ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel

Irányítási rendszerek

egyetemi jegyzet

Muha Lajos – Szádeczky Tamás

Nemzeti Közszolgálati Egyetem

Budapest, 2014

Tartalom

Bevezetés

Az irányítási rendszer „rendszer politika és célok megfogalmazásához, valamint a célok eléréséhez.”[1] „Egy szervezet irányítási rendszere különböző irányítási rendszereket tartalmazhat, például minőségirányítási rendszert, pénzügyi irányítási rendszert vagy környezetközpontú irányítási rendszert.”[2]

Ez azt jelenti, hogy egy irányítási rendszeréről magába foglalja a szervezet politikáját és céljait, és a szervezet vezetése a szervezet tevékenységei működtetésére meghatározza a különböző tevékenységek folyamatainak végrehajtási szabályait. Így a szervezet — a politikájának és céljainak megvalósítása érdekében — tervezetten és szabályozottan működik. A tervezett és szabályozott működés része a folyamatos javítás, valamint az elvégzett tevékenységek és eredmények dokumentálásának rendszere.

A gyakorlatban különböző irányítási rendszerekkel találkozunk, például:

- minőségirányítási rendszer;
- környezetközpontú irányítási rendszer;
- informatikai biztonsági irányítási rendszer;
- munkahelyi egészségvédelmi és biztonságirányítási rendszer[3];
- élelmiszer-biztonsági irányítási rendszer[4];
- egyéb speciális iparági vagy ügyfélkövetelmények.

A fenti irányítási rendszerek mindegyik tanúsítható.

Amennyiben a szervezet működése, környezete szempontjából fontos, hogy több irányítási rendszert is alkalmazzon, akkor úgynevezett **integrált irányítási rendszer**t is létrehozható. Az integrált irányítási rendszer a különböző irányítási rendszerek tetszőleges kombinációját ötvözheti. Az integrált irányítási rendszerek tanúsítására ugyanúgy, integráltan van lehetőség.

A jegyzetünk szempontjából az elektronikus információs rendszerek biztonságát leíró **Informatikai Biztonsági Irányítási Rendszer**[5] **(IBIR)** az irányítási rendszerek közül az

[1] MSZ EN ISO 9000:2005
[2] MSZ EN ISO 9000:2005
[3] A munkahelyi egészségvédelmi és biztonság-irányítási rendszerrel, illetve az annak követelményeit leíró OHSAS 18001 szabvánnyal jegyzetünkben nem foglalkozunk**.**
[4] Az élelmiszer-biztonsági irányítási rendszer rendszerrel, illetve az annak követelményeit leíró ISO 22000 szabvánnyal jegyzetünkben nem foglalkozunk.
[5] Information Security Management System – **ISMS**

elsődleges. Az IBIR az ISO/IEC 27001 szabvány alapvető fogalma. Az IBIR egy általános irányítási rendszer, amely az üzleti kockázat elemzésen alapul, megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot. Az irányítási rendszer magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési tevékenységeket, a felelősségeket, a gyakorlatokat, az eljárásokat, a folyamatokat és az erőforrásokat.

Az Informatikai Biztonsági Irányítási Rendszer akkor hatékony, ha hasznos a szervezet számára. Az információbiztonság a szervezet működési és üzleti kultúrájának szerves része kell, hogy legyen. Az információbiztonság a technikai problémákkal ellentétben elsődlegesen vezetői probléma, bár vannak nem elhanyagolható technikai problémák, különösen az informatikai használatától való általános függőség.

A jól irányított információbiztonság a sikeres üzleti tevékenység egyik alapfeltétele. Egyetlen szervezet sem tud napjainkban sikeres lenni információbiztonság nélkül. Az információbiztonság érdekében hozott, jól megválasztott vezetési intézkedések megfelelően megvalósítva, és pozitív hozzáállással használva nem csak költséget jelentenek, hanem sikeressé tehetik a szervezetet.

1. Az Információbiztonsági Irányítási Rendszer és más irányítási rendszerek összehasonlítása

1.1 Az ISO 27001:2013 szabvány

Az információ a szervezetek számára a legnagyobb érték.

Az információ megfelelő védelme nélkül:

a) Ellenőrizetlen az adatok kiszivárgása;

b) Az átgondolatlan, ellenőrizetlen módosítások adatvesztést okozhatnak;

c) Nyomnélküli adatvesztés esetén kicsi a helyreállíthatóság esélye;

d) Az információk nem érhetőek el, amikor szükség van rájuk.

Ezért az információ megfelelő védelme az összes vezető, az informatikai rendszerek tulajdonosai, a rendszergazdák és üzemeltetők, valamint az összes felhasználó felelőssége kell, hogy legyen, így lehet biztosítani az információk védelmét a sokrétű fenyegetettségekkel szemben minden szervezet esetében.

A fenti célok összegzéseként védeni kell a bizalmasságot, sértetlenséget és rendelkezésre állást. Ennek gyakorlati szabálya az ISO/IEC 27002:2013, Az információbiztonság irányítási gyakorlatának kézikönyve,[6] amely az 27002:2005 szabvány továbbfejlesztése, és melyet az ipar, a kereskedelem területein praktizáló információbiztonsági szakértők egy csoportja fejlesztett, a nagy, a közepes, valamint a kisvállalatok számára.

Az ISO 27001 aktuális verzióját 2013-ben adták ki „Az Információbiztonság Irányítási Rendszerei”[7] címmel, amelyet a korábbihoz hasonlóan fejlesztették ki az összes olyan szervezet számára, melyek megfelelően fel szeretnének készülni az ISO 27000 alapú tanúsításra. A szabvány követelményrendszert határoz meg az Informatikai Biztonsági Irányítási Rendszer tervezéséhez, létrehozásához, ellenőrzéséhez és bevezetéséhez, az informatikai biztonsági rendszer teljes életciklusában bekövetkező tevékenységekre vonatkozólag.

[6] Information Technology – Code of practice for information security management
[7] Information security management systems – Requirements

Az Informatikai Biztonsági Irányítási Rendszer[8] (IBIR, angolul Information Security Management System, ISMS) az ISO/IEC 27001:2013 szabvány alapvető fogalma. Az IBIR egy általános irányítási rendszer, amely az üzleti kockázat elemzésén alapul, megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot. Az irányítási rendszer magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési tevékenységeket, a felelősségeket, a gyakorlatokat, az eljárásokat, a folyamatokat és az erőforrásokat.

Az Informatikai Biztonsági Irányítási Rendszer akkor hatékony, ha hasznos a szervezet számára. Az információbiztonság a szervezet működési és üzleti kultúrájának szerves része kell, hogy legyen. Az információbiztonság a technikai problémákkal ellentétben elsődlegesen vezetői probléma, bár vannak nem elhanyagolható technikai problémák, különösen az informatikai használatától való általános függőség.

A jól irányított információbiztonság a sikeres üzleti tevékenység egyik alapfeltétele. Egyetlen szervezet sem tud napjainkban sikeres lenni információbiztonság nélkül. Az információbiztonság érdekében hozott, jól megválasztott vezetési intézkedések megfelelően megvalósítva és pozitív hozzáállással használva nem csak költséget jelentenek, hanem sikeressé tehetik a szervezetet.

Az ISO/IEC 27002 ajánlás alapját képező BS 7799 eredetileg a Brit Szabványügyi Hivatal (British Standard Institute) által kiadott brit szabvány. Előzményei az 1987 májusában alapított brit DTI/CCSC[9] tevékenységéhez nyúlnak vissza, amelynek feladata volt nemzetközi szinten is elfogadható informatikai biztonság értékelési és tanúsítási kritériumok és mechanizmus kidolgozása. Ennek eredménye vált valóra az ITSEC[10], valamint a UK ITSEC Scheme[11] dokumentumokban. Az ITSEC az informatikai rendszerek, de elsősorban informatikai termékek biztonsági funkcióira, valamint ezek biztonsági értékelésére és tanúsítására vonatkozó követelményeket tartalmazza. A UK ITSEC Scheme az értékelési, tanúsítási és minősítési folyamatokat határozza meg.

A DTI/CCSC másik feladatában a brit számítógép felhasználók támogatását tűzte ki célul, amely 1989-ben *„A Users Code of Practice”* címen került kiadásra, mint az

[8] Information Security Management System – **ISMS**
[9] DTI/CCSC = Department of Trade and Industry's, Commercial Computer Security Centre (Kereskedelmi és Ipari Minisztérium, Kerekedelmi Számítógép Biztonsági Központ)
[10] ITSEC = IT Security Evaluation Criteria (Információtechnológiai Biztonság Értékelési Kritériumok)
[11] UK ITSEC Scheme = Egyesült Királyság Információtechnológiai Biztonság Értékelési Kritériumok Eljárásrend

informatikai biztonság megteremtésére és fenntartására vonatkozó legjobb gyakorlatot leíró dokumentum. A brit Nemzeti Számítóközpont az ipari terület felhasználóiból szervezett konzorcium bevonásával ezt továbbfejlesztette. Az eredmény a PD 0003 jelű BSI ajánlás tervezet lett „*A Code of Practice for Information Security Management, Az információbiztonság*[12] *menedzsmentjének gyakorlati kódexe*" címmel. A dokumentum számítógépes felhasználók további bevonásával továbbfejlesztésre került, és végül a BSI 1995-ben BS 7799 szabványként adta ki, amelynek menedzselésére, utógondozására a BSI az egyik osztályát, a BSI-DISC[13]-et jelölte ki. Időközben igény támadt e szabvány olyan jellegű bővítésére, amely az informatikai biztonság menedzsmentjével foglakozik. A BS 7799 2. része „*Az információbiztonság menedzsment rendszerének specifikációja" (Specification for Information Security Management Systems*) címmel került kiadásra 1998-ban, az első rész kiegészítéseként.

A BS 7799 szabvány első revíziója 1999-ben történt meg, és az első részét nemzetközi szabványként (ISO[14]) történő elfogadásra javasolta BSI. A Nemzetközi Szabványügyi Szervezet 2000 augusztusában a BS 7799 1. részét változatlan szerkezetben, és gyakorlatilag változatlan tartalommal nemzetközi szabványnak fogadta el ISO/IEC 17799 néven.

A BS 7799 szabványt 1995 előtt egyszer már benyújtották a Nemzetközi Szabványügyi Testülethez, de ekkor a tagnemzetek többsége még nem fogadta el. Néhány ország, így például Új-Zéland, Ausztrália és Hollandia bizonyos kiegészítésekkel bevezette saját nemzeti szabványaként. Hollandia volt az első, amely a brit mintára alapozva elkészítette a saját biztonságértékelési, tanúsítási és minősítési sémáját. Ez az érdeklődés ösztönözte a BSI-t a szabvány továbbfejlesztésére, és az újbóli benyújtásra. E folyamat során került felismerésre az a tény, hogy nem elég egy szervezet részére az informatikai biztonsági rendszer kialakításának legjobb gyakorlatát kidolgozni, hanem – elsősorban a menedzsment részére – azt is meg kell határozni, hogy melyek azok a feltételek, követelmények, amelyeket teljesíteni kell a szabványnak való megfeleléshez. Ezek alapján egy külső tanúsító cég is egyértelműen el tudja dönteni, hogy az adott szervezet informatikai biztonsági rendszere megfelel-e a

---

[12] A BSI által használt „*információbiztonság*" kifejezést a hazai gyakorlatban egyre inkább terjedő „*informatikai biztonság*" kifejezéssel azonos értelműnek vesszük azzal a feltételezéssel, hogy a BS 7799-ben és a jelen kézikönyvben is alapvetően az informatikai rendszerben kezelt információk biztonságáról van szó. Ezért a kézikönyv szövegében mindenhol az „*informatikai biztonság"* kifejezést használjuk. *Az* „*információbiztonság*" kifejezést csak az angol címekben használt „*Information Security*" magyar fordításaként használjuk.

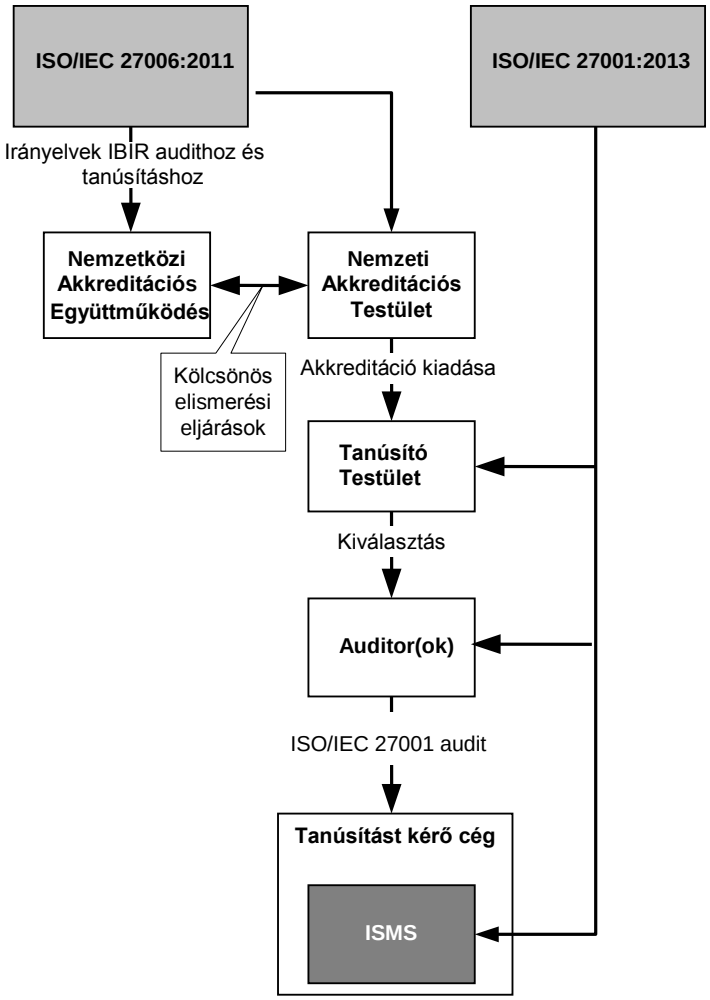
[13] BSI-DISC: BSI Delivering Information Solutions to Customers (BSI Információs Megoldások Szállítása Ügyfeleknek)

[14] ISO = International Standard Organization (Nemzetközi Szabványügyi Testület)

szabványnak vagy sem. A BS 7799-re alapozott értékelési és tanúsítási folyamatot az Egyesült Királyságban az úgynevezett *c:cure* eljárásrendben írták le, amely magába foglalt egy olyan akkreditálási rendszert is, amely a tanúsítást kérő cégtől független, és a brit akkreditáló szervezet, az UKAS[15] által akkreditált tanúsító cégek alkalmazását teszi lehetővé.

A c:cure-t azonban két évvel az elfogadás után visszavonták. Egy alternatív tanúsítási séma, mely az EA7/03, „Útmutató az Akkreditációs Testületeknek, melyek Információbiztonsági Irányítási Rendszereket tanúsítanak/regisztrálnak" címet viselte, sokkal elfogadottabbá vált az Európai Unióban, mint az angol séma, így Nagy-Britannia is áttért ennek használatára. 2007-ben ISO/IEC 27006:2007 címmel nemzetközi szabványként is ezt a sémát fogadták el, amelyet 2011-ben ISO/IEC 27006:2011 jelezettel frissítettek. Felülvizsgálata a 2013 év végén megjelent 27001 és 27002 frissítés miatt a közeljövőben várható.

[15] UKAS = UK Accreditation Service (Egyesült Királyság Akkreditációs Szolgálat)



Az utóbbi években jelentős előrelépés történt az információbiztonsági szabványok egységesítése érdekében. A már említett ISO 27001, 27002 és 27006 szabványok mellett több tucat további szabványt fogadott el, illetve tervez az ISO elfogadni a 27000-es szabványcsaládban. Ezekre vonatkozóan további információt a Információbiztonsági szabványok tárgy jegyzetében találnak.[16]

A telekommunikáció mellett több más iparághoz (pl. egészségügy, pénzintézetek) is terveznek IBIR útmutatókat kiadni. Emellett olyan területeket is szabványosítani akarnak a 27000-es családon belül, melyek az informatikai biztonság meghatározó elemei (pl. alkalmazásfejlesztés, üzletmenet-folytonosság, hálózatbiztonság), azonban az IBIR-hez kevésbé kapcsolódnak.

[16] Szádeczky Tamás: Információbiztonsági szabványok. NKE, Budapest, 2013.

1.2 Az ISO 9001:2008 szabvány

Az átdolgozott és ma érvényes ISO 9000:2008 szabványsorozat több szabványból áll. Ezek az alábbiak:

a) ISO 9000:2005 (MSZ EN ISO 9000:2005) Minőségirányítási rendszerek. Alapok és szótár.
b) ISO 9001:2008 (MSZ EN ISO 9001:2009) Minőségirányítási rendszerek. Követelmények.
c) ISO 9004:2009 (MSZ EN ISO 9004:2010) A szervezet tartós sikerének irányítása. Minőségirányítási megközelítés.

Az ISO 9000 szabványsorozat rendszerszabvány, ami azt jelenti, hogy előírásai nem a termék meghatározott tulajdonságait határozzák meg, hanem a szervezet működésének egészét átszövő minőségirányítás elveit, amelyek a következők (a következő felsorolás szó szerinti idézet az MSZ EN ISO 9000:2005 szabványból):

a) Vevőközpontúság

A szervezetek vevőiktől függenek, ezért ismerniük kell a jelenlegi és a jövőbeli vevői szükségleteket, teljesíteniük kell a vevők követelményeit, és igyekezniük kell felülmúlni a vevők elvárásait.

b) Vezetés

A vezetők megteremtik a szervezet céljainak és igazgatásának egységét. Hozzanak létre és tartsanak fenn olyan belső környezetet, amelyben a munkatársak teljes mértékig részt vehetnek a szervezet céljainak elérésében.

c) A munkatársak bevonása

A szervezet lényegét minden szinten a munkatársak jelentik, és az Ő teljes mértékű bevonásuk teszi lehetővé képességeik kihasználását a szervezet javára.

d) Folyamatszemléletű megközelítés

A kívánt eredményt hatékonyabban lehet elérni, ha a tevékenységeket és a velük kapcsolatos erőforrásokat folyamatként irányítják.

e) Rendszerszemlélet az irányításban

Az egymással összefüggő folyamatok rendszerként való azonosítása, megértése és irányítása hozzájárul ahhoz, hogy a szervezet eredményesen és hatékonyan valósítsa meg céljait.

f) Folyamatos fejlesztés

A szervezet teljes működésének átfogó, folyamatos fejlesztése legyen a szervezet állandó célja.

g) Tényeken alapuló döntéshozatal

Az eredményes döntések az adatok és egyéb információ elemzésén alapulnak.

h) Kölcsönösen előnyös kapcsolatok a (be)szállítókkal

A szervezet és (be)szállítói kölcsönösen függnek egymástól, és kölcsönösen előnyös kapcsolatuk fokozza mindkettejük értékteremtő képességét.

A minőségirányítási rendszerekkel szemben támasztott követelményeket az ISO 9001:2008 (magyar megfelelője MSZ EN ISO 9001:2009) szabvány rögzíti. Ez a szabvány egy olyan szervezet követelményeit írja le, amely képes a vevők igényeinek kielégítésére és felkészült e képességek független külső fél által végzett értékelésére.

A szabvány:

a) nem kötelező érvényű, minden alkalmazó önként vállalja e szabvány követelményeinek teljesítését,
b) a követelményeket általánosan fogalmazza meg, és a felhasználóra bízza a teljesítés részleteinek kialakítását. E tulajdonsága miatt nem csak a termelő és szolgáltató szervezetekre alkalmazható,
c) piac által vezérelt szabvány, amely a vevő és a szállító közötti kapcsolatot a vevő szemszögéből szabályozza.

Milyen előnyök várhatók az ISO 9000 szabványsorozat követelményrendszerének megvalósításától?

a) versenyelőny a piacon,
b) szabályozottabb termelés, szolgáltatás,
c) jobb, pontosabb vezetői információk,
d) hatékonyabb irányítás és munkavégzés,
e) javul a belső működés hatékonysága, szervezettsége,
f) csökkennek az üzemeltetési költségek,
g) ösztönző hatást gyakorol a beszállítói körre,
h) kialakul a folyamatos fejlődés igénye.

A minőségirányítási rendszer kiépítésének lépései a következők:

a) Előkészítés
    1) A vállalkozás tevékenységi folyamatainak, eljárásainak, ügymenetének felmérése,

2) Szervezeti átvilágítás,
3) A rendelkezésre álló dokumentáció átvizsgálása,
4) Minőségügyi tréning a társaság vezetői, a kijelölt minőségügyi megbízott, valamint a rendszer kiépítésében közreműködő dolgozók számára,
5) A működőképes minőségirányítási rendszer kiépítéséhez szükséges erőforrások meghatározása.

b) A minőségirányítási dokumentumrendszer kidolgozása
1) Minőségpolitika és minőségcélok,
2) Minőségirányítási kézikönyv,
3) Eljárási utasítások,
4) Munka- és vizsgálati utasítások,
5) Bizonylatok, formanyomtatványok, űrlapok, stb.

c) A minőségirányítási rendszer bevezetése
1) Minőségügyi tréningek,
2) Fizikai rendteremtés,
3) Hitelesítések, kalibrálások elvégeztetése,
4) Belső felülvizsgálók képzése,
5) Belső auditok,
6) A szükséges helyesbítő intézkedések meghatározása, végrehajtása.

A vevői bizalom elnyeréséhez természetesen nem elegendő a minőségirányítási rendszer megléte, az ISO 9000 nemzetközi szabványsorozatban rögzített követelményrendszernek való megfelelés független tanúsító szervezet általi tanúsítása is szükséges.

A tanúsítás folyamata:

a) Előaudit (nem kötelező, választható),
b) Dokumentáció vizsgálat,
c) Helyszíni audit,
d) Auditjelentés készítése (pozitív esetben javaslat a tanúsítvány odaítélésére).

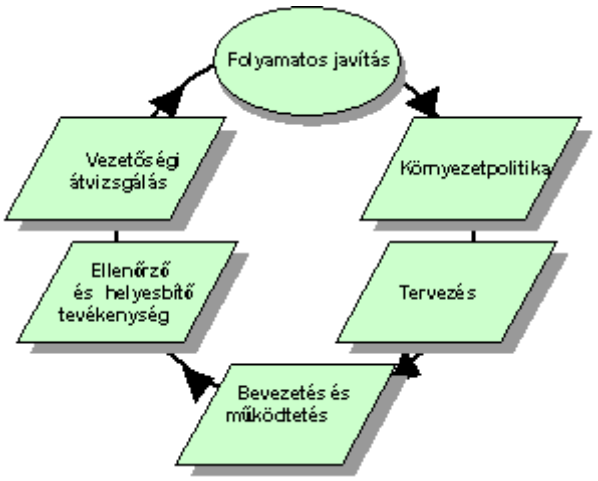
A minőségirányítási rendszer kiépítésének időszükséglete a cég vezetési szintjeinek számától és tevékenységének összetettségétől függően mintegy 6 - 12 hónap.

1.3 Az ISO 14001:2004 szabvány

A környezeti menedzsment rendszerek (KMR) nemzetközi szabványát, az ISO 14001-et, 1996 szeptemberében adták ki. A Magyar Szabványügyi Testület jelentette meg a magyar nyelvű fordítását "Környezetközpontú Irányítási Rendszerek. Követelmények és alkalmazási irányelvek (ISO 14001:1996)"címmel, MSZ EN ISO 14001 jelzettel, melyet 2004-ben nemzetközi szinten, majd 2005-ben Magyarországon is frissítettek.

Az ISO 14001 a gazdaság minden szektorában alkalmazható a szervezetekre: az iparban, a mezőgazdaságban, a szolgáltatóiparban.

A környezetközpontú irányítási rendszer modelljét a következő ábra szemlélteti

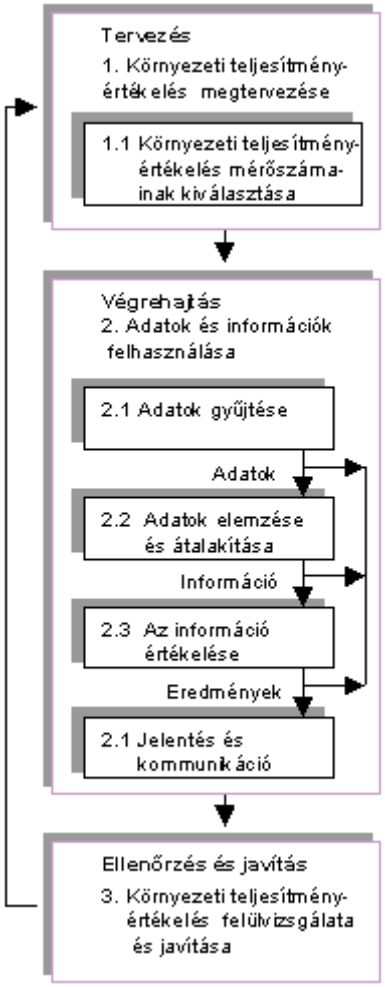


a) Környezeti Politika. A szervezet felvázolja a környezetvédelmi céljait, a környezetvédelmi jogszabálynak való megfelelés és a folyamatos javítás melletti elkötelezettséget.
b) Tervezés. Célokat és előirányzatokat kell kitűznie a szervezetnek a jövőbeni környezetvédelmi teljesítményét illetően, és ezekhez cselekvési terveket kell meghatároznia.
c) Végrehajtás és működés. Az alábbi követelményeknek kell megfelelni: feladatok és felelősök meghatározása, az alkalmazottakban erősíteni kell a környezetvédelem fontosságát, alkalmazottak képzése, a szervezet környezeti teljesítményét befolyásolható tevékenységek ellenőrzése/szabályozása (beszállítók és alvállalkozók tevékenységét is) haváriatervek kidolgozása balesetek esetére, tájékoztatási rendszer kidolgozása és működtetése környezetvédelmi kérdésekben, a rendszer-dokumentáció és a nyilvántartások ellenőrzési mechanizmusának kidolgozása.

d) Ellenőrzés és helyesbítő tevékenységek. A legfontosabb követelmények: a jogszabályoknak, valamint a kitűzött céloknak, előirányzatoknak való megfelelés ellenőrzése, belső eljárások ellenőrzése auditálással kapcsolatos rendelkezések, helyesbítő és megelőző tevékenységek.

e) Vezetőségi átvizsgálás. A vezetőség rendszeresen értékeli a szervezet környezeti teljesítményében elért eredményeket, és az eredmények ismeretében hozza meg a szükséges változtatásokat. Az ISO 14001 szabvány követelményeiből látható, hogy a hajtóerő, amely a szervezeteket a tanúsítására készteti, a törvényeknek való megfelelés.

A környezeti teljesítményértékelés modelljét a következő ábra szemlélteti.



2. A PDCA (TVEB) modell

Az IBIR létrehozása és működtetése ugyanolyan megközelítést igényel, mint sok más irányítási rendszer. Az ISO 27001-es szabvány erre a célra az OECD[17] által is támogatott TVEB[18] folyamatmodell használatát vezette be az Informatikai Biztonság Irányítási Rendszerének fejlesztésének, megvalósításának és hatékonyságának biztosítására. Ezek a folyamatok lefedik a teljes tevékenységi ciklust, megcélozva az effektív informatikai biztonság irányítását egy folytonos fejlesztési programon keresztül.

A TVEB bármilyen műveletre, tevékenységre, folyamatra, rendszerre, működtetésre, koncepcióra, elgondolásra vonatkoztatható, zárt hatásláncú, folytonosan ismétlődő körfolyamat-elv. A nemzetközi szakirodalomban elterjesztőjéről, W.E. Demingről elnevezve Deming ciklusnak (Deming's Cycle) is nevezik.

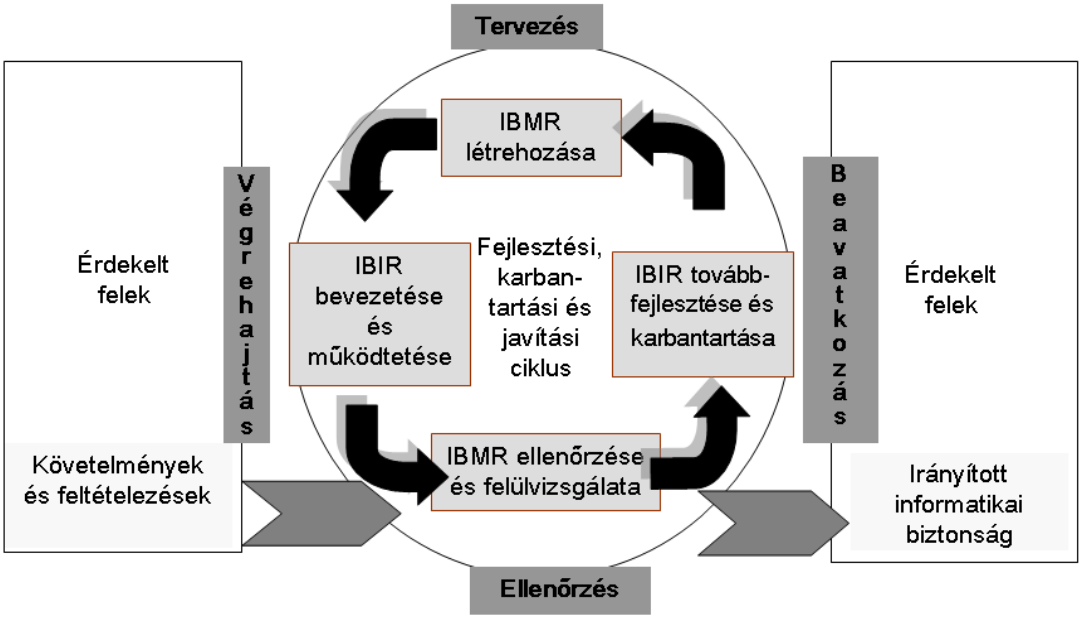
A TVEB modell négy szakaszból áll:

a) első szakasz a **Tervezés** (Plan) – a fennálló helyzet tanulmányozása, adatgyűjtés, javítás megtervezése;
b) második szakasz a **Végrehajtás** (Do) – a terv kipróbálása kísérleti jelleggel egy kisebb projekt vagy a felhasználók egy szűkebb körén belül alkalmazva;
c) harmadik szakasz az **Ellenőrzés** (Check) – a változtatások hatásának elemzése és értékelése);
d) negyedik szakasz a **Beavatkozás** (Act) – a bevált módszer bevezetése és szabványosítása.

Ez a ciklus minden folyamatjavító koncepció alapja.

A TVEB modell az alábbi ábrán látható:

[17] Organistaion for Economic Co-Operation and Development = Gazdasági Együttműködési és Fejlesztési Szervezet
[18] Tervezés - Végrehajtás - Ellenőrzés – Beavatkozás = Plan-Do-Check-Act – **PDCA**



2.1 A TVEB modell értelmezése az Információbiztonsági Irányítási Rendszerben

a) **Tervezés** (Az Informatikai Biztonsági Irányítási Rendszer létrehozása): A szervezet általános szabályainak megfelelő biztonságpolitika, célok, módszerek, folyamatok és eljárások meghatározása, amelyek relevánsak a kockázatkezelés és az informatikai biztonság fejlesztése szempontjából.

b) **Végrehajtás** (Az Informatikai Biztonsági Irányítási Rendszer bevezetése és működtetése): A biztonsági szabályzat, intézkedések, módszerek és eljárások megvalósítása és üzemeltetése.

c) **Ellenőrzés** (Az Informatikai Biztonsági Irányítási Rendszer ellenőrzése és felülvizsgálata): Fel kell becsülni és – ahol alkalmazható – fel kell mérni a biztonságpolitika végrehajtásának folyamatát, a célok és a gyakorlati tapasztalatok alapján az eredményeket a vezetés számára jelenteni kell.

d) **Beavatkozás** (Az Informatikai Biztonsági Irányítási Rendszer továbbfejlesztése és karbantartása): A vezetői felülvizsgálat eredményén alapuló korrigáló és megelőző intézkedéseket kell hozni, illetve folyamatosan tovább kell fejleszteni az Informatikai Biztonsági Irányítási Rendszert.

2.1.1 Az Információbiztonsági Irányítási Rendszer létrehozása

Az Informatikai Biztonsági Irányítási Rendszer létrehozása érdekében a következő **tervezés**i lépéseket kell megtenni tervezés során:

a) **Az Informatikai Biztonsági Irányítási Rendszer területének, kiterjedésének definiálása** a szervezet üzleti jellegzetességeinek, elhelyezkedésének, aktíváinak értelmében. Az IBIR alkalmazási területét pontosan meg kell határozni. Az IBIR alkalmazási területét a szervezet egy behatárolt részén a többitől függetlenül kell meghatározni, vagy meghatározható akár az egész szervezetre is. Az alkalmazási terület meghatározása igényli a csatlakozási felületeket más rendszerekhez, szervezetekhez, külső beszállítókhoz, és szintén figyelembe kell venni olyan igényeket és függőségeket, mint pl. hogy a biztonsági követelmények kielégíthetőek-e az Informatikai Biztonsági Irányítási Rendszerrel.

b) **Az informatikai biztonságpolitika definiálása** a szervezet üzleti jellegzetességeinek, elhelyezkedésének, aktíváinak értelmében figyelembe véve a törvényi és szabályozási követelményeket. A vezetésnek el kell fogadnia az informatikai biztonsági politikát. A informatikai biztonsági politika magában foglalja a biztonsági célokat, megadja a vezetői irányítást és tevékenységeket, megállapítja a kockázatkezelési összefüggéseket és kritériumokat melyek ellenében, kiértékeli a kockázatot.

c) **A kockázatelemzési eljárás meghatározása.** A szervezeteknek szüksége van egy követelményrendszerre az elfogadható kockázatok és az elfogadható kockázatok szintjének meghatározására. Minden esetben a szervezet dönti el, hogy melyik kockázatelemzési eljárást alkalmazza. Fontos megjegyezni, hogy akármelyik módszert is kívánja használni szervezet, az Informatikai Biztonsági Irányítási Rendszer egészére kell kiterjeszteni. Az IBIR a kockázatelemzési eljárással kapcsolatban a következő, kockázatokkal összefüggő szervezeti szempontoknak a teljes lefedését igényli:

   1) humán intézkedések;
   2) üzleti folyamatok;
   3) üzemeltetési és karbantartási módszerek és eljárások;
   4) törvényi, szabályozási és szerződési ügyek;
   5) információfeldolgozási lehetőségek és eszközök.

A kockázatelemzés kötelező követelmény, de ez nem teszi kötelezően szükségessé néhány automatizált szoftver eszköz használatát, azonban néhány esetben előnyt jelent ezen eszközök használata, különösen akkor, ha a kockázatok és a kockázatokkal összefüggő információk (fenyegetések, sebezhetőségek, vagyontárgyak) újraértékelésére van szükség. A kockázatelemzés összetett módszer, és ennek szemléletétől függ az IBIR felülvizsgálatának teljessége. A különféle technikák alkalmazásának meg kell egyeznie azzal az összetettségi igénnyel és szinttel, melyre a szervezetnek szüksége van.

d) **A kockázatok azonosítása** a vagyontárgyakról szóló jelentések, és a vagyontárgyakkal kapcsolatos fenyegetettségek: a bizalmasság, a sértetlenség, és a rendelkezésre állás elvesztése figyelembevételével történik.

e) **A kockázatok elemzése** a d) pontban szereplő információk feldolgozásán alapul, ügyelve arra, hogy magába foglalja az összes szervezeti irányítási területet, olyanokat, mint:

   1) humán intézkedések;
   2) üzleti folyamatok;
   3) üzemeltetési és karbantartási módszerek és eljárások;
   4) törvényi, szabályozási és szerződési ügyek;
   5) adatfeldolgozási lehetőségek és eszközök.

   Az eljárás magába foglalja a biztonsági hibákból bekövetkező üzleti károk becslését, és az esemény bekövetkezési valószínűségének a meghatározását. A szervezet a fentieken kívül még igényli a kockázat szintjének becslését, és annak meghatározását, hogy vajon ezek a kockázatok még elfogadhatóak, vagy szervezetileg meghatározott eljárást igényelnek.

f) **A kockázatok kezelési módjának megállapítása és kiértékelése.** A szervezet által már megállapított, felbecsült, és ismert kockázatok kihatásának (arányának) megfelelő, szervezet szintű intézkedéseket tudunk hozni. A szervezet válaszlépésként mérlegelheti a következő, megfelelően alkalmazható kockázatcsökkentő intézkedéseket:

   1) Távol tartja magát a nem elfogadható kockázatokkal járó tevékenységektől;
   2) Teljesen vagy részben áthelyezi a kockázatot egy másik fél terhére, (pl. biztosítók);
   3) Tudatosan és tárgyilagosan felvállalja (elfogadja) a kockázatot.

g) **A kockázatkezelési intézkedések tárgyának és céljának a kiválasztása**. Ha a szervezet biztonsági intézkedések alkalmazhatóságáról dönt, akkor ki kell választania azt az intézkedési rendszert, amely megfelel kockázat kezelésére.

h) **Az alkalmazhatósági nyilatkozat előkészítése.** Az alkalmazhatósági nyilatkozat minden szervezet számára kötelező dokumentum, amely bemutatja az intézkedés tárgyát és célját, valamint a kiválasztott intézkedéseket, melyeket egy kockázatelemzés eredményeinek és a kockázatkezelési eljárásoknak kell alátámasztania, így igazolva az intézkedések kiválasztását. Az alkalmazhatósági nyilatkozat kockázatelemzés nélkül indokolatlan, érvénytelen.

2.1.2 Az Információbiztonsági Irányítási Rendszer bevezetése és működtetése

A **végrehajtási** szakaszban a szervezetnek biztosítania kell a tervezési szakaszban létrehozott IBIR eljárások használatát. Ezek magukba foglalnak egy jól működő kockázatkezelési rendszert, melyet az informatikai biztonsági fenyegetések azonosítására és kezelésére terveztek. A tervnek meg kell határoznia a biztonságot érintő események, és a biztonsági fenyegetettségek esetén használatos vezetői és felhasználói tevékenységeket, valamint a vezetői és a felhasználói felelősségi köröket az Informatikai Biztonsági Irányítási Rendszer alapján. A szervezetnek el kell készítenie egy kockázatkezelési tervet, ami tulajdonképpen egy olyan eljárásgyűjtemény, amely a kiválasztott biztonsági intézkedéseket, a szabályokat, a felelősségek meghatározását, a felhasználói tréningek leírását, az erőforrás-kezelést, és a biztonsági események (incidensek) kezelését tartalmazza. A kiválasztott intézkedések megvalósításakor a legfontosabb szempont azok hatékonysága. A kiválasztott intézkedéseknek hatékonyan kell kezelniük a biztonsági kockázatokat, de a megvalósítás költséghatékonyságát is figyelembe kell venni. A költséghatékonyság mértéke függ attól, hogy például mennyibe kerül a felhasználók képzése, a különféle követő és jelentéskészítő tevékenység – vagyis az implementációs költség –, és ezzel szemben mennyibe kerül a veszélyforrás által okozott tényleges kár. A biztonsági intézkedések hatással vannak a munkafolyamatokra, és úgy kell megválasztani őket, hogy felesleges terhelést ne okozzanak. Nem szabad megfeledkezni arról, hogy a biztonsági intézkedések nehezítik, lassítják a folyamatokat, de ennek ellenére használni kell őket! Kétségkívül meg kell állapítani megbízhatóságukat, és akkor a biztonság javára lesz a szervezetnek, nem pedig terhére.

2.1.3 Az Információbiztonsági Irányítási Rendszer ellenőrzése és felülvizsgálata

Az **ellenőrzés**i szakaszban a szervezetnek biztosítania kell a végrehajtási szakaszban létrehozott IBIR eljárások használatát. Ezek egy jól működő kockázatkezelési rendszert kell, hogy tartalmazzanak, amelyet az informatikai biztonsági fenyegetések azonosítására és kezelésére terveztek. Ahhoz, hogy Informatikai Biztonsági Irányítási Rendszer hatékonyan kezelje a biztonsági kockázatokat, folyamatosan ellenőrizni és nyomon követni kell az Informatikai Biztonsági Irányítási Rendszert érintő összes változást.

A fenyegetések folyamatosan változnak, így hatásuk, a gyenge pontok, sebezhetőség is folyamatosan változik, így:

a) folyamatosan változik az üzleti környezet: új üzleti partnerek, új szállítási láncok, új vevőkörök, új piaci területek, új piaci körülmények, külső személyek bevonása, outsorcing alkalmazása, otthoni munka (home working) megoldások;
b) változnak az üzleti és a politikai célok;
c) változik a szervezeti struktúra, a munkakörnyezet, a munkatársak cserélődnek;
d) új technológiák kerülnek bevezetésre: új rendszerek és alkalmazások, frissítések implementálása, a hálózat terjeszkedése, a rendszer platformok sokfélesége, távmunka, harmadik fél hozzáférése, és még több outsorcing megállapodás.
e) változik a jogszabályi és a szabályozási környezet.

A fenti felsorolásban szereplő, a szervezeteket érintő változások mindegyike valamilyen fenyegetést, kockázatot hordoz magában. Csak úgy garantálhatjuk az Informatikai Biztonsági Irányítási Rendszer hatékony működését, ha ezeket a kockázatokat újraelemezzük, és a maradék kockázatok szintjét az elviselhető szintre csökkentjük.

Az ellenőrzési szakaszban a szervezeteknek újra kell vizsgálniuk az Informatikai Biztonsági Irányítási Rendszert: megfelel-e a hatóköre, az intézkedési rendszere kellően hatékony-e és megfelelő-e, az eljárások használata megfelel-e a követelményeknek, a létrehozott szabályzatok használhatók-e, a felelősségek kezelése megfelel-e a követelményeknek, a biztonsági tevékenységek elfogadottak-e, a biztonsági események alapján vannak-e kifejlesztve az eseménykezelő eljárások, továbbra is megfelelő-e az üzletfolytonossági terv.

Az ellenőrzési szakasz alatt vezetői felülvizsgálatokra van szükség: biztonsági vizsgálat, rendszertesztek, a biztonsági események jelentéseinek a vizsgálata, a rendszergazdák, üzemeltetők javaslatainak figyelembevétele, mindezek biztosítják, hogy az IBIR megfeleljen

az üzleti követelményeknek, és az információbiztonsági kockázatok az elviselhető szinten maradjanak.

2.1.4 Az Információbiztonsági Irányítási Rendszer továbbfejlesztése és karbantartása

A **beavatkozás**i szakaszban a szervezetnek biztosítania kell a végrehajtási szakaszban létrehozott IBIR eljárások karbantartását, javítását, valamint az ellenőrzési szakaszban meghatározott további eljárások felülvizsgálatát. Az ellenőrző szakasz vizsgálatai által az Informatikai Biztonsági Irányítási Rendszer folyamatait érintő azonosított változások miatt szükség van a biztonsági folyamatok javítására, csak így kezelhetők megfelelően a informatikai biztonsági rendszert érintő kockázatok.

A kockázatok, fenyegetések folyamatosan változnak, kívülről vagy belülről fejtik ki nem várt hatásukat. Ezért szükséges az Informatikai Biztonsági Irányítási Rendszert folyamatosan felülvizsgálni, és válaszolni a megváltozott, az ellenőrzési szakaszban azonosított fenyegetésekre. A biztonsági események bekövetkezése esetén, az adott fenyegetésre azonnal és hatékonyan válaszolni kell. A fenyegetettségekre, kockázati tényezőkre folyamatosan figyelni kell a helyi kockázatok újraelemzésével, valamint a szabályozási rendszer felülvizsgálatával. Ebben helyenként szükség lehet javító és megelőző intézkedések bevezetésére. A szervezetnek azonosítania kell az Informatikai Biztonsági Irányítási Rendszerben implementált, de nem alkalmazható eljárásokat, ezeket meg kell szüntetni, és javító intézkedésekkel meg kell akadályozni ismétlődésüket. A szervezetnek azonosítania kell a nem alkalmazható intézkedések kiváltó okait, és megelőző intézkedéseket kell hozni ezek kiküszöbölésére.

Fontos szempont, hogy minden javító és megelőző intézkedés rögzítve legyen, és ezen intézkedések eredménye megfelelő kommunikációs csatornákon jusson el a szervezet megfelelő munkatársai részére. Ez a kommunikáció a tevékenységek implementációjához elengedhetetlen. A szervezetnek biztosítania kell, hogy az Informatikai Biztonsági Irányítási Rendszerben implementált javító intézkedések megegyezzenek a kitűzött követelményekkel, és megvalósítsák az elérendő célokat.

3. Az Információbiztonsági Irányítási Rendszer létrehozása

3.1 Helyzetfelmérés

3.1.1 Az információbiztonság aktuális állapotának felmérése

Az IBIR-t bevezetni kívánó szervezetnek a bevezetést megelőzően fel kell mérnie és meg kell ismernie a szervezetben jelenleg uralkodó információbiztonsági kultúrát, az alkalmazott kontrollokat, azok működési hatékonyságát. Ezen állapot felméréséhez segítséget nyújt az ISO 27002-es szabvány, Az információbiztonság menedzsmentjének gyakorlati kódexe. Ahhoz hogy a bevezetendő IBIR teljeskörűségét biztosítani tudjuk, a szabvány által definiált, minden területre kiterjedő felmérést kell végrehajtania a szervezetnek, mely felmérés eredményeképpen részletes és teljeskörű képet kap a vezetés az információbiztonság jelenlegi helyzetéről a szervezetben, megismeri gyenge pontjait, szabályozott vagy esetleg még szabályozatlan területeit. Az alábbi területek részletes felmérését kell végrehajtani:

a) Szabályozási környezet
b) Szervezeti biztonság
c) Vagyontárgyak biztonsága
d) Emberi erőforrások biztonsága
e) Fizikai és környezeti biztonság
f) A kommunikáció és üzemeltetés biztonsága
g) Hozzáférés-ellenőrzés
h) Fejlesztés, beszerzés, karbantartás
i) Incidenskezelés
j) Működés folytonosságának irányítása
k) Megfelelés (jogszabályi, törvényi)

A felmérés eredményeképpen a szervezet átfogó képet fog kapni a szervezetben aktuálisan uralkodó információbiztonság helyzetéről, megismeri a gyenge és támadható pontokat, ezáltal felmérheti a lehetséges fenyegető tényezőket, melyek az IBIR bevezetésekor végrehajtandó kockázatmenedzsment sikeres végrehajtásának alapinformációi. Az információbiztonsági helyzetfelmérés hiányában az IBIR bevezetését tervező szervezet nem lesz tisztában a bevezetés során felmerülő feladatok számosságával, mely elengedhetetlen fontosságú a hatékony tervezés szempontjából.

3.1.2 Az informatikai irányítás aktuális állapotának felmérése

Az IBIR-t bevezetni szándékozó szervezet számára az információbiztonság helyzetfelmérése mellett javasolt megismerni az Informatikai irányítás jelenlegi szintjét a szervezetben, mely során megismeri szabályozási környezetét, a szervezet munkatársainak viszonyát az informatikai irányításhoz, a folyamatok eljárások szabályozottságát, az informatikai kultúra milyenségét. Ezen felmérés végrehajtásához segítséget nyújthat a COBIT-ban[19] definiált ún. „érettségi modell" módszere,[20] mely egy olyan pontozásos értékelő rendszert határoz meg, amely segítségével minden szervezet a „nem létező" és az „optimalizált" szélső értékek közötti skálán felmérheti saját helyzetét. A módszertan segítségével az IBIR-t bevezető szerveztek megismerik:

a) A szervezet jelenlegi helyzetét – hol tart jelenleg a szervezet
b) Az ágazat piacvezető szervezeteinek jelenlegi helyzetét – összehasonlítás
c) A nemzetközi szabványok által meghatározott ideális helyzetet – összehasonlítás
d) A szervezet fejlődésének stratégiáját – hova szeretne eljutni a szervezet

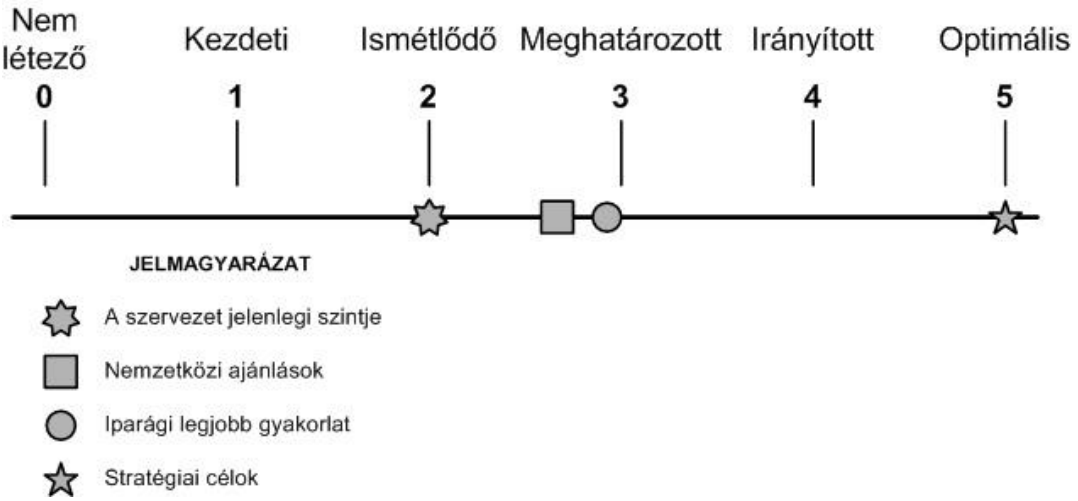
A COBIT által meghatározott módszertan alkalmazásával a szervezet meghatározhatja az informatikai irányításának jelenlegi szintjét, megismeri hiányosságait, kitűzheti a stratégiai céljait. A módszer alkalmazásának előnye, hogy a szervezet a felmérést követően könnyen elhelyezheti saját szervezetét a skálán, és felmérheti, hogy mire van szüksége a kívánt állapot eléréséhez. Ezen a ponton lehet összekapcsolni a COBIT minőségi besorolása által biztosított tervezési módszert és az IBIR bevezetési feladatait. A módszertan alkalmazásával végzett felmérés segítségével a szervezet egy általános képet kap az informatikai irányítás, a biztonság és az alkalmazott kontrollok jelenlegi helyzetéről a szervezetben. Ezen paraméterek ismeretében a szervezet meg tudja határozni azt, hogy az IBIR bevezetéséhez és működtetéséhez milyen lépéseket kell megtennie, milyen feladatok állnak még előtte, hogy hatékony, jól működő informatikai irányítási rendszert vezessen be és működtessen.

Az IBIR sikeres bevezetéséhez és hatékony működtetéséhez az értékelési skálán minimálisan a 4-es, optimális esetben az 5-ös érettségi szintet kell elérnie és teljesítenie a szervezetnek. A hazai tapasztalatokat figyelembe véve, amennyiben a szervezet nem éri el az IBIR bevezetésekor a 3-as szintet, abban az esetben csak nagy erőforrás ráfordítással és

[19] COBIT = Control Objectives for Information and related Technology
[20] A COBIT 4.1 Matury Modelt a COBIT 5-ben leváltotta a Process Capability Model, de a jelen értékelésben a korábbi érettségi modell jobban alkalmazható

szervezeti kultúra átformálással lehet csak bevezetni és hatékonyan működtetni az IBIR-t. Tehát az előbbieket figyelembe véve javasolt a felmérés eredményeinek figyelembe vételével megtervezni az IBIR bevezetésének folyamatát.

Az alkalmazandó minőségi skálát az alábbi ábra szemlélteti.



Az egyes szintek jelentéséről bővebben:[21]

0 (Nem létező)

Teljesen hiányzik az informatikai irányítás működésére utaló bármilyen eljárás. A szervezet nem ismerte fel még azt sem, hogy foglalkozni kellene ezzel a kérdéssel, ezért nincs is napirenden a kérdés.

1 (Kezdeti/Ad hoc jellegű)

Bizonyítható, hogy a szervezet felismerte az informatikai irányításhoz kapcsolódó kérdések létezését és kezelésének szükségességét. Mindazonáltal nem alkalmaznak egységes eljárásokat, csupán ad hoc jellegű megoldásokat, egyedi illetve eseti alapon. A vezetés hozzáállása a kérdéshez kaotikus, és csak elvétve és alkalmanként kerülnek szóba az ilyen jellegű kérdések és a kezelésükhöz szükséges módszerek. Előfordul, hogy a vezetés bizonyos mértékig tisztában van azzal, hogy az informatika milyen értékekkel járul hozzá a kapcsolódó vállalati eljárások teljesítményéhez. Nem működik egységes értékelési eljárás. Az informatikai eljárások ellenőrzésére csupán utólagos jelleggel kerül sor olyan esetek kapcsán,

[21] Az érettségi szintek és a 2013. évi L. törvényben meghatározott biztonsági szintekbe sorolás között logikai párhuzam vonható

amelyek nyomán veszteségek keletkeztek, illetve amelyek zavart okoztak a szervezet működésében.

2 (Ismétlődő, de intuitív jellegű)

A szervezet általános szinten tisztában van az informatikai kérdések fontosságával. Folyamatban van az informatikai irányításhoz kapcsolódó tevékenységek és teljesítmény-mutatók kidolgozása, ideértve az informatikai tervezést, valamint az eljárások működtetését és felügyeletét is. Ezen kezdeményezések részeként az informatikai irányítási tevékenységeket formálisan is integrálják a szervezet változás-kezelési eljárásába a felső vezetés aktív közreműködése és felügyelete mellett. A szervezeti alapfolyamatok hatékonyságának javítása illetve kontrollálása céljából kiválasztanak bizonyos informatikai eljárásokat, amelyeket megfelelően megterveznek és felügyelnek, mint beruházásokat, és a meghatározott informatikai architektúra keretrendszer alapján alakítanak ki. A vezetés meghatározta informatikai irányításra vonatkozó alapvető mérési és értékelési módszereket és technikákat, az eljárást azonban nem alkalmazzák a szervezet egészére kiterjedően. Nincsen az irányítási normákra vonatkozó formális képzés és tájékoztatás, és a felelősségi körök egyénekre vannak bízva. Bizonyos egyének határozzák meg az irányítás módját a különböző informatikai projekteken és eljárásokon belül. Irányítási eszközöket csak korlátozott mértékben alkalmaznak az irányításhoz kapcsolódó mérési mutatók összegyűjtésére, de előfordul, hogy ezeket sem használják fel a lehetséges maximális mértékben a funkcionalitásukra vonatkozó szakértelem hiánya miatt.

3 (Meghatározott eljárás)

Az informatikai irányításhoz kapcsolódó tevékenységek szükségessége tudott és elfogadott a szervezetnél. Kidolgoztak az informatikai irányításhoz kapcsolódó bizonyos alap-mutatókat, amelyek kapcsán meghatározták, dokumentálták és beépítették a stratégiai és operatív tervezés és felügyelet folyamataiba az eredmény-mutatók és a teljesítményt meghatározó tényezők közötti összefüggéseket. A bevezetett eljárásokat szabványosították és dokumentálták. A vezetés megfelelő módon kommunikálta a szervezet felé a szabványosított eljárásokat és informális képzési formákat alakított ki. Az informatikai irányítás tevékenységeihez kapcsolódó teljesítmény-mutatókat nyilvántartják és elemzik, amely vállalati szintű

javulásokat eredményez. Bár az eljárások mérhetőek, nem túlzottan kifinomultak, csupán a meglévő gyakorlatok formalizációi. Az eszközök szabványosak, és az aktuálisan rendelkezésre álló technikákra épülnek. A szervezet ún. Egyensúlyi Üzleti Eredménymutatókat (Balanced Business Scorecards.) alkalmaz. A képzettség megszerzése és a szabványok követése és alkalmazása azonban az egyénre van bízva. Kiváltó okokra irányuló elemzésére csak ritkán kerül sor. Az eljárások többségének működését bizonyos (alapvető) mérési mutatók alapján kísérik figyelemmel, de az esetleges eltéréseket, amelyek többségére bizonyos egyének kezdeményezése nyomán kerül sor, nem valószínű, hogy fel tudja deríteni a vezetés. Mindazonáltal a kulcsfontosságú eljárásokhoz kapcsolódó általános felelősségi körök világosak, és a vezetés díjazása a kritikus teljesítményi mutatók alapján történik.

4 (Irányított és mérhető)

A szervezet minden szintjén teljes mértékben tisztában vannak az informatikai irányításhoz kapcsolódó kérdések fontosságával, amelyet formális jellegű képzés is támogat. Világosan látják, hogy ki az informatikai eljárások vevője, és a felelősségi köröket szolgáltatási szintekre vonatkozó megállapodásokon keresztül határozzák meg és felügyelik. A felelősségi körök világosak, és minden eljárásnak megvan a maga gazdája. Az informatikai eljárások igazodnak az üzleti és az informatikai stratégiához. Az informatikai eljárások fejlesztése elsősorban kvantitatív megértésre alapul, és lehetséges az eljárásokra vonatkozó mérési mutatók szerinti mérés. Az eljárásokban érintett felek tisztában vannak a kockázatokkal, az informatika fontosságával és az általa kínált lehetőségekkel. A vezetés meghatározott bizonyos tolerancia-határokat az eljárások működésére vonatkozóan. Megfelelő válaszlépéseket eszközölnek az olyan esetek többségében, de nem minden esetben, ahol az eljárások láthatóan nem működnek megfelelő hatékonysággal illetve eredményességgel. Az eljárások fejlesztése alkalomszerű, és a legjobb belső gyakorlatok alkalmazását szorgalmazzák. A kiváltó okokra irányuló elemzések szabványos jellegűek. A szervezet elkezdett foglalkozni a folyamatos fejlesztés kérdésével. A technológia használata korlátozott, elsősorban taktikai jellegű, amely érett technikákra és szabványos eszközökre épül. Az összes érintett belső szakértő közreműködik az informatikai irányításban. Az informatikai irányítás szervezeti

szintű eljárássá fejlődik. Az informatikai irányításhoz kapcsolódó tevékenységek fokozatosan beintegrálódnak a szervezet-irányítási eljárásba.

5 (Optimális)

Az informatikai irányításhoz kapcsolódó kérdések és megoldások megértése és ismerete előrehaladott és előretekintő jellegű. A képzést és a kommunikációt innovatív koncepciókkal és technikákkal támogatják. Az eljárásokat külső normák alapján alakítják, a folyamatos fejlesztések és a más szervezetekhez viszonyított érettségi modellek eredményei alapján. Az alkalmazott szervezet-politika eredményeként a szervezet, az ott dolgozó emberek és az eljárások gyorsan tudnak alkalmazkodni az informatikai irányításhoz kapcsolódó követelményekhez, és teljes mértékben támogatják azokat. Minden probléma és eltérés esetén megvizsgálják a kiváltó okokat, és az elemzés eredménye alapján megfelelő intézkedéseket kezdeményeznek. Az informatikát kiterjedt, integrált és optimalizált módon használják fel a munkafolyamatok automatizálása és a minőség és az eredményesség javítása céljából. Meg vannak határozva az informatikai eljárások kockázatai és előnyei, és a szervezet egésze tájékoztatást kapott azokról. Külső szakértőket is igénybe vesznek, és viszonyítási normákat használnak útmutatásként. Az ellenőrzés, az önértékelés és az irányításra vonatkozó elvárások kommunikációja általános jellegű a szervezeten belül, és optimálisan használják fel a technológiát a mérések, az elemzések, a kommunikáció és a képzés támogatásához. A szervezet-irányítás és az informatikai irányítás stratégiai szinten kapcsolódnak egymáshoz, úgy, hogy a rendelkezésre álló technológiát, emberi erőforrásokat és anyagi erőforrásokat a vállalkozás versenyképességének javítását szem előtt tartva hasznosítják.

Az információbiztonsági és az informatikai irányítási helyzetfelmérések eredményeképpen az IBIR-t bevezetni szándékozó szervezetnek dokumentumban kell rögzítenie a helyzetfelmérés során megismert állapotokat, ún. audit vagy felülvizsgálati jelentést kell készítenie, melynek tartalmaznia kell a feltárt és beazonosított fenyegető tényezőket és az aktuálisan alkalmazott védelmi intézkedéseket, stratégiákat. Jelen dokumentum képezi az alapját a jövőben kialakítandó IBIR bevezetési koncepciójának, tekintettel arra, hogy a dokumentum tartalmazza mindazon hiányosságokat, melyek kezelése szükséges az IBIR kialakításához.

3.2 Vagyonleltár elkészítése

Az adatvagyonleltár célja, hogy a szervezet naprakész nyilvántartással rendelkezzen a védendő információs, szoftver és fizikai vagyonáról, azok tulajdonosáról (adatgazdájáról) és az egyes vagyonelemek értékéről. Miért is fontos ez? Mert úgy tudunk hatékony és megfelelő szintű védelmet kialakítani, ha pontosan ismerjük, hogy mit is kell megvédeni. Erre ad megfelelő választ egy szervezet tételes vagyonleltára. Egy szervezet vagyonleltárának az alábbiakat kell tartalmaznia:

a) ***Információ-vagyon:*** az adatok, adatbázisok, szoftver-kezelési kézikönyvek, oktatási, üzemviteli, üzemeltetési, biztonsági segédletek és nyilvántartások.
b) ***Szoftver-vagyon***: rendszerszoftverek, alkalmazói szoftverek, fejlesztő-eszközök és szolgáltatások.
c) ***Fizikai-vagyon:*** hardver (számítógépek, perifériák, mobil számítástechnikai eszközök), kommunikációs eszközök (telefonok, faxok, modemek, hálózati csatoló eszközök, telefon-alközpontok), adathordozók és egyéb műszaki berendezések (szünetmentes tápegység, légkondicionáló berendezés, villámhárító, stb.).

A vagyonleltár elkészítése során ezen vagyonelemek értéke kerül meghatározásra az egyes vagyontárgyak tulajdonosainak értékelése alapján. Az érték meghatározásának alapja az előre elkészített ún. kárérték táblázat (Lásd. **Hiba! A hivatkozási forrás nem található. Hiba! A hivatkozási forrás nem található.**). Az érték meghatározása során a vagyonelem tulajdonosa a vagyonelem sérülése esetén a következményeként a szervezetet érő kárt határozza meg. A vagyonleltár eredménye egy tételes lista (leltár), mely megadja a feltérképezett vagyonelemeket és azok értékét, mely dokumentum elengedhetetlen fontosságú az Informatikai Biztonsági Irányítási Rendszer bevezetése érdekében.

A vagyonleltár elkészítéséhez fel kell mérni a szervezet által kezelt adatokat; azon papír alapú, vagy digitális adathordozókat, amelyeken a kezelt adatok megjelennek, valamint mindazon működési folyamatokat, amelyek az adatokat használják (Lásd. **Hiba! A hivatkozási forrás nem található. Hiba! A hivatkozási forrás nem található.**) Meg kell nevezni az egyes vagyonelemek tulajdonosát, azon személyeket, akik a vagyonelemért felelősek, illetve akik jogosultak meghatározni a vagyonelem értékét. A vagyonelem értékének meghatározása során azt kell mérlegelni, hogy milyen mértékű kárt szenvedne el a szervezet, ha a vagyonelemek bizalmassága, sértetlensége, rendelkezésre állása sérülne. A

vagyontárgyak értékének meghatározása alapján történik a vagyontárgyak, és az azokat tároló/feldolgozó informatikai eszközök védelmi igényének meghatározása.

A vagyonleltár elkészítéséhez a szervezet működési folyamatát kell végigkövetni, és rögzíteni minden olyan vagyonelemet, amelyeken az üzleti folyamatok ellátásához megjelennek a kezelt adatok, illetve az adatok feldolgozási folyamatait és tevékenységeit. A vagyonelemek meghatározásánál általánosságban elmondható, hogy csak olyan részletességig érdemes a felmérést végrehajtani, ahol még elválik a vagyonelem tulajdonosának személye, az elszenvedhető kár mértéke, vagy a hozzáférés módja.

A vagyontárgyak értékét az adott vagyonelemért felelős személyek, az adatgazdák jogosultak meghatározni. Ilyenkor minden esetben azt kell mérlegelni, hogy milyen jellegű következményei lehetnek annak, ha a vizsgált vagyonelem bizalmassága, sértetlensége, rendelkezésre állása sérül, és ezek a következmények mekkora kárt okozhatnak a szervezetnek. Az adatgazdának nem kell azzal foglalkoznia, hogy milyen módon (technikailag hogyan) sérülhetnek a biztonsági kritériumok (bizalmasság, sértetlenség, rendelkezésre állás), csak azt kell mérlegelnie, hogy milyen következményekkel jár, ha megtörtént a biztonsági kritériumok sérülése. A kárérték meghatározásánál mindig a legrosszabb esetre kell felkészülni.

Ahhoz, hogy a vagyontárgyak értéke az egész szervezetre egységes képet adjon, a felmérést a szervezetre vonatkozó egységes kárérték szintek kialakításával kell kezdeni. A kárérték szintek meghatározásához segítséget nyújthatnak az IBIK 7.2.1.-es pontjában definiált kárérték szintek. Az egységes kárérték szintek elkészítésekor a szervezet vezetői megnevezhetik a releváns (egymástól független) kártípusokat (pl.: közvetlen anyagi kár, társadalmi / politikai hatás, törvényi következmény, dologi kár, személyi kár), és az egyes kártípusok esetén a kárérték skála elemeit (amelyek kártípusonként függetlenek lehetnek egymástól). A végleges kárérték szintekhez felsővezetői jóváhagyás szükséges.

A végleges kárértékszintek kialakítását követően az adatgazdáknak a szervezet egységes kárértékszintek alapján kell besorolniuk a vagyontárgyak értékét úgy, hogy a legsúlyosabbnak ítélt következmény kárértékét kell a vagyonelemhez rendelni.

A vagyonleltár elkészítésnél az alábbi pontokra érdemes hangsúlyt fektetni, továbbá a felmérés során kinyert plusz információkat rögzíteni a dokumentációban:

a) Meg kell határozni az adott adatgazda felelősségi körébe tartozó vagyonelemek körét;

b) Meghatározni a vagyonelemek biztonsági besorolását (nyilvános, üzleti titok, titkos, nagyon titkos);
c) Kárértéket kell meghatározni, ha a vagyonelem bizalmassága, sértetlensége vagy rendelkezésre állása sérülne;
d) A feldolgozás kritikus időszakait;
e) A kiesési időt kell meghatározni, azaz mennyi ideig tolerálható az, hogy a vagyonelemhez nem képes a felhasználó hozzáférni;
f) Az információt feldolgozó alkalmazást nevesíteni kell;
g) A vagyontárgy lehetséges fenyegető tényezőinek felmérését és regisztrálását kell végrehajtani;

A felmérését követően meg kell határozni az egyes vagyonelemek közötti kapcsolatokat, majd a kapcsolódásokat függőségi mátrixban ábrázolni. A függőségek erősségének meghatározásánál törekedni kell a súlyozásra, ezzel is jelezve, hogy milyen szoros kapcsolat áll fenn az egyes adatok között.

A függőségek és kárértékek meghatározása után rangsort lehet felállítani a szervezet számára kritikus vagyonról, továbbá meg lehet határozni, hogy az egyes vagyonelemeket kitől és mitől kell megvédeni.

A vagyonleltár elkészítését követően a szervezetnek rendelkeznie kell a szervezet egészét átfogó vagyontérképpel, vagyonleltár dokumentummal, továbbá a szervezet által meghatározott kritikusnak tekintett vagontárgyak körével. Ezen ismeretek alapvetően fontosak ahhoz, hogy a szervezet a későbbiek során végre tudja hajtani kockázatelemzését, és annak hatására a szükséges védelmi intézkedések bevezetését.

3.3 Kockázatfelmérés (Fenyegetettség- és sebezhetőség-elemzés)

A vagyonleltár elkészítését követően a szervezetnek el kell készítenie a vagyonelemeket érintő kockázatok felmérését. Olyan módszertant kell kialakítania a szervezetnek, mely illeszkedik az IBIR-hez, valamint a működés meghatározott információbiztonsági, jogi és szabályozási követelményeihez. A választott kockázatfelmérési módszertant úgy kell kialakítani, hogy az biztosítsa a kockázatfelmérések során született eredmények összehasonlíthatóságát és megismételhetőségét. A kockázatok felmérése érdekében a szervezetnek fenyegetettség- és sebezhetőség-elemzést kell végrehajtania. A fenyegetettség- és sebezhetőség-elemzés során végre kell hajtani a vagyonelemeket feldolgozó informatikai

erőforrások feltérképezését és összerendelését az egyes vagyonelemekkel, továbbá végrehajtani az erőforrások sebezhetőség-vizsgálatát.

Az informatikai infrastruktúra sebezhetőségének vizsgálatát el kell végezni

a) a fizikai biztonság,
b) a logikai biztonság,
c) a szervezeti biztonság

részterületekre.

A vizsgálat során össze kell gyűjteni a szervezet informatikai erőforrásait, majd a kritikus információkat az erőforrásokhoz kell rendelni. A sebezhetőség-vizsgálatot a kritikus vagyonelemek feldolgozásában részt vevő minden informatikai erőforrásra el kell végezni!

Az egyes részterületek sebezhetőségét különböző módszerekkel lehet meghatározni:

Szervezet, személyek esetén át kell vizsgálni a meglévő dokumentumokat, továbbá személyes interjúkkal meg kell győződni arról, hogy a munkavállalók mennyire ismerik az előírásokat, értékelni kell az alkalmazottak biztonságtudatosságának jelenlegi szintjét.

Sebezhetőségnek kell tekinteni:

a) a hiányzó dokumentumokat,
b) a létező, de a gyakorlatba be nem vezetett szabályzókat;
c) a nem megfelelő minőségű szabályzókat;
d) mindazon szabályokat, melyek végrehajtására nincsenek meg a személyi feltételek, valamint
e) minden olyan esetet, amikor összeférhetetlenség áll fenn a végrehajtandó utasítás és hozzárendelt felelős személy között (pl.: az adminisztrátor ellenőrzését az adminisztrátor önmaga végzi).

A **technológia** átvizsgálása összetett feladat. Egyrészt át kell vizsgálni az infrastruktúra dokumentációjának naprakészségét, amit adott esetben aktualizálni kell, másrészt javasolt a rendszer auditálását végrehajtani. Az átvizsgálás során külön vizsgálni kell, hogy a jelen pillanatban hatályos biztonsági előírások milyen módon és formában realizálódnak a technológiai elemeken.

A **fizikai biztonsággal** kapcsolatban léteznek-e védelmi intézkedések a hardver eszközök, berendezések, a központi számítógép és a gépterem fizikai meghibásodásának, károsodásának kiküszöbölésére (hidegtartalék eszközök, stb.); a számítógépekhez, gépteremhez, az egyéb eszközökhöz való hozzáférések korlátozására (zárt helyiségek, BIOS jelszó, billentyűzetzárolás, stb.); a jogosult hozzáférések regisztrálására, naplózására.

A **logikai biztonsággal** kapcsolatban léteznek-e védelmi intézkedések

a) a felhasználók azonosítására, hitelesítésére, valamint
b) a bejelentkezések ellenőrzésére,
c) a jelszavak, kulcsszavak kiadására, használatára, visszavonására és nyilvántartására;
d) a nem aktív felhasználók kiszűrésére;
e) a speciális jogosultságokkal, privilégiumokkal rendelkezők hozzáféréseinek nyomon követésére,
f) a sikertelen bejelentkezések figyelésére, naplózására;
g) a hozzáférés-biztonsági és jogosultsági rendszer kiterjed-e az alkalmazások, adat- és program-állományok, adatbázisok, tranzakciók kezelésének engedélyezésére, szabályozásának kialakítására és betartásuk ellenőrzésére.

A fenyegetettség és sebezhetőség elemzés végrehajtását követően a szervezetnek elő kell állnia, vagy aktualizálnia kell:

a) az informatikai infrastruktúrájának aktualizált logikai leírását;
b) az informatikai infrastruktúrájának aktualizált fizikai leírását;
c) a hálózat felépítését leíró dokumentációt;
d) az érintett rendszerelemek listáját;
e) az vagyonelemek és rendszerelemek függőségi mátrixát;
f) az informatikai erőforrások sebezhetőségeinek listáját;

3.4 Kockázatelemzés

A kockázatelemzés célja, a feltárt sérülékenységek és fenyegető tényezők között a kapcsolat kiépítése, a biztonsági sértések előfordulási valószínűségének meghatározása, az információvagyon biztonsági „kitettségének”, a szervezet által vállalható és nem-vállalható kockázatoknak a meghatározása.

Tekintettel arra, hogy a biztonság a tudatosan felvállalt kockázatokon keresztül realizálódik, a szervezet vezetőségének a kockázatok vállalására vonatkozó döntései alapján kell kidolgoznia védelmi rendszerét.

A kockázatelemzés során a szervezet feladata, hogy megvizsgálja, hogy az egyes feltárt fenyegetések milyen sebezhetőségen keresztül, milyen támadási forgatókönyv szerint képesek kifejteni hatásukat, azaz milyen összefüggés állítható fel. A leggyakrabban feltett kérdések:

a) Az adott támadási forgatókönyv mely sérülékenységeket kihasználva fejtheti ki tevékenységét?

b) Az információvagyon mely elemei sebezhetők a támadás által?
c) Mely kritérium sérül a támadás által (bizalmasság, sértetlenség, rendelkezésre állás);
d) Mi a legnagyobb valószínűsége annak, hogy ez a támadás bekövetkezik és eléri célját?
e) Az egyes információelemek ellen indított támadások közül melyiknek a legnagyobb a valószínűsége?

A gyakoriságok meghatározásához a szervezet felhasználhat különböző statisztikákat, melyek tartalmaznak bekövetkezési gyakoriságokat.

A fenyegetések valószínűsége és a sikeres fenyegetés által elszenvedhető kár mértéke alapján alapfenyegetettségenként el kell döntenie a szervezetnek, hogy az a szervezet számára elfogadható-e vagy sem, azaz eléri-e a vezetés által elfogadott és meghatározott kockázatkezelési szintet.

A kockázatelemzési módszer megválasztásában segítséget nyújt az IBIK 4.1.-es pontjában bemutatott kockázatmenedzsment módszertanok, melyek valamelyikének alkalmazásával a szervezet végre tudja hajtani az IBIR bevezetéséhez, működtetéséhez és fejlesztéséhez szükséges kockázatelemzést. A módszertan kiválasztása esetén törekednie kell a szervezetnek arra, hogy az alkalmazott módszertan illeszkedjen, és összhangban legyen a kialakítandó IBIR-rel, továbbá a vonatkozó egyéb jogszabályi és törvényi elvárásokkal szemben. Az alkalmazott kockázatelemzési módszertant, továbbá a kockázatelemzés során feltárt kockázatok kezelési módjának szabályait dokumentumban kell rögzíteni, melyről részletesebben a következő fejezetben szólunk.

A kockázatelemzés végrehajtását követően a szervezet rendelkezni fog az informatikai erőforrások sérülékenységeit kihasználó fenyegető tényezők listájával, valamint azok sebezhetőségekkel történő összerendelésével. Megismeri és meghatározza a feltárt fenyegető tényezők bekövetkezési valószínűségét, továbbá meghatározza az elfogadható és nem elfogadható, tehát a későbbiekben kezelendő kockázatok listáját.

3.5 Kockázatkezelés

A kockázatkezelési intézkedések célja azoknak a biztonsági kockázatoknak az elfogadható/méltányos költségen történő azonosítása, kézbentartása, minimalizálása vagy megszüntetése, amelyek hatással lehetnek az információs rendszerekre.

A kockázatkezelés során feltárt kockázatok kezelési lehetőségeit szabályzati szinten kell rögzítenie a szervezetnek, továbbá meg kell határoznia a kockázatkezeléssel kapcsolatos

feladatokat és felelősségeket. A kockázatkezelés során a szervezet az alábbi kockázatkezelési lehetőségeket alkalmazhatja:

a) Megfelelő **biztonsági intézkedések alkalmazása** a kockázatok csökkentése érdekében;
b) A **kockázatok tudatos, objektív felvállalása**, feltéve, hogy azok egyértelműen eleget tesznek a szervezeti politikának a kockázatelfogadási kritériumoknak;
c) A **kockázatok elkerülése** úgy, hogy a szervezet nem használja azokat a szolgáltatásokat, vagy eljárásokat, ahol az adott kockázatok előfordulnak;
d) A **kockázatok áthárítása** úgy, hogy a szervezet számára kockázatos szolgáltatásokkal, eljárásokkal kapcsolatos veszélyeket áthárítják másik felekre, pl. biztosítókra vagy beszállítókra

A szervezetnek meg kell határoznia, és ki kell alakítania kockázatkezelési folyamatát, melyhez meg kell teremtenie a szabályozási környezetet olyan formában, mely tartalmazza a kockázatkezelés során kötelezően elvégzendő lépéseket, a kapcsolódó feladatokat és felelősségeket. A kockázatkezelés során az alábbi tevékenységeket kell végrehajtania a szervezetnek:

a) Ki kell alakítania, és vezetői szinten kell elfogadnia az elfogadható kockázatok szintjét;
b) Ki kell választani a kockázatok kezelésére szolgáló kontrollokat;
c) Olyan kontrollokat kell bevezetni a kockázatok csökkentése érdekében, melyek összhangban állnak a kockázatfelmérés és elemzés során feltárt fenyegetésekkel és sérülékenységekkel.
d) A kockázatok kezelésére támpontot adnak az ISO 27001-es szabvány "A" mellékletében definiált szabályozási célok és intézkedések, melyek értelmezéséhez, és a gyakorlatban történő megvalósításához segítséget nyújt az ISO 27002 szabvány és/ vagy az IBIK.
e) A maradványkockázatok elfogadásához a szervezet vezetői szintű elfogadását kell biztosítani.

A szervezet által nem elviselhető kockázatok kezelésére ellenintézkedéseket vagy védelmi intézkedéseket kell foganatosítani. A kockázatok kezelésére bevezetett védelmi intézkedések meghatározzák (Lásd **Hiba! A hivatkozási forrás nem található. Hiba! A hivatkozási forrás nem található.**) a:

a) védelmi intézkedés célját;

b) végrehajtásért felelős személyek körét;
c) az ellenőrzéssel megbízott személyek körét;
d) az elvégzendő lépéseket, megadva az önellenőrzés szempontrendszerét; valamint
e) költségbecslést ad a védelmi intézkedés bevezetésére.
f) Javasolt a védelmi intézkedéseket végrehajtásuk fontossága alapján sorrendbe állítani. A nagyobb valószínűséggel bekövetkező fenyegetések, és az érintett vagyonelemek kárértékeinek alapján javasolt a szervezetnek mérlegelnie a kialakított védelmi intézkedések bevezetési sorrendjét. A sorrendet javasolt úgy meghatározni, hogy a nagyobb valószínűséggel bekövetkező és nagyobb kárt okozó események elleni védelmek kerüljenek elsősorban implementálásra.

A védelmi intézkedések kidolgozása során javasolt, megvizsgálni a bevezetéshez szükséges idő és erőforrás ráfordítást, továbbá a költséghatékonyságot. Célszerű csoportosítani a védelmi intézkedés javaslatokat funkciójuk és hatásuk alapján, mely csoportok lehetnek:

a) hibamegelőző (preventív),
b) hibaérzékelő (detektív) és
c) hibajavító (korrektív) kontrollok.

A felsorolt csoportokról részletesebben az „0. 5. Az Információbiztonsági Irányítási Rendszer ellenőrzése és felülvizsgálata”, továbbá a „0. 6. Információbiztonsági Irányítási Rendszer továbbfejlesztése és karbantartása” fejezetek szólnak.

A kockázatkezelés során bevezetett kontrollok, védelmi intézkedések, amennyiben teljes egészében nem szűntetik meg a kezelendő sebezhetőségeket, felvethetnek új fenyegetési lehetőségeket, esetleg az információbiztonsági rendszerben új sebezhetőségi pontok jelenhetnek meg, amelyek ún. maradványkockázatot hordozhatnak magukban. Emiatt a kockázatkezelés során figyelemmel kell kísérni a bevezetett kontrollok hatásosságát, és amennyiben maradványkockázatok realizálódnak, akkor szükséges azokat szabályozott formában kezelni, újra a döntéshozó személy vagy fórum elé terjeszteni, és dönteni a maradványkockázatok kezelési módjáról.

A kockázatkezelés eredményeképpen a szervezet számára rendelkezésre állnak a kockázatok kezelésére kidolgozott védelmi intézkedések, melyek tartalmazzák a bevezetéshez szükséges erőforrásokat, a védelmi intézkedés bevezetésének ütemezését, továbbá a várható költségeket. A meghatározott védelmi intézkedések bevezetésének priorizálását végre kell

hajtani, és a meghatározott prioritások alapján ki kell alakítani a védelmi intézkedések sorrendjét.

3.6 Alkalmazhatósági nyilatkozat

Az alkalmazhatósági nyilatkozat célja, hogy támpontként szolgáljon az Informatikai Biztonsági Irányító Rendszert ellenőrző auditor és a rendszerért felelős vezetők számára annak megállapításában, hogy az információ-feldolgozó rendszer milyen módon védett a vonatkozó kockázatok tükrében. Az alkalmazhatósági nyilatkozatot célszerű az alkalmazott kockázatelemzési eljárás által előállt kockázati szintek felhasználásával elkészíteni. A kockázati tényezők elemzése révén eldönthető, hogy a szabvány által javasolt védelmi intézkedések közül melyeket szükséges implementálni, melyek azok, amelyek csak részben szükségesek és mik azok a kontrollok, amelyek szükségességét nem indokolják a feltárt kockázatok.

Jelenleg több fajta – ám hasonló információtartalommal bíró – alkalmazhatósági nyilatkozat használata terjedt el. Azonban az IBIR bevezetése érdekében javasolt az ISO 27001-es szabvány által meghatározott alkalmazhatósági nyilatkozat elkészítése, mely tartalmazza a védelmi intézkedések tételes felsorolását és az egyes védelmi intézkedések bevezetésének helyét (a kapcsolódó szabályzat-dokumentum megnevezését). Az alkalmazhatósági nyilatkozat hatékony kezelésének érdekében célszerű az egyes védelmi intézkedések bevezetésének módját minél precízebben leíró (alacsony szintű) szabályzatot, végrehajtási utasítást meghivatkozni a dokumentumban, és nem a bevezetett kontroll tényleges leírását rögzíteni.

Az alkalmazhatósági nyilatkozatnak (Lásd **Hiba! A hivatkozási forrás nem található. Hiba! A hivatkozási forrás nem található.**) az alábbiakat kell tartalmaznia:

a) Kiválasztott szabályozási célokat, kontrollokat, valamint a kiválasztásuk indoklását
b) A bevezetésre kerülő szabályozási célokat és kontrollokat
c) Azon szabályozási célokat és kontrollokat, melyek kizárásra kerülnek (pl. nem értelmezhetőek az adott szervezetre), és azok indoklását.

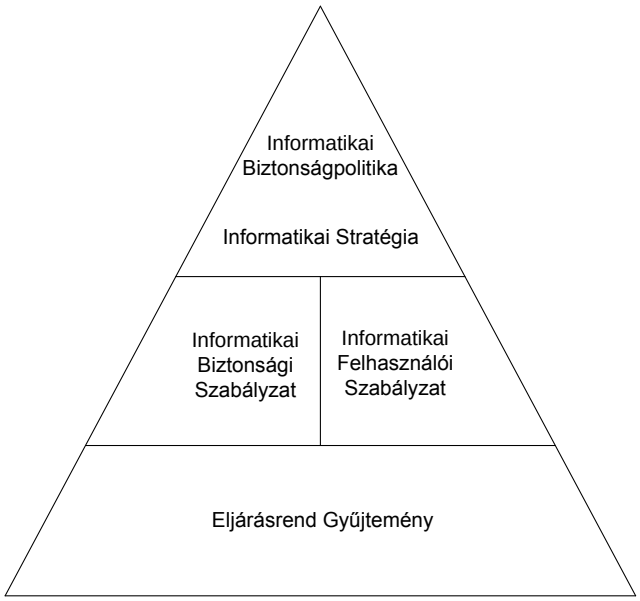
3.7 Szabályzati környezet kialakítása

Fontos, hogy az Informatikai Biztonsági Irányítási Rendszer egy jól dokumentált irányítási rendszer legyen.

Az IBIR dokumentációjának többek között tartalmaznia kell a következőket:

a) az Informatikai Biztonsági Irányítási Rendszert támogató eljárásokat és intézkedéseket;
b) a kockázatelemzési és kezelési követelményeket;
c) A hatékony tervezéshez szükséges intézkedéseket;
d) A bizonyítékok rögzítését.

Javasolt egy háromszintű szabályzati struktúra kialakítása, így biztosítható, hogy a szabályzat különböző (érzékenységű) elemeihez csak azok férjenek hozzá, akikre az adott szabályok vonatkoznak. Ezáltal nő a szabályzatok alkalmazhatósága, és lehetővé válik a bizalmas adatokat tartalmazó szabályzó dokumentumok zártkörű terjesztése. Egyszerűbbé válik a szabályzatok karbantartása, mert a hierarchia különböző szintjein lévő szabályzatokhoz rendelt felelősségek megoszthatók a szervezeti struktúra különböző szintjei között.



3.7.1 Az Informatikai Biztonsági Politika

A biztonsági célú tevékenységekhez szükséges megfelelő mértékű támogatás biztosítása érdekében az informatikai biztonságpolitikát a felső vezetésnek kell kiadmányozni (jóváhagyni), és a szükséges mértékben közzétenni. Az Informatikai Biztonsági Politika kinyilvánítja a menedzsment biztonság iránti elkötelezettségét, a biztonsági célt, valamint magas szintű biztonsági elvárásokat fogalmaz meg, amelyek a biztonsági cél elérését szolgálják, és amelyeket érvényesíteni kell a védelmi intézkedések specifikálása során. A

biztonságpolitika dokumentum elkészítésekor segítséget nyújthat az ISO 9000-es szabványban definiált minőségpolitika dokumentuma, tekintettel arra, hogy hasonló koncepció és elvárások szerint kell kialakítani a biztonságpolitikát természetesen az informatikai biztonsági irányelvek rögzítése mellett.

Az informatikai biztonságpolitikát úgy kell kialakítani és gondozni, hogy az a szervezet egyéb céljaival, továbbá működési, biztonsági és informatikai politikájával, valamint a biztonsági szabályozásokkal összhangban legyen.

Az informatikai biztonságpolitikát jelentősen befolyásolja az, hogy a szervezet miként alapozza működését az általa használt informatikára. Minél fontosabb az informatika, és minél inkább támaszkodunk rá, annál magasabb szintű biztonságra van szükség ahhoz, hogy garantáljuk a szervezet céljainak elérését. A szervezeti szintű informatikai biztonságpolitika kialakításakor figyelembe kell venni a környezeti, szervezeti és kulturális jellemzőket, mivel ezek befolyásolhatják a biztonság megközelítését.

Az informatikai biztonságpolitikában meghatározott, biztonsághoz kapcsolódó tevékenységek a következőkre alapozhatók: szervezeti célok és stratégia, korábbi kockázatfelmérések és vezetői ellenőrzések, valamint olyan kísérő tevékenységek eredményei, mint az alkalmazott biztosítékok biztonsági megfelelőségének ellenőrzése, az informatikai biztonsággal kapcsolatos napi gyakorlat folyamatos ellenőrzése és felülvizsgálata, továbbá a biztonsági eseményekről szóló jelentések. Bármilyen komoly fenyegetés vagy gyenge pont derül ki eközben, azt figyelembe kell venni az informatikai biztonságpolitikában. A részletezett tevékenységeket a szervezet informatikai biztonsági szabályzatában, a különféle informatikai rendszerszintű biztonsági politikákban, biztonsági szabályzatokban, vagy más kiegészítő-támogató dokumentumokban (például üzemeltetés biztonsági leírás) írjuk le.

Az informatikai biztonságpolitika kialakításakor a következő területek részvételére van szükség:

a) felsővezetés,
b) biztonság,
c) informatika (informatikusok és felhasználók),
d) belső ellenőrzés,
e) pénzügy,
f) épület- és egyéb infrastruktúrák üzemeltetői,
g) humán erőforrás menedzsment.

A biztonsági célok szabják meg az informatikai biztonságpolitika kívánt részletezettségi szintjét. Legalább a következő iránymutatásokat foglalja magában:

h) az informatikai biztonságpolitika kiterjedését és célját,
i) az informatikai biztonság meghatározását, általános célkitűzéseit és tárgykörét, valamint a biztonság fontosságát,
j) a vezetőség szándéknyilatkozatát, hogy támogatja az informatikai biztonság céljait és elveit,
k) az informatikai biztonság szervezési elveit, ide értve a szervezeti struktúrát, a személyi felelősségeket és hatásköröket,
l) a szervezet tulajdonában levő adatvagyon elemeinek érzékenységét, az ennek megfelelő védelmi szinteket, és a biztonsági osztályozási rendszert, továbbá – ha van ilyen – az osztályba sorolástól eltérő védelmi igényű adatkörök védelmére vonatkozó politikát,
m) a kockázatok felmérésére és kezelésére vonatkozó elveket,
n) a belső személyzettel és a külső partnerekkel kapcsolatos biztonságpolitikát,
o) az informatikai biztonsági ellenőrzés rendszerét,
p) az informatikai biztonsági feladatok megosztására vonatkozó elveket,
q) a biztonságpolitika változásának ellenőrzési eljárását és felülvizsgálatának körülményeit.

Az informatikai biztonságpolitikára alapozva egy kézikönyvet kell készíteni, mely hozzáférhető, érthető és kötelező az összes vezető és más munkavállaló számára. Ennek megismerését az aláírásukkal igazolják az érintettek, mellyel az aláíró elismeri a szervezeten belüli biztonságért való felelősségét. Ki kell fejleszteni, és alkalmazni szükséges egy programot a biztonságtudatosság fejlesztésére és az oktatásra e szempontok hatékony kommunikációjának érdekében.

3.7.2 Az Informatikai Biztonsági Stratégia

Az Informatikai Biztonsági Stratégia célja, hogy a szervezet üzleti igényeinek jövőbeni változásaival összhangban meghatározza az információbiztonság fejlesztésének tervét (középtávú, hosszú távú). Az Informatikai Biztonságpolitika alapján el kell készíteni a szervezet informatikai biztonsági stratégiáját, amely a biztonsági és az informatikai stratégiák szerves részét képezi. A stratégiát alapul véve kell az éves szintű terveket elkészíteni. A

jóváhagyott éves terv a beszerzési, beruházási és projekt-előkészítési tevékenységeket érintő intézkedési tervek összeállításának kiindulási alapja. Az információbiztonsági stratégia meghatározásánál a szervezetnek:

a) fel kell mérnie, ismernie kell a jelenlegi információbiztonsági helyzetét,
b) számba kell vennie mindazon biztonsági kihívásokat, melyekkel a közeljövőben számolnia kell, valamint
c) fel kell mérnie a biztonság területén lehetséges fejlesztési potenciálokat.

3.7.3 Az Informatikai Biztonsági Szabályzat

Az Informatikai Biztonsági Szabályzat rögzíti az IBIR működéséhez, működtetéséhez szükséges folyamatokat, megadja az érintett szereplők (pl.: információbiztonsági vezető, üzemeltető, rendszergazda, fejlesztési vezető, adatgazda stb.) feladatait, felelősségeit, hatásköreit. Rögzíti az információfeldolgozó rendszer elemeivel (dolgozók, alkalmazások, technológiai elemek, helyiségek stb.) kapcsolatos biztonsági követelményeket. Az Informatikai Biztonsági Szabályzatot olyan mélységig kell elkészíteni, hogy technológia-független tudjon maradni.

Az Informatikai Biztonsági Szabályzat elkészítése az elfogadott Informatikai Biztonsági Politika alapján valósul meg, nem hoz létre a szervezet működésétől független struktúrát és mechanizmusokat. Az Informatikai Biztonsági Szabályzat nem ismétli a kapcsolódó szabályzatok rendelkezéseit, azokra csak hivatkozik, azokkal összhangban fejti ki hatását. Az Informatikai Biztonsági Szabályzat elkészítése során szükség lehet a kapcsolódó dokumentumok módosítására, harmonizálására. Az Informatikai Biztonsági Szabályzathoz kapcsolódó dokumentumok három területet fednek le:

a) az irányítás területe, ahova beleértjük a Szervezeti és Működési Szabályzatot, a szervezeti ügymenet rendjét (Ügyrend), a munkavállalás rendjét, a titkos ügykezelés rendjét;
b) a technikai területe, ami magában foglalja az ügyiratkezelési szabályokat, az informatikai eszközök használatának szabályait, a selejtezési (megsemmisítési) sokszorosítási előírásokat, a biztonságtechnikai házirendet és rendészeti előírásokat;
c) egyéb speciális területek, mint a tűzvédelmi szabályzat, a munkavédelmi szabályzat, stb.

Az IBSZ rendelkezéseinek konkrét utasításokká történő kifejtését a Végrehajtási utasítások vagy Eljárásrendek tartalmazzák. Az IBSZ szerkezeti felépítésénél az IBIK tartalmi struktúrájának követése javasolt.

A szervezet Informatikai Biztonsági Szabályzatát a jogszabályokkal, a Biztonsági politikával és a szervezet más szabályzóival összhangban kell elkészíteni. Az Informatikai Biztonsági Szabályzat a biztonsággal kapcsolatos alapvető dokumentum, amelynek legalább az alábbiakra kell kitérnie:

a) a szervezet vezetésének egyértelmű nyilatkozata az informatikai biztonság szabályozott kialakítására, illetve fenntartására,
b) az informatikai biztonság alapvető fogalmaira,
c) az informatikai biztonsággal kapcsolatos feladat- és hatáskörökre, felelősségekre,
d) a biztonsági események jelentésének rendjére,
e) elvek, követelmények, kötelező eljárások, szabványok.

Az egyes informatikai rendszerek esetében a szervezet Informatikai Biztonsági Szabályzata alapján az adott alkalmazási területen megvalósítandó, a fejlesztéssel és az üzemeltetéssel kapcsolatos tevékenységeket kell részleteiben szabályozni.

3.7.4 Informatikai Felhasználói Szabályzat

A dokumentum részletesen szabályozza a felhasználók kötelességeit az informatikai eszközök használata során, meghatározza azokat a peremfeltételeket, melyek között a felhasználó kapcsolatot létesít az informatikai osztállyal, vagy az adatgazdákkal. A szabályzat részletesen kifejti a felhasználó által elvégezhető és tiltott tevékenységeket, megadja a számonkérés formáját és módját, rögzíti a biztonsági események jelentésével kapcsolatos kötelezettségeket.

E szabályzat képezi alapját a felhasználói oktatásoknak, melyeken a felhasználóknak kötelességük részt venni és aláírásukkal elfogadni, hogy a szabályzat tartalmát megértették, magukra nézve kötelezőnek tekintik.

3.7.5 Eljárásrend Gyűjtemény

Az eljárásrend gyűjteménybe tartozó végrehajtási utasítások olyan alacsony szintű szabályzatok, amelyek részletesen, rendszer specifikusan rögzítik azokat a tevékenységeket, melyeket az informatikai biztonsági szabályzat rendszerfüggetlenül megkövetel. Az eljárásrend kidolgozása az adott szakterület vezetőjének kötelessége, melyet hatályba léptetés

előtt az informatikai biztonsági tevékenységek koordinálásával megbízott vezetőnek (pl. az informatikai biztonsági felügyelőnek) el kell fogadnia. Az Informatikai Biztonsági Szabályzat rendelkezik az egyes szabályzati pontokhoz kötött eljárások kidolgozásáról és az adott eljárás részletes kidolgozásért felelős szervezeti egységről.

Az elkészült eljárásrendeket új munkaerő belépése esetén csatolni lehet a munkaköri leíráshoz, viszont mivel bizalmas információkat tartalmaz minden egyes végrehajtási utasítás és eljárásrend, ezért biztosítani kell, hogy csak azok férjenek hozzá, akinek munkaköri kötelessége az adott tevékenységek elvégzése és/vagy ellenőrzése.

3.8 Dokumentációk és jegyzőkönyvek kezelése

A dokumentációk és jegyzőkönyvek kezelésére, védelmére, felügyeletére vonatkozó követelményeknek megfelelő eljárásokkal kell biztosítani a dokumentációk és jegyzőkönyvek védelmét és felügyeletét. Ennek fontos része, hogy a kockázatelemző eljárásokkal párhuzamosan kell meghozni az egyéb információvédelmi intézkedéseket.

Az események vizsgálata különösen fontos része az információbiztonságnak. Amikor biztonsági esemény történik, fontos hogy foglalkozzunk annak időszerűségével, prioritásával és súlyosságával. Általában bizonyíték szükséges, hogy foglalkozzunk az eseménnyel, a legmegfelelőbb módszer, ha rögzítjük, hogy:

f) mikor és hol történik,
g) milyenek a körülmények,
h) ki mit csinált,
i) és mi az eredménye.

Fontos az esemény rögzítése és a bizonyítékok megőrzése. Természetesen bűncselekmény esetén a bizonyítékok gyűjtése, valamint megőrzése törvényi követelmény. Ezért nem csak az a fontos, hogy megőrizzük a jegyzőkönyveket, hanem ezek védelmét, sértetlenségét és bizalmasságát is biztosítani kell.

Az Informatikai Biztonsági Irányítási Rendszer dokumentációkra és jegyzőkönyvekre vonatkozó követelményei összhangban kell, hogy legyenek, meg kell, hogy feleljenek más irányítási rendszerek követelményeinek is, különösen a minőségirányításra vonatkozó ISO 9001 szabványnak. Ez számos előnyt jelent a szervezet számára: elősegíti az egységesített kombinált vizsgálatokat, kevesebb erőforrást igényel a rendszerdokumentációk és a jegyzőkönyvek kezelése, ezáltal zavartalanul és egységesen kezelhetők az üzleti értékek.

3.9 A vezetés elkötelezettsége

Fontos, hogy a vezetés bizonyíthatóan felelősséget vállaljon az Informatikai Biztonsági Irányítási Rendszerrel kapcsolatos tevékenységekért, ideértve annak létrehozását, bevezetését, működtetését, ellenőrzését és felülvizsgálatát, továbbfejlesztését és karbantartását.

A konkrét felelősségek a következők:

a) az Informatikai Biztonsági Szabályzat elkészítése;
b) a célok, a hatás- és felelősségi körök meghatározása,
c) folyamatos kapcsolattartás a biztonsági vezetés és az üzleti vezetők között,
d) gondoskodás az IBIR működéséhez szükséges erőforrásokról,
e) az üzleti szempontból elviselhető kockázatok szintjének meghatározása.

Az informatikai biztonság olyan felelősség, amelyen a vezetés valamennyi tagja osztozik. Ezért kellő elkötelezettséggel és a szükséges erőforrások rendelkezésre bocsátásával kell, hogy a vezetés támogassa az informatikai biztonságot. Ennek a testületnek olyan embereket kell magába foglalnia, akiknek megvan a követelmények azonosításához, politikák kialakításához, biztonsági programok írásba foglalásához, a munka értékeléséhez és az Informatikai Biztonsági Vezető irányításához szükséges képessége. A hatékony működéshez szükséges, hogy a fórumnak legyenek olyan tagjai is, akik komolyabb háttérrel rendelkeznek a biztonság és az informatikai rendszerek műszaki területén, de olyan tagjai is, akik az informatikai rendszerek, mint szolgáltatások nyújtásában, valamint felhasználásában vesznek részt. Mindezen területek tudására és tapasztalatára szükség van.

A felső vezetés hatáskörébe tartozik**:**

a) javaslattétel az informatikai vezető testület számára a stratégiai tervezéshez,
b) az informatikai biztonsági irányelvek és feladatok vizsgálata és jóváhagyása, a megvalósításhoz szükséges humán és anyagi erőforrások biztosítása,
c) az információs erőforrások súlyos veszélyhelyzeteknek való kitettségében bekövetkező jelentős változások nyomon követése,
d) az informatikai biztonsági események nyomon követése,
e) az informatikai biztonság fokozását szolgáló jelentős kezdeményezések jóváhagyása,
f) az Informatikai Biztonsági Vezető személyének kijelölése, feladat- és hatáskörének meghatározása.

3.10 Az informatikai biztonsági feladatok megosztása

Tisztán és pontosan, azaz egyértelműen kell meghatározni a szervezet értékei védelmének és a biztonsági folyamatoknak a felelőseit.

Az informatikai biztonságpolitika általános, az Informatikai Biztonsági Szabályzat részletes iránymutatással szolgáljon az egész szervezetben a biztonsági feladatokra, felelősségekre és hatáskörökre.

Az Informatikai Biztonsági Vezető felelőssége az informatikai biztonság megtervezése és fenntartása, de emellett az erőforrások megszerzése és a védelmi intézkedések megvalósítása gyakran más vezetőkre hárul.

Pontosan meg kell meghatározni minden olyan területet, amelyért az egyes vezetők felelnek, és különösen a következőket ajánlatos megtenni:

a) pontosan kell azonosítani, és egyértelműen meghatározni minden egyes önálló rendszerhez hozzárendelt eszközt és folyamatot,
b) az egyes eszközökért és az egyes folyamatokért felelős vezető személyében ajánlatos megegyezni, a vonatkozó felelősséget ajánlatos írásban foglalni (dokumentálni),
c) tisztán és pontosan kell meghatározni a hatásköröket (jogosultsági szinteket), és ezt írásba kell foglalni (dokumentálni).

3.10.1 Biztonsági Vezető

Gondoskodik az informatikai biztonságra vonatkozó jogszabályok, illetve az informatikai biztonságpolitika, az informatikai stratégia és az Informatikai Biztonsági Szabályzat végrehajtásáról, e körben szabályozási koncepciókat, szabályzat tervezeteket készít, a szakterületek megkeresésére vagy saját hatáskörben szakmai állásfoglalást ad ki.

Az informatikai biztonság szempontjából véleményezi a szervezet szabályzatait és szerződéseit.

Az informatikai biztonságot érintő jogszabályi változások, és a gyakorlati tapasztalatok alapján javaslatokat készít az informatikai biztonságpolitika, az informatikai stratégia és az Informatikai Biztonsági Szabályzat módosítására, szükség esetén kezdeményezi új szabályozások kibocsátását.

Gondoskodik az informatikai biztonságra vonatkozó rendelkezések betartásának rendszeres (legalább évente egyszeri) ellenőrzéséről, a lefolytatott ellenőrzések, vizsgálatok eredményéről tájékoztatja a szervezet vezetését.

Irányítja és ellenőrzi az Informatikai Biztonsági Vezető munkáját.

3.10.2 Informatikai Biztonsági Vezető

Általános feladata a szervezet (szakterület, projekt, rendszer) által üzemeltetetett, illetve a szervezet (szakterület, projekt, rendszer) adatait feldolgozó informatikai és távközlési rendszerek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtése és fenntartása, ennek tervezése, szervezése, irányítása, koordinálása és ellenőrzése.

Feladatai:

a) Felméri és elemzi a szervezet (szakterület, projekt, rendszer) működéséből eredő, az informatikai biztonsággal összefüggő veszélyforrásokat, meghatározza a kockázatkezelés módszerét.
b) Kidolgozza, és döntésre előterjeszti az informatikai biztonság kialakítására, a megfelelő informatikai biztonság elérésére, illetve fenntartására vonatkozó szabályokat, utasításokat, terveket és irányelveket.
c) Részt vesz:
    1) a rendkívüli események kezelésére szolgáló tervek elkészítésében, azok naprakészen tartásában;
    2) a fizikai biztonsági feltételek kialakításában, követelményeinek meghatározásában;
    3) az informatikai biztonság szempontjából fontosnak minősített munkakörök betöltési szabályainak, feltételeinek meghatározásában;
    4) a biztonsági követelmények és az előírások betartásának ellenőrzésében.
d) Szakmai szempontból közvetlenül irányítja a szervezet (szakterület, projekt, rendszer) informatikai biztonsági tevékenységét.
e) Szakmai szempontból irányítja az informatikai biztonságra vonatkozó oktatást.
f) Szakmai szempontból egyezteti és jóváhagyja a szakterületi (a projekt- és rendszerszintű) Informatikai Biztonsági Szabályzatokat.

g) Elemzéseket végez, szükség esetén javaslatokat tesz a szükséges informatikai biztonsági intézkedésekre, valamint a biztonságos működéssel összefüggő szabályok megváltoztatására.
h) Ellenőrzi az informatikai biztonsági előírások végrehajtását.
i) Ellátja az informatikai biztonsággal összefüggő vállalkozók szakmai irányítását, ellenőrzi tevékenységüket.
j) Ellátja a szakterületi (projekt, rendszer) Informatikai Biztonsági Vezetők szakmai irányítását.

Külön felhatalmazás nélkül jogosult:

a) Az ellenőrzési, vizsgálati tevékenysége során a szervezet (szakterület, projekt, rendszer) tulajdonában, használatában vagy a területén lévő, illetve a szervezetre (szakterületre, projektre, rendszerre) vonatkozó bármilyen (a Titokvédelmi törvény hatálya alá nem tartozó) iratba, dokumentumba, okmányba, adatbázisba, számítógépes vagy más adathordozó tartalmába való betekintésre.
b) A szervezet (szakterület, projekt, rendszer) tulajdonában lévő, vagy általa bérelt épületben és azon belül minden – a szervezet (szakterület, projekt, rendszer) tulajdonában, kezelésében vagy használatában lévő – helyiségben a berendezések, különösen az informatikai és távközlési eszközök vizsgálatára.

Az informatikai biztonsági feladatok folyamatos végrehajtásának megkönnyítése érdekében a szervezet (szakterület) vezetője nevezzen ki, vagy bízzon meg Informatikai Biztonsági Vezetőt (megbízottat, felelőst) minden informatikai rendszerhez és projekthez (rendszerszintű fejlesztésekhez).

Feladatai a működési területén:

a) A biztonsági eszközök állapotának figyelemmel kísérése azok teljes életciklusában, javaslattétel azok cseréjére, bővítésére.
b) Részvétel az üzletmenet-folytonossági terv (katasztrófa-elhárítási terv) összeállításában.
c) A rendszerek biztonsági hiányosságainak, az informatikai biztonsággal összefüggő számítástechnikai, informatikai problémák jelentése a munkahely vezetőjének és az Informatikai Biztonsági Vezetőnek.

3.11 Erőforrások biztosítása

Az informatikai biztonságot jelentősen befolyásolja az, hogy a szervezet miként alapozza működését az általa használt informatikára. Minél fontosabb az informatika, és minél inkább támaszkodunk rá, annál magasabb szintű biztonságra van szükség ahhoz, hogy garantáljuk a szervezet céljainak elérését. A szervezeti szintű informatikai biztonságpolitika kialakításakor figyelembe kell venni a környezeti, szervezeti és kulturális jellemzőket, mivel ezek befolyásolhatják a biztonság megközelítését. A biztonságpolitika megvalósításához a szervezetnek biztosítania kell a megfelelő erőforrásokat az informatikai biztonsági követelmények megvalósításához.

4. Az Információbiztonsági Irányítási Rendszer bevezetése és működtetése

Az Informatikai Biztonsági Irányítási Rendszer bevezetéséhez a szervezet az alábbi lépéseket tette meg:

a) Felmérte jelenlegi helyzetét;
b) Felmérte a védendő értékeit;
c) Kockázatértékelést végzett;
d) Kialakította a szabályzati környezetét;
e) Létrehozta az IBIR működtetéséhez szükséges szervezetet;
f) Meghatározta a felelős személyek körét, azok feladatait, jogait és felelősségeit.

Ahhoz, hogy működő Informatikai Biztonsági Irányítási Rendszerrel rendelkezzen a szervezet, a fent leírt lépések végrehajtása során megfogalmazott kontrollokat érvényesítenie kell a napi működése során, be kell építenie a szervezet már meglévő folyamataiba, vagy szükség esetén új folyamatokat, eljárásokat kell kialakítania a teljesítésük érdekében.

Természetesen a kialakításra került IBIR működtetése a napi gyakorlatban kihívások elé állítja a szervezetet, főleg a kezdeti időszakban, mikor az új folyamatok megismerését és a gyakorlatban történő alkalmazását a működtetésért felelős személyeknek el kell sajátítaniuk, és be kell építeniük a napi tevékenységeik közé. Emiatt a bevezetési időszakban a szervezetben nemcsak a végrehajtói és alkalmazói oldalon merülnek fel új feladatok, hanem a szabályzatok és az azokban megfogalmazott kontrollok létrehozásáért felelős személyekre és a munkavállalók feletteseire is hárulnak egyaránt. Az IBIR bevezetése és működtetése kapcsán a vezetőkre háruló feladatok lehetnek:

a) A szabályok szükségességének tudatosítása a dolgozókban;
b) Az IBIR bevezetésének hatására megnövekedett feladatok és a bevezetett kontrollok magyarázata;
c) Folyamatos kommunikáció a beosztottakkal a bevezetett kontrollokkal kapcsolatban
    1) Végrehajthatóak-e a gyakorlatban az előírások?
    2) Szükséges-e plusz erőforrás a működtetéséhez?
    3) Szükséges-e a kontroll módosítása?

Ahhoz, hogy megbizonyosodjon a szervezet a bevezetett kontrollok működőképességéről, szükséges biztosítani a folyamatos ellenőrzést. Az ellenőrzési

tevékenységre a bevezetési időszakban javasolt nagyobb hangsúlyt fektetni, tekintettel arra, hogy az új szabályok következtében megnövekedett adminisztrációs és egyéb új feladatok miatt a munkavállalók felől ellenállásba ütközhet a vezetés. Az ellenőrzések végrehajtásával az IBIR-t kialakító szervezet feltárhatja azon részterületeket, melyek esetében az érvényesítendő kontrollok gyakorlati megvalósítása nehézségekbe ütközik. A problémás területek megismerését követően a szervezet módosíthatja a kapcsolódó kontrollokat, esetleg több erőforrást biztosít az előírt feladatok végrehajtására.

Annak érdekében, hogy a munkavállalók válláról a vezetés terhet vegyen le az IBIR bevezetése miatt, javasolt a szabályzatban megfogalmazott kontrollok bevezetésekor törekedni az automatizált megoldások alkalmazására. Automatizált megoldások alatt kell érteni azokat a jellemzően technológiai megoldásokat, melyek alkalmazásával felhasználói beavatkozás nélkül is ki lehet kényszeríteni a szabályzatokban megfogalmazott kontrollokat (pl. a szervezet központi spam és vírusellenőrzőt telepít a levelezőszerverre, mely elvégzi az automatikus szűréseket, ezáltal a felhasználók számára már a szűrt tartalom jut, el, nem szükséges egyedi döntéseket hozniuk a felhasználóknak arról, hogy megnyithatják-e a kapott állományt vagy nem).

A fentieket figyelembe véve az IBIR bevezetése és működtetése során az alábbi lépéseket kell minimálisan végrehajtania a szervezetnek:

a) Biztosítania kell a kialakított szabályzati környezetnek megfelelő működési környezetet.
b) Kockázatjavítási tervet kell kidolgoznia.
c) Az Informatikai Biztonsági Stratégiában lefektetett stratégiai célokat meg kell valósítani.
d) Biztosítani kell az IBIR személyi hatálya alá tartozó személyek megfelelő képzését, oktatását.
e) Biztosítania kell a keletkezett dokumentumok és feljegyzések megfelelő tárolását kezelését.
f) A személyzet körében alkalmassági vizsgálatot kell végezni.
g) Biztosítani kell az erőforrások megfelelő felhasználását.
h) Irányítani és működtetni kell az Informatikai Biztonsági Irányítási Rendszert
i) Fel kell készülnie a biztonsági események kezelésére.

4.1 Szabályzati környezetnek megfelelő működés kialakítása

Az IBIR kialakítása kapcsán a szervezet elkészítette háromszintű szabályzati struktúráját, melyben megfogalmazta a biztonság iránti elkötelezettségét, továbbá meghatározta mindazon követelményeket, melyek betartásával és betartatásával biztosítani tudja a vezetés által elvárt, és a kockázatokkal arányos informatikai biztonságot.

A szervezet a szabályzati rendszerében megfogalmazta mindazon elvárásait, melyek szükségesek az egyenszilárd és a kockázatokkal arányos védelmi rendszer megteremtéséhez. Ahhoz, hogy az adminisztratív védelmi intézkedések elérjék a kívánt hatásukat a szervezeten belül, azokat érvényesíteni kell a gyakorlatban. A gyakorlati megvalósítás során az alábbi lépéseket kell megtenni:

a) A működési folyamatokat a szabályzatokban és eljárásrendekben megfogalmazott követelményrendszernek megfelelően át kell alakítani úgy, hogy biztosítva legyen a hatékony és megfelelő munkavégzés;
b) Technológiai szinten meg kell valósítani és ki kell kényszeríteni a szabályzatokban megfogalmazott elvárásokat. Ehhez sok esetben informatikai eszközberuházásokra és munkaerőképzésekre lehet szükség, melyek elengedhetetlenek a hatékony és biztonságos működési környezet kialakításához;
c) A szabályzatokban és eljárásrendekben előírt nyilvántartásokat és dokumentálási kötelezettségeket folyamatosan és következetesen kell vezetni, azok meglétét rendszeres időközönként ellenőrizni. A nyilvántartások vezetése az IBIR működtetése során különös fontosságú, tekintettel arra, hogy az ellenőrzések kapcsán az ellenőrzést végző személy vagy auditor a szabályzatoknak megfelelő működés ellenőrzését elsősorban a vezetett nyilvántartások meglétével azok tartalmi ellenőrzésével hajtja végre.

Ahhoz hogy az IBIR rendszer fejlesztését a szervezet végre tudja hajtani, az IBIR bevezetésével párhuzamosan ki kell alakítani egy mérőrendszert, mellyel a bevezetett kontrollok hatékonyságát és hatásosságát tudja mérni és értékelni a szervezet. A mérési rendszert úgy kell kialakítani, hogy a kapott értékek összehasonlíthatók és a mérések megismételhetők legyenek.

4.2 Kockázatjavítási terv kidolgozása

A vezetésnek az IBIR kialakítása során végrehajtott kockázatelemzés és értékelés kapcsán meghatározott kockázatok kezelésére kockázatjavítási tervet kell kidolgoznia, melynek tartalmaznia kell a vezetés által kezelni kívánt kockázatok tételes listáját. A kockázatjavítási tervben szükséges rögzíteni a kockázatok kezeléséhez szükséges irányítási beavatkozások módját és formáját, a szükséges erőforrások meghatározását. A kockázatok gyakorlati kezelése kapcsán a kapcsolódó védelmi intézkedések bevezetésekor a tervben meg kell határozni a kapcsolódó felelősségi köröket.

A kockázatjavítási tervben kell a vezetésnek a szakmai területek képviselőivel közösen meghatároznia a feltárt kockázatok kezelési sorrendjét (priorizálását). A prioritások meghatározását sok tényező befolyásolhatja, azonban információbiztonsági szempontból javasolt azon kockázatok elsődleges kezelése, melyek bekövetkezése esetén az információvagyon esetleges sérülésénél a szervezetet ért kár mértéke a legmagasabb (kárérték táblázat alapján) értéket érheti el, továbbá a sérülékenységet kihasználó fenyegetések bekövetkezési valószínűsége a legmagasabb.

A kockázatjavítási terv jelöli ki és határozza meg a jövőben elvégzendő feladatokat, azaz a stratégiai célokat fekteti le.

4.3 Stratégia megvalósítása

A szervezet az Informatikai Stratégiájában rögzíti a kockázatjavítási tervben kijelölt feladatok végrehajtásának módját, a szükséges erőforrások, határidők és felelősök meghatározásával. Természetesen a stratégiai célok megvalósítása során az IBIR által szabályozott környezet szükség szerint módosuláson megy keresztül, mely szükségessé teszi az IBIR szabályozási és működési környezetének módosítását az új feltételeknek megfelelően. Tehát ebből is látható, hogy az IBIR nem egy statikus rendszer, hanem egy folyamatosan változó, és a környezeti feltételeket figyelembe vevő, és ahhoz igazodó rendszer. A stratégiai célok megvalósítása során a szervezetnek az alábbi lépéseket kell követnie:

Vezetés elkötelezettsége a stratégiai célok megvalósítása mellett: A stratégiában megfogalmazott célok a megfelelő szintű erőforrás rendelkezésre állásának hiányában nem kivitelezhetők, tehát vezetőségi támogatás, elkötelezettség szükséges a célok gyakorlatban történő megvalósításához.

Erőforrások rendelkezésre bocsátása: A fejlesztések és rendszermódosítások végrehajtásához elengedhetetlenek mind a humán, mind a technológiai és pénzügyi erőforrás ráfordítások. A vezetés és a szakmai szervezetek közös döntése alapján kell meghatározni, hogy az adott stratégiai cél elérése érdekében elegendőek-e, és megfelelő minőségben (szakmai hozzáértés) rendelkezésre állnak a belső erőforrások, vagy szükséges bevonni harmadik külső felet. Harmadik fél bevonása a stratégiai cél elérése érdekében számos biztonsági problémát is felvet, ezért a szervezetnek szerződéses szinten kell rögzíteni mindazon elvárásait, melyekkel biztosítani tudja a munkavégzés során a harmadik fél számára hozzáférhető szervezeti vagyon biztonságát. A szerződések biztonsági követelményeinek kialakítása során az IBIK 6.2-es fejezetében meghatározott irányelvek segítségre lehetnek.

Folyamatos figyelemmel kísérés: A fejlesztési és módosítási eljárásokat folyamatosan nyomon kell követnie a szervezetnek, esetleg a hosszabb időtávot átívelő fejlesztések esetén már a megvalósítás folyamán is szükség lehet hatékonysági és hatásossági mérésekre, melyek eredményeit figyelembe véve lehetősége nyílik a szervezetnek módosítani a fejlesztési-kivitelezési irányt az optimális megoldás elérése érdekében. Az egyes célok megvalósítását tervezni és ütemezni szükséges, továbbá a fejlesztési folyamatba ellenőrzési pontokat, mérföldköveket kell meghatározni, továbbá a sikerkritériumokat kell megfogalmazni.

Utólagos értékelés: A bevezetést követően a meghatározott sikerkritériumok teljesülésének vizsgálata szükséges, továbbá a stratégiai cél megvalósítását követően szükséges a szervezetnek utólagos kockázatelemzést végrehajtania, hogy megbizonyosodjon róla, hogy a bevezetett intézkedés, fejlesztés meghozta-e a várt eredményeket, és a rendszermódosításból fakadó esetleges maradványkockázatok feltárásra, majd a jövőben kezelésre kerüljenek.

A stratégiai célok kivitelezését dokumentált módon kell végrehajtani, tehát a megvalósítás során elkészített rendszerleírásoknak, jegyzőkönyveknek a dokumentumait meg kell őrizni úgy, hogy a visszakereshetőségük a belső szabályzókban meghatározott ideig biztosított legyen.

4.4 Képzési és tudatossági oktatások

A felhasználókat, a vezetőket és a vállalkozókat oktatásban kell részesíteni a saját feladatukkal kapcsolatban lévő szabályokról, feladatokról és az őket érintő információbiztonsági felelősségekről. A szervezetnek tudatosítania kell a felhasználókkal és a vezetőkkel, hogy az információbiztonság napról-napra fontos aspektusa az üzletnek. A

szervezetnek az alaptanfolyamok részeként tudatosító programokat kell szerveznie, beleértve az információbiztonság kezelését, és ki kell osztania azokat a jogokat, szabályokat és felelősségeket melyek az információbiztonsági feladatokkal kapcsolatosak. Alapszinten meg kell értetni az alapfeladatokat, például: jelszavak kezelése, alapvető fizikai biztonsági intézkedések, e-mail használati kérdések, vírusvédelem, és magasabb szinten: a tűzfalak konfigurálását, valamint az információbiztonságot érintő események kezelését.

Gondoskodni arról, hogy a felhasználók tudatában legyenek az informatikai biztonság fenyegetéseinek és gondjainak, és fel legyenek szerelve mindazzal, amire azért van szükség, hogy az informatikai biztonságpolitikában és más szabályzókban előírtakat szokásos napi munkájuk során betartsák. A felhasználók legyenek kioktatva a biztonsági eljárásokról és az adatfeldolgozó eszközök helyes használatáról a lehetséges biztonsági kockázat minimalizálása érdekében.

A felhasználóknak ismerniük kell a biztonsági felelősségüket, a biztonsági eljárások alkalmazását és az adatfeldolgozó lehetőségek korrekt használatát, hogy ezzel is a minimálisra csökkentsék a lehetséges biztonsági kockázatokat, és alá kell írniuk az erről szóló nyilatkozatot.

A felhasználói oktatás a biztonsági elképzeléseket is figyelembe vevő Képzési Terven alapul.

Az informatikai vezetőnek – az informatikai biztonságpolitika elveinek, valamint a saját hatáskörben meghatározott képzési elveknek megfelelően – a humánerőforrás-gazdálkodással, illetve a Biztonsági Vezetővel egyeztetve ki kell dolgoznia a Képzési Tervet.

A szervezet valamennyi munkatársát, és ahol szükséges, a harmadik fél felhasználóit is, megfelelő képzésben kell részesíteni a szervezet biztonsági szabályairól és eljárásairól. Ezeket az ismereteket rendszeresen naprakész ismeretek közlésével fel kell újítani. A képzés foglalja magába a biztonsági követelményeket, a jogi felelősséget, az üzleti óvintézkedéseket, valamint az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát. A képzést azelőtt kell lefolytatni, még mielőtt a felhasználók megkapnák a hozzáférési jogot (jogosultság) az informatikai rendszerekhez, vagy az adatokhoz.

Az oktatási és képzési dokumentáció, valamint a módszertani kézikönyv megfelelő fejezetei részletesen kell, hogy tartalmazzák a biztonsági oktatásra vonatkozó információkat.

Az általános biztonságtudatosítási képzés mellett, melynek mindenkire vonatkoznia kell a szervezetben, különleges biztonsági képzés is szükséges az informatikai biztonsággal

foglalkozó személyzet számára. A biztonsági képzés mélységének az informatikának a szervezeten belüli általános fontosságához kell igazodnia, és az adott szerep biztonsági követelményeinek megfelelően kell változnia. Amennyiben szükséges, sokkal kiterjedtebb oktatást, például egyetemi kurzusokon való részvételt is biztosítani kell. Egy informatikai biztonsági képzési programot kell kialakítani az összes biztonsághoz kapcsolódó igény lefedésére.

A különleges biztonsági képzésre küldendő személyzet kiválasztásakor a következőket kell figyelembe venni:

a) az informatikai rendszerek tervezésében és fejlesztésében kulcsszerepet játszó személyzet,
b) az informatikai rendszerek üzemeltetésében kulcsszerepet játszó személyzet,
c) szervezeti, projekt és rendszerszintű Informatikai Biztonsági Vezetők,
d) a biztonság adminisztrációjáért felelős személyzet, például a hozzáférés ellenőrzés vagy a címtár kezelés területén.

Minden esetben ellenőrizni kell, hogy a tevékenységekhez (projektekhez) szükséges-e különleges biztonsági képzés. Valahányszor olyan tevékenységek vagy projektek kezdődnek, melyek speciális biztonsági követelményeket támasztanak, biztosítani kell a megfelelő biztonsági képzési program kialakítását és lebonyolítását még a projekt indulása előtt.

Az informatikai biztonsági képzési program egyik legfontosabb célja a biztosítékok helyes kialakítása és használata. Minden szervezetnek az igényeknek és a létező, valamint a tervezett biztosítékoknak megfelelő módon ki kell alakítania a saját informatikai biztonsági képzési programját.

4.4.1 Miért is fontos a képzés?

Az IBIR bevezetése kapcsán számos új feladattal szembesül az IBIR hatóköre alá tartozó felhasználói kör, és sok esetben nem értik, hogy miért is van szükség az eddigi bevált munkavégzési gyakorlat változtatásán. Tekintettel arra, hogy a bevezetett védelmi intézkedések a kockázatelemzés hatására kerültek meghatározásra, a vezetés tényekkel alá tudja támasztani a módosítások szükségességét, melyről tájékoztatni kell a felhasználókat, és tudatosítani bennük, hogy pontosan miért is van szükség a működési folyamatok módosítására, esetleg bemutatni azokat az előnyöket, melyek támogatják a munkavállalót.

Az informatika rohamosan fejlődő ágazat, és számos új fejlesztés és technológiai változás jelenik meg nap, mint nap. Emiatt a rendszert működtető és használó munkatársak számára:

Szakmai képzéseket kell biztosítania a szervezetnek mely hatására az újonnan bevezetett rendszerek hatékony és biztonságos üzemeltetését és használatát kell biztosítani.

Biztonságtudatossági oktatásokat kell szervezni, tekintettel arra, hogy a fejlődés és változás számos új fenyegető tényezőt hordoz magában, melyek ismeretének hiánya nem jelenti azt, hogy nem is érintheti az adott szervezetet. Ennek érdekében a szervezet munkatársainak figyelmét fel kell hívni a releváns fenyegető tényezőkre, továbbá oktatni és tudatosítani kell bennük a megfelelő viselkedési formát a megelőzés és észlelés tekintetében.

4.4.2 A képzések hatásosságának mérése

Ahhoz, hogy a szervezet megbizonyosodjon az oktatások hatékonyságáról és hatásosságáról, utólagos ellenőrzési rendszert, folyamatot kell kialakítania. Ezen folyamat kialakítása során az oktatáson elhangzottak gyakorlati ellenőrzését kell megvalósítania a szervezetnek, mely történhet a tényleges munkafolyamatok helyszíni, személyes vizsgálatával, vagy utólagos tesztek és ellenőrző kérdések formájában. Ahhoz, hogy az oktatásokon elhangzottak betartását biztosítani tudja a szervezet, szükséges megalkotni az ellenőrző, és a szükség esetén alkalmazható szankcionáló rendszert. A folyamatos ellenőrzések és a szankcionálás lehetőségének alkalmazásával a szervezet dolgozói átérzik és felismerik az oktatásokon elhangzottak szükségességét, melynek megfelelően fogják végrehajtani napi munkafolyamataikat. A szabályok betartatásával válik biztosítottá a bevezetett védelmi intézkedések által várt biztonság megteremtése, mely elengedhetetlen az IBIR által meghatározott egyenszilárd védelmi rendszer működtetéséhez.

4.5 Feljegyzések kezelése

Ahhoz, hogy az IBIR rendszer vizsgálható, auditálható legyen, az IBIR-t kialakító és működtető szervezetnek dokumentumokkal kell alátámasztania a működési folyamatok gyakorlatban történő megvalósulását. Ezt a szervezet az oktatásokkal kapcsolatban úgy tudja biztosítani, hogy dokumentálja az oktatáson résztvevők körét, azok aláírásukkal igazolják a részvételüket, az elvégzett ellenőrzésekről jegyzőkönyvet vezetnek, továbbá a szervezet az oktatások anyagát megőrzi. Mindezen dokumentumokat a szervezetnek meg kell őriznie a

belső szabályokban foglaltakban megfelelően, továbbá biztosítania kell a visszakereshetőségüket esetleges felülvizsgálatok, ellenőrzések során.

4.6 Alkalmasság vizsgálata

Az emberi hibák, lopás, csalárd magatartás vagy a létesítmények és az eszközök nem megfelelő használata során fellépő, az előírások szándékos vagy véletlen megsértéséből eredő biztonsági kockázatokat mérsékelni kell, a következők szem előtt tartásával:

a) A biztonsági követelményeket a munkaerő-felvételnél, a szerződésekben, valamint az egyén foglalkoztatása során egyaránt érvényesíteni kell.
b) A munkaerő-felvételi eljárás során – törvényes keretek között – olyan vizsgálatokat kell lefolytatni, melyek egyértelmű képet adnak a jelentkező informatikai biztonság oldaláról tekintett alkalmasságáról, ez különösen fontos az informatikai biztonság szempontjából kiemelt fontosságú munkakörök esetén. Minden munkavállalónak, a rendszerek külső használóinak (a velük kötött szerződés alapján), alá kell írniuk egy titoktartási nyilatkozatot.
c) A munkavállalótól csak olyan nyilatkozat megtétele vagy olyan adatlap kitöltése kérhető, illetve vele szemben csak olyan alkalmassági vizsgálat alkalmazható, amely a személyiségi jogait nem sérti, a munkaviszony szempontjából lényeges tájékoztatást nyújthat, és ahhoz az érintett írásban hozzájárult.

4.6.1 Biztonsági követelmények érvényesítése a munkaköri leírásokban

Valamennyi munkaterületre részletes munkaköri leírást kell készíteni. A munkaköri leírásnak tartalmaznia kell az adott munkaterületre vonatkozó, a biztonsággal kapcsolatos követelményeket is a felelősség egyértelmű megjelölésével.

A funkcionalitásokat úgy kell meghatározni, hogy azok teljes terjedelmükben hozzárendelhetők legyenek a munkakörökhöz, és ezáltal el lehessen azokat határolni egymástól, hogy minden munkavállaló csak a szigorúan rá vonatkozó feladatot hajtsa végre.

Az informatikai biztonság szempontjából elengedhetetlen a humánerőforrás-gazdálkodási és biztonsági szakterületek folyamatos együttműködése a be- és kiléptetési folyamatokkal kapcsolatban.

A be- és kilépéskor a hozzáférési jogosultságokat is meg kell határozni, és azokat a kellő időben érvényesíteni kell.

4.6.2 Biztonsági átvilágítás

A munkatársak esetében ellenőrzést kell végezni a felvételi eljárás során. Ez foglalja magába:

d) az üzleti és személyi referenciák meglétét,
e) a felvételre jelentkező életrajzának ellenőrzését teljességre és pontosságra,
f) a legmagasabb iskolai végzettség (szakképzettség) megerősítését,
g) hatóság által kibocsátott azonosító iratot (személyi igazolvány vagy útlevél).

Államtitok vagy szolgálati titok kezelésének szükségessége esetén a nemzetbiztonsági ellenőrzés pozitív eredményéhez (NATO vagy EU biztonsági tanúsítvány) kell kötni az alkalmazhatóságot (véglegesítést).

A személyzeti politikát a humánerőforrás-gazdálkodás készíti el a biztonsági szegmensek figyelembe vételével. A személyzet biztonsági átvilágításáról külön szabályzatban kell részletesen intézkedni. Ennek mindenképpen ki kell térnie a munkavállaló referenciáinak értékelésére, az életrajz pontosságának és teljességének vizsgálatára, a szakképzettség, és az azt igazoló iratok meglétének ellenőrzésére, illetve az összeférhetetlenség fennállásának vizsgálatára.

4.6.3 Titoktartás

A titoktartási nyilatkozat (megállapodás) célja, hogy felhívja a figyelmet az adott információk bizalmasságára. A munkatársak az ilyen megállapodást alkalmazásuk feltételei tudomásul vétele keretében írják alá. Alkalmi munkaerőnek és a külső személynek, akikről a meglévő, a titoktartási megállapodást is tartalmazó szerződés nem intézkedik, külön titoktartási megállapodást kell aláírniuk, még mielőtt az adatokhoz, vagy az informatikai eszközökhöz hozzáférést nyernének.

A titoktartási megállapodást felül kell vizsgálni, amikor az alkalmazási feltételek megváltoznak, különösen pedig akkor, amikor egy-egy munkavállaló arra készül, hogy elhagyja a szervezetet, vagy ha a szerződés lejártának időpontja várható.

A titoktartási nyilatkozatról a szervezet sajátosságának megfelelő Titokvédelmi Szabályzatban kell részletesen intézkedni.

4.6.4 Foglalkoztatás feltételei

A foglalkoztatás alapvető biztonsági feltételei az általános és a munkakörre vonatkozó speciális biztonsági előírások megismerése, elfogadása, a titoktartási nyilatkozat aláírással történő elfogadása.

Az alkalmazás feltételei között ajánlatos megállapítani a munkatárs informatikai biztonsági felelősségeit. Ahol lehetséges (vezető beosztású, vagy más kiemelt munkakörök), ezek a felelősségek meghatározott időtartamra terjedjenek ki az alkalmazás megszűnése után is. Ebbe bele kell foglalni azokat az intézkedéseket, kötelezettségeket, amelyek akkor lépnek életbe, ha a munkatárs nem tartja be az előírt biztonsági követelményeket.

A munkatársak jogai és kötelességei, például a szerzői jogokra vagy a személyes adatok védelmére vonatkozóan, legyenek az alkalmazás feltételei közé sorolva. Ugyancsak ajánlatos belefoglalni a munkatársra vonatkozó adatok biztonsági osztályba sorolásának és kezelésének felelősségét. Az alkalmazási feltételekben szerepeljen, hogy ezek a felelősségek fennállnak a szervezet telephelyein kívül is, a munkatárs rendes napi munkaidején túl is, például az otthoni munkavégzés alatt is.

4.7 Gazdálkodás az erőforrásokkal

Az IBIR-t a szervezeti jogszabályi, törvényi, és működésbeli változások hatására egy folyamatosan változó rendszerként kell elképzelni. A rendszer változása szükség szerint erőforrás ráfordítást igényel. Ahhoz, hogy az IBIR fejlesztését, módosítását a szervezet végre tudja hajtani, ahhoz a vezetésnek biztosítania kell a megfelelő erőforrásokat (pénzbeli, humán, technológiai, stb.). Az erőforrások hiányában természetesen a szükséges szervezeti változások és működési folyamatok a gazdasági és piaci nyomás miatt megtörténnek, azonban az IBIR rendszer hozzáigazítása a megváltozott feltételeknek megfelelően annak módosítása és aktualizálása jellemzően nem történik meg. Az IBIR-t működtetők számára a szabályok plusz teherként jelennek meg ezért csak felsővezetői nyomás hatására, vagy a szükséges erőforrások biztosítását követően valósulnak meg a megkívánt szervezeti, működésbeli változások.

A vezetésnek az IBIR kialakításához, bevezetéséhez, működtetéséhez, felülvizsgálatához és fejlesztéséhez biztosítania szükséges a megfelelő erőforrásokat, mert hiányában a biztonság tekintetében megfogalmazott célok (biztonságpolitika) a gyakorlati érvényesítése kudarcra ítélt. Az IBIR bevezetése kapcsán a vezetésnek biztosítania kell

mindazon erőforrásokat, melyek szükségesek a bevezetett kontrollok gyakorlatban történő érvényesítése és működtetése érdekében.

4.8 Az Informatikai Biztonsági Irányítási Rendszer irányítása

A vezetésnek és az IBIR kialakítása kapcsán kijelölt felelősöknek az előírt feladatokat végre kell hajtaniuk, mellyel biztosítják az IBIR működését. Ahhoz, hogy az IBIR irányítása megtörténjen, az irányítást végző vezetésnek visszacsatolással kell rendelkeznie a bevezetett kontrollok működőképességéről, azok hatékonyságáról. Ehhez szükséges egy ellenőrző, mérő rendszer kialakítása melyről részletesebben az 0. „5. Az Információbiztonsági Irányítási Rendszer ellenőrzése és felülvizsgálata" fejezetben szólunk.

A vezetés a kapott információk alapján dönt a szükséges módosítási fejlesztési irányok meghatározásáról. A döntések hatására az IBIR folyamatos változáson, fejlődésen megy keresztül melyhez szükséges kijelölni fejlődési folyamatot, melyhez alapvetően szükséges az irányítási tevékenységek ellátása.

4.9 Biztonsági események kezelése

A szervezetnek olyan eljárásokat és belső folyamatokat kell kialakítania, melyek lehetővé teszik az esetlegesen bekövetkező biztonsági események észlelését, továbbá az irányítási rendszerben olyan belső szabályzókat kell létrehozni, mellyel biztosítottá válik a biztonsági események hatékony és gyors kezelése. A biztonsági események követelményrendszerének kialakítása során, és a gyakorlati megvalósítás kapcsán segítséget nyújt az IBIK 13-as fejezetében megfogalmazott követelménylista.

4.10 A Bevezetés kockázatai

Az IBIR bevezetése a fent leírtak alapján számos feladatot ró a bevezetést végrehajtó szervezetre. A bevezetés sikerességét számos tényező befolyásolhatja, melyek közül a legfontosabbakat kiemeljük. Ezen feltételek teljesülésének hiányában a szervezet nem, vagy csak részben képes bevezetni az IBIR-t, vagy a bevezetett rendszert nem képes a belső kontrolloknak megfelelően működtetni. Mik is ezek a pontok?

Vezetőségi elkötelezettség hiánya: A vezetőségi elkötelezettség hiányában a szabályok érvényesítését és betartását végző személyzet sem fogja érezni a bevezetett kontrollok szükségességét, nem érzik személyi felelősségüket a biztonságos működés elérése érdekében.

Erőforrások biztosítása: A rendszer bevezetéséhez szükséges erőforrások hiányában a tervezési és koncepcionális fázisban megálmodott és kialakított szabályozási környezet gyakorlati megvalósítására nem lesz lehetőség, tekintettel arra, hogy mind humán mind pénzügyi erőforrás ráfordítás szükséges a rendszer bevezetéséhez és folyamatos működtetéséhez.

Racionalizált végrehajtandó kontrollok bevezetése: A tervezési fázisban a kockázatmenedzsment eredményeképpen bevezetett kontrollok utólagos követése szükséges a gyakorlati megvalósítás során. Folyamatos kapcsolatot kell tartani az alkalmazó személyzettel, a kontroll gyakorlati alkalmazásának hatékonyságáról, kivitelezhetőségéről párbeszédet kell folytatni. Amennyiben a bevezetett kontroll a gyakorlatban nem érvényesíthető (túlzott terhet ró az alkalmazó személyzetre, vagy a rendelkezésre álló erőforrásokkal nem kivitelezhető, stb.) akkor szükséges a kontroll racionalizálását végrehajtani úgy, hogy a kontroll által kezelt kockázatokkal arányosan történjenek meg a módosítási lépések, és a kontroll gyakorlati megvalósítása biztosított legyen. Amennyiben ezen kérdések nem kerülnek kezelésre, az IBIR rendszer biztonságos működtetése kerül veszélybe.

Ellenőrző rendszer kiépítésének hiánya, ellenőrzések elmaradása: Az ellenőrző rendszer hiányában a bevezetést végző szervezet nem lesz tisztában az érvényesített kontrollok hatásosságában. Ezen visszacsatolás hiányában a szervezetben kialakulhat egy ún. hamis biztonsági érzet, továbbá nem nyílik lehetősége a szervezetnek a kockázatokkal arányos védelmi rendszer kiépítésére. Tekintettel arra, hogy ez az IBIR egyik alappillére, kiemelten fontos az ellenőrző és mérőrendszer kialakítása és működtetése.

5. Az Információbiztonsági Irányítási Rendszer ellenőrzése és felülvizsgálata

Az Informatikai Biztonsági Irányítási Rendszer ellenőrzése és felülvizsgálata során biztosítania kell a szervezetnek a rendszer bevezetési és működtetési szakaszában érvényesített kontrollok a meghatározott szabályok szerinti hatékony működését és működtetését. Ahhoz, hogy Informatikai Biztonsági Irányítási Rendszer hatékonyan kezelje a működtetés során azonosított biztonsági kockázatokat, biztosítani kell az Informatikai Biztonsági Irányítási Rendszer folyamatos ellenőrzését és a rendszert érintő összes változás nyomonkövetését.

A folyamatosan változó működési környezet hatására a szervezetet érintő fenyegetések folyamatos változásokon mennek keresztül, új fenyegetések jelenhetnek meg, ezáltal az Informatikai Biztonsági Irányítási Rendszert is fel kell készíteni a változó környezet hatásaira. Ezt figyelembe véve az Informatikai Biztonsági Irányítási Rendszer gyenge pontjai, sebezhetőségei folyamatosan változnak. Mik befolyásolhatják az Informatikai Biztonsági Irányítási Rendszer változását:

a) A szervezetet körülölