsolódó folyamatok. Ezek megfelelő tervezését, megvalósítását, hatékony működését és menedzselését – mint az összes többi szervezeti erőforrás esetében - folyamatosan monitorozni kell, melyhez szintén kialakíthatóak mérőszámok. Az erőforrás menedzsment hatékonyságát mérő mutatók a következők lehetnek:
  - problémafeltárás gyakorisága
  - tudás-megosztás hatékonysága
  - folyamatok standardizáltsága, dokumentáltsága
  - megfelelően definiált szerepkörök és felelősségek (információbiztonsági irányítási rendszerhez kapcsolódóan)
  - az információbiztonsági terület bevonásának mértéke az egyes projektek tervezésébe, más folyamatokba
  - információbiztonsági terület, az információbiztonsági irányítási rendszer működtetését ellátó munkatársak száma
  - eszközök meghibásodásának száma, gyakorisága
  - eszközök karbantartásának gyakorisága
  - érintett személyek képzésének mutatói
- **Teljesítmény mérés**: Annak érdekében, hogy meggyőződjünk arról, hogy az információbiztonsági stratégiában foglaltak és megvalósítottak elérik a szervezeti célokat, az információbiztonsági folyamatok teljesítményének mérése, monitorozása, különböző riportok készítése szükséges. Nagyon fontos, hogy a mutatók a célcsoportnak megfelelően kerüljenek kialakításra, más riportot kell készíteni a menedzsmentnek, más riportot az üzemeltetőknek, illetve egyéb szereplők számára. Ezek a mutatószámok általában a következőket kell, hogy foglalják magukban:
  - információbiztonsági incidensek észlelésének és jelentésének ideje (mennyi idő telik el átlagosan, míg jelentésre kerül egy incidens)
  - az utólagosan felfedezett, azonban nem jelentett incidensek száma és gyakorisága

- költségek és működési hatékonyság összehasonlítása más hasonló szervezetekkel (benchmarking)
- védelmi intézkedések hatékonyságának mutatói
- arra vonatkozó mutatók, hogy az információbiztonsági célok milyen arányban és milyen eredménnyel teljesülnek
- arra vonatkozó mutatók, hogy az információbiztonsági célok és az üzleti célok milyen mértékben találkoznak
- nem várt biztonsági események, incidensek száma
- várható fenyegetések száma, ismerete
- azonosított sérülékenységek száma, jelentősége
- az azonosított kockázatok nyomon követésének, monitorozásának módszerei
- naplózás, logok felülvizsgálatának megfelelősége és gyakorisága
- üzletfolytonossági és helyreállítási tesztelés gyakorisága és eredményei

9. Rendszeres riportok, jelentések

A stratégia megvalósítása során rendszeresen figyelemmel kell kísérni, monitorozni kell az információbiztonsági irányítási rendszer működését és a célok megvalósulásának előrehaladását az előre definiált, szervezetre szabott mutatók segítségével. Az eredményeket riportok formájában rögzíteni kell, melyeket az érintett személyeknek kell eljuttatni, akik értékelik azok eredményét, összehasonlítják a tényértékeket az előre tervezett célértékekkel, és szükség esetén beavatkoznak az érintett folyamatokba annak biztosítása érdekében, hogy a célkitűzések teljesüljenek.



Monitorozás és riport-készítés

A mutatószámok és a riportolási rendszer kialakításánál a következők kérdéseket kell figyelembe vennünk (CISM Review Manual, 2014):

- Milyen információk fontosak ahhoz, hogy az információbiztonsági irányítási rendszer megfelelően működtethető, irányítható legyen?
- Melyek az információbiztonsági követelmények?
- Mi az, amire az üzleti területeknek szükségük van?
- Mi az, amit a felső vezetésnek kell tudnia?

A riportok elkészítésekor meg kell határozni és biztosítani kell, hogy azok megfelelő

- forrásból,
- célközönségnek,
- tartalommal,
- formátumban,
- gyakorisággal,
- időszakra vonatkozóan

kerüljenek elkészítésre és kommunikálásra.

Forrás

Meg kell határozni azon személyeknek, csoportoknak a körét, akik az érintett riport elkészítéséért felelősek, illetve akik a riportoláshoz adatot szolgáltatnak, valamint honnan, mely rendszerekből származnak a kinyert adatok. A mérési adatok csak abban az esetben tekinthetőek eredetinek és hitelesnek, amennyiben az előre meghatározott forrásból, adatszolgáltatásért felelős személytől vagy szervezettől érkeznek.

Célközönség

A riportok összeállításánál nagyon fontos annak ismerete, hogy az elkészített jelentést ki és hogyan fogja feldolgozni, mi a riportolás célja. Ennek érdekében meg kell határozni az egyes célcsoportokat, célközönséget, illetve azok információs igényét. Például az elmúlt hónap során bekövetkezett nem várt rendszer leállások teljes részletei, körülményei valószínűleg inkább csak az információbiztonsági vezető számára nyújtanak értékelhető és hasznos információkat, és a menedzsment számára mindebből inkább csak a költség vonzatú, üzleti folyamatokat érintő adatok lesznek relevánsak.

Azon túl, hogy meghatározásra kerül, hogy az egyes célcsoportok jelentései milyen információkat kell tartalmazzanak, ezek hatékony teljesítésének és megfelelőségének biztosításához ki kell jelölni, hogy az egyes célcsoportok részére ki készíti a riportokat. Ennek köszönhetően az előző példában az üzemeltetésről érkezett részletes riportokból az információbiztonsági vezető összeállíthat egy, a felső vezetés számára megfelelő és feldolgozható információtartalmú jelentést.

Az információbiztonsági irányítási rendszer működésével kapcsolatban általában a következő személyeknek, szervezeti egységeknek kell jelentést készíteni a célcsoportot érintő tartalommal:

Riportot kapja	Riportot készíti	Tartalom
Felső vezetés	Információbiztonsági vezető	Magas szintű, vezetői összegfoglaló, elsősorban a költségekre vonatkozó, kevésbé szakmai információkat tartalmazó jelentés.
Információbiztonsági irányítási szervezet/bizottság	Információbiztonsági vezető	Szakmai és költségekre vonatkozó információkat tartalmazó riport.
Információbiztonsági vezető	Folyamat és erőforrás gazdák (üzemeltetés)	A feladatok összehangolásának, a stratégia megvalósításának előrehaladása, elsősorban szakmai és technológiai jellegű információkkal.

Célcsoportok

A fenti táblázatban felsorolt célcsoportokon kívül egyéb személyek, vagy szervezeti egységek is meghatározásra kerülhetnek, mind a riportot készítő, mind a riportot feldolgozó felek oldalán, ezek köre a szervezeti felépítéstől, sajátosságoktól függően kerül kijelölésre.

A folyamatgazdák és erőforrásgazdák (üzemeltetők) számára szakterületi, információbiztonsági relevanciájú riportok, jelentések az általuk meghatározott tartalommal és formában saját munkatársaiktól kérhetőek. A felsővezetői döntéseket, meghatározott célokat az információbiztonsági vezető kommunikálja feléjük.

Tartalom

A riportok tartalmát az egyes célcsoportok érdekeltségének, igényeinek, képességeinek megfelelően kell összeállítani. Az alábbiakban néhány általános tartalmi elemet tüntettünk fel példaként, ezek azonban szervezetenként eltérőek lehetnek.

Felsővezetői riportok:

- Az információbiztonsági rendszer bevezetésének státusza.
- Üzleti hatáselemzés és felülvizsgálatainak magas szintű eredménye.
- Kockázatelemzés és felülvizsgálatainak magas szintű eredménye.

- Bevezetett kontrollok, védelmi intézkedések költség-hatékonyságát mérő mutatók
- Információbiztonsági projektek jelentéseinek vezetői összefoglalói.
- Biztonsági incidensek, észlelt fenyegetések statisztikája és költségvonzatai
- Külső, független felülvizsgálatok auditjelentései. (Például ISO/IEC 27001:2013 tanúsítás audit jegyzőkönyvében szereplő megállapítások.)
- Üzleti célokhoz, működési folyamatokkal való igazodás és a szervezeti kultúrába történő illesztés eredményességét tükröző mutatók. (Például biztonságtudatossági oktatások tesztjének eredményei.)
- A stratégia és célok módosításának gyakorisága, jellege, oka, ütemezési és erőforrás ráfordítási változtatások.
- Költségbecslések helyességének elemzése, eltérések, többletköltségek okainak feltárása.

Információbiztonsági irányítási szervezet/bizottság részére készülő riportok:

- Az információbiztonsági rendszer bevezetésének státusza.
- Üzleti hatáselemzés és felülvizsgálatainak eredménye.
- Kockázatelemzés és felülvizsgálatainak eredménye.
- Bevezetett kontrollok, védelmi intézkedések működési és költség-hatékonyságát mérő mutatók
- Információbiztonsági projektek magas szintű eredményei.
- Biztonsági incidensek, észlelt fenyegetések statisztikája, magas szintű elemzése
- Külső, független felülvizsgálatok auditjelentései. (Például ISO/IEC 27001:2013 tanúsítás audit jegyzőkönyvében szereplő megállapítások.)
- Üzleti célokhoz, működési folyamatokkal való igazodás és a szervezeti kultúrába történő illesztés eredményességét tükröző mutatók. (Például biztonságtudatossági oktatások tesztjének eredményei.)
- A stratégia és célok módosításának gyakorisága, jellege, oka, ütemezési és erőforrás ráfordítási változtatások részletes elemzése.
- Költségbecslések helyességének elemzése, eltérések, többletköltségek okainak feltárása és részletes elemzése.

Információbiztonsági vezető részére készülő riportok:

- Információbiztonsági projektek státusza, részletes eredményei
- Információbiztonsági védelmi intézkedések, kontrollok bevezetésének és működtetésének státusza, részletes eredményei

- Sérülékenységi vizsgálatok részletes eredményei
- Üzleti folyamatokban történő változások
- Folyamatgazdák felé delegált információbiztonsági feladatok végrehajtásának státusza (például adatvagyonleltár, üzleti hatáselemzés felülvizsgálata)
- Üzletfolytonossági akciótervek tesztelésének eredményei
- Humán erőforrással kapcsolatos változások (például kulcs felhasználók változása)
- Üzemeltetési mutatók
    - Biztonsági mentésekkel kapcsolatos mutatók (például sikeres/sikertelen mentések, meghibásodások, visszaállítási statisztikák)
    - Biztonsági frissítésekkel kapcsolatos mutatók (például megjelenésük gyakorisága, megjelenéstől a telepítésükig tartó időintervallum hossza)
    - Naplózással kapcsolatos mutatók (például gyakoriság, eredmények felülvizsgálata, kivizsgálások eredményei)
    - Vírusvédelmi rendszer statisztikái
    - Patch-menedzsment
    - Sérülékenység vizsgálatok eredményei
    - Konfiguráció menedzsment
    - IDS/IPS rendszerek riportjai
    - Tűzfal logelemzés
    - Nem tervezett leállások statisztikái, okai
    - Észlelt biztonsági incidensek
    - Helyreállítási akciótervek tesztelésének eredményei
- Fejlesztésekkel, rendszerbevezetésekkel kapcsolatos információbiztonsági mutatók, teszteredmények
- Biztonsági incidensek, észlelt fenyegetések, bekövetkezett károk listája, részletes elemzése
- Észlelt nem-megfelelőségek, fejlesztési javaslatok
- Külső, független felülvizsgálatok auditjelentései. (Például ISO/IEC 27001:2013 tanúsítás audit jegyzőkönyvében szereplő megállapítások.)
- Üzleti célokhoz, működési folyamatokkal való igazodás és a szervezeti kultúrába történő illesztés eredményességét tükröző mutatók. (Például biztonságtudatossági oktatások tesztjének eredményei.)

Formátum

A riportok formátumát tekintve készülhetnek egy, a szervezetnél alkalmazott rendszerből generáltan, dash-board szerűen, szöveges dokumentumként, illetve prezentáció formájában.
A definíciókat tekintve a *riportok* leginkább a vázlatos, táblázatos, diagramos vagy dashboard jellegű formában, röviden, tömören és értelmezhetően közlik az adatokat, terv- és tényértékeket. Ezzel szemben a *jelentések* inkább a szöveges értékelést, részletesebb kifejtést takarják, céljuk a tartalom részletesebb, mélyebb kifejtése, az eredmények megmagyarázása.
A felső vezetés számára általában magasabb szintű, könnyen értelmezhető, tömör riportok az előnyösek, míg a szakterületi vezetők elsősorban a részletesebb jelentéseket tartják használhatónak, melyek tényleges támpontot adnak az eltérések kezeléséhez. A gyakorlatban ezek egyszerre történő alkalmazása a jellemző.

Gyakoriság, időszak

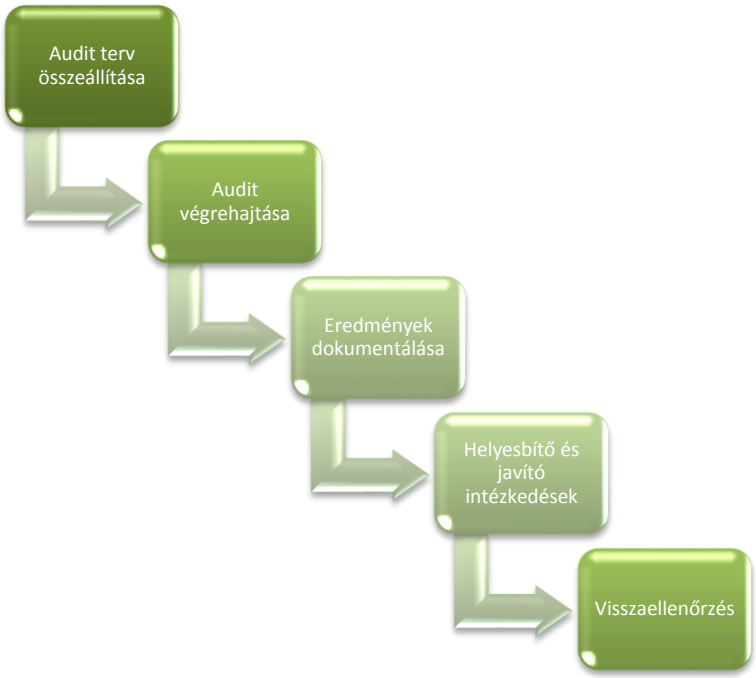
A riportok gyakoriságát a célcsoportok igényei, illetve a riportok tartalma, jellege határozza meg. Az operatív jellegű riportok inkább napi, heti vagy havi gyakoriságúak, a stratégiai jelentések pedig féléves, éves rendszerességűek. Ezek alkalmazása, meghatározása szervezetenként eltérő, de általában a következők lehetnek:

- **Napi riportok**: például napi biztonsági mentések statisztikája
- **Heti riportok**: például bejelentett incodensek, problénák listája és azok kivizsgálásának, megoldásának státusza, projekt státuszok
- **Havi riportok**: például kilépő-belépő felhasználók hozzáférési jogosultságainak beállításai, időráfordítások
- **Negyedéves, féléves gyakoriságú jelentések**: például belső auditok, rendszeres belső felülvizsgálatok eredményei
- **Éves rendszerességű jelentések**: például külső auditok eredményei, információbiztonsági stratégia megvalósításának, felülvizsgálatának eredményei.

10. Audit, felülvizsgálat

A rendszeres (félévente, évente, vagy kétévente történő) felülvizsgálatok célja az információbiztonsági irányítási rendszer megfelelő működésének ellenőrzése, illetve speciális auditok esetén a kijelölt kritikus erőforrások biztonságának, védelmi intézkedések, kontrollok megfelelő működésének vizsgálata.

Az audit végrehajtásának az alábbi lépései különböztethetőek meg:



Az audit végrehajtása

Első lépésként össze kell állítani egy audit tervet, amely tartalmazza, hogy

- mi a vizsgálat hatóköre, tárgya
- milyen követelményeknek, előírásoknak kell megfelelni
- hogyan, milyen módon szeretnénk a követelmények, előírások teljesülését vizsgálni (például tesztelés, mintavétel, megfigyelés),
- mik a vizsgálat várt, illetve lehetséges kimenetelei,
- kik a vizsgálatba bevont személyek,
- milyen más erőforrások bevonása szükséges a vizsgálat végrehajtásához.

Az auditot az audit tervnek megfelelően, az abban definiáltak alapján kell lefolytatni. A vizsgálatok eredményét az audit jelentésben dokumentáltan rögzíteni kell. Az audit jelentés tartalmazza

- a vizsgálat tárgyát
- a vizsgálat célját, leírását, teszteseteket
- a vizsgálat időpontját
- a vizsgálatot végző személyt
- a vizsgálatban résztvevő, bevont személyeket
- a vizsgálat módszerét
- a vizsgálat részletes eredményeit, észrevételeket

- az eredmények minősítését (megfelelő/nem megfelelő)
- evidenciákat, bizonyítékokat
- a javító vagy helyesbítő intézkedéseke vonatkozó javaslatot
- megelőzésre irányuló javaslatokat, egyéb észrevételeket,
- a visszaellenőrzésekkel kapcsolatos teendőket (a javító vagy helyesbítő intézkedések megtörténte ismételt ellenőrzés keretein belül megtörténik-e).

Az elkészült audit jelentés alapján a helyesbítő és javító intézkedéseket az érintett szakterületi vezetőknek kell részleteiben kidolgozniuk, illetve jóváhagyást követően az azokban meghatározottak megvalósításáról gondoskodniuk. Jelentős nem.megfelelőség vagy hiányosság esetén az azt kiküszöbölő helyesbítő vagy javító intézkedések megtörténte az auditot végrehajtó személyek által is visszaellenőrzésre kerülhet.
A rendszeres auditok végrehajtása lehet kötelező jellegű (például törvényi követelmények teljesítése, vagy szabványnak való megfelelés biztosítása miatt), vagy belső előírás által kiváltott (például belső szabályzatnak való megfelelés vizsgálata). Az auditot végző fél függvényében megkülönböztethetünk belső és külső auditot.

Belső audit

A belső auditok jellemzően a belső működési szabályzatokban előírt, a szervezet saját maga által megkövetelt rendszeres felülvizsgálatok. Általában éves, féléves gyakoriságúak, valamint ad-hoc elrendeltek (például biztonsági incidens kivizsgálása esetén), de ezektől eltérő gyakoriság is előfordulhat. Az információbiztonsági irányítási rendszer esetében a felülvizsgálatok célja mind magának a rendszer megfelelő működésének, a szabályozási környezetének a vizsgálata, mind pedig az alkalmazott védelmi intézkedések, kontrollok megfelelő működéséről és hatékonyságáról való meggyőződés.
Az információbiztonsági irányítási rendszer működtetésének belső auditjában az információbiztonsági vezető, a vizsgálatban érintett szakterületek vezetői, illetve egyéb érintett munkavállalók vesznek részt.

Külső audit

A szervezet keretein kívüli, külső felek által végrehajtott auditok célja lehet valamilyen külső követelménynek való megfelelés vizsgálata, vagy független szakértői vélemény biztosítása.
A külső követelmények teljesítését vizsgáló audit lehet

- kötelező jellegű, melynek nem, vagy nem megfelelő teljesítése szankciót, büntetést, vagy akár a működés ellehetetlenülését vonja maga után, például
    - törvényi kötelezettségek, jogszabályi előírásoknak,
    - iparági szabványok feltételei, valamint
    - bizonyos értelemben a csoportszintű előírásoknak való megfelelés,
- opcionális jellegű, azonban nem, vagy nem megfelelő teljesítésük negatív következményekkel járhat, mint például:
    - tanúsítványok megszerzése és fenntartása (például ISO/IEC 27001:2013 tanúsítás).

Ezen auditok során tett hiányosságokra, nem-megfelelőségre vonatkozó észrevételeket – amennyiben az audit jelentés másként nem rendelkezik - a következő felülvizsgálat időpontjáig kezelni kell, a helyesbítő, illetve javító intézkedéseket be kell építeni az információbiztonsági stratégiába, tervekbe.

A külső auditok másik típusának az a célja, hogy független szakértői véleményt nyújtson az információbiztonsági irányítási rendszer által bevezetett védelmi intézkedések, kontrollok megfelelő működéséről, fejlesztési lehetőségeiről, illetve sebezhetőség vizsgálatok keretein belül feltárja a kritikus támogató erőforrások sérülékenységeit, és támogassa azok megfelelő kezelését.

Ezen biztonsági auditokat a megbízó szervezet felügyelete, támogatása mellett a vizsgálatot végző szervezet munkatársai végzik. Az általuk tett megállapítások és javaslatok csak tájékoztatást adnak a vizsgált szervezet részére, azok felhasználásáról, alkalmazásáról, az információbiztonsági stratégiába illesztéséről a szervezet hozza meg a döntést.

11. Az eredmények felhasználása

A visszamérés, ellenőrzés célja, hogy a stratégiában foglaltak megvalósulásának státuszáról, illetve megfelelőségéről információt kapjunk. A monitorozás során készült riportok, rendszeres jelentések, belső és külső auditok eredményei alapján lehet meghatározni, hogy a stratégiában foglalt célok és a mért értékek, megállapítások egyeznek-e, és amennyiben eltérés tapasztalható, mit és milyen irányban, mértékben kell fejleszteni, módosítani. Ezen információk képezik a stratégia felülvizsgálatok bemenő adatait, alapjait.

Az eredmények felhasználása

A visszamérés során gyűjtött információkból választ kapunk a következőkre:

- a stratégiában foglalt célok megvalósulásának státusza, megvalósult, folyamatban levő, csúszásban levő, illetve ellehetetlenült célok azonosítása,
- a megvalósult célok megfelelősége, eredeti célkitűzésektől való eltérések, módosítások száma és jellege,
- melyek azok a bevezetett védelmi intézkedések, kontrollok, melyek nem hatékonyak, vagy nem megfelelően működnek (meghibásodások, incidensek kivizsgálása),
- felmerülő összeférhetetlenségek a rendszer elemi között melyekkel a stratégia alkotás során nem számoltunk,
- az egyes stratégiákban foglalt célok összehangolásának eredménye, a kapcsolódó funkciók, szakterületek elégedettsége, tapasztalatai a megvalósított célokkal, bevezetett intézkedésekkel kapcsolatban,
- milyen szervezeti, környezeti, vagy technológiai változások vannak, melyek a stratégia módosítását indokolhatják,
- melyek az átgondolandó célkitűzések, milyen feltételei vannak a megvalósíthatóságuknak,
- milyen hatékonyságnövelési lehetőségek állnak rendelkezésre,
- mely erőforrások, eszközök felülvizsgálata szükséges,
- milyen egyéb támogató erőforrások vonhatóak be, illetve milyen plusz erőforrások allokálása indokolt,
- milyen átütemezések szükségesek,

- melyek a stratégia kidolgozása során szándékosan vagy véletlenül figyelmen kívül hagyott tényezők, melyekkel mégis foglalkozni kell.

Természetesen a visszamérés és monitorozás csak abban az esetben teljesíti a feladatát és éri el a célját, amennyiben az eredményei ténylegesen és megfelelően felhasználásra kerülnek, ezáltal valóban hozzájárul az információbiztonsági rendszer megfelelő működtetéséhez és a stratégia hatékony megvalósításához.

Felhasznált irodalom

- 1. CISM Review Manual 2014, ISACA (2013)
- 2. ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements (2013)
- 3. MÉSZÁROS T., A stratégia jövője – a jövő stratégiája, Aula Kiadó (2005)
- 4. MOLNÁR B.; KŐ A., Információrendszerek auditálása, Corvinno Kft. (2009)
- 5. STACKPOLE, B.; OKSENDAHL, E., Security Strategy: From Requirements to Reality, Auerbach Publications (2010)

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.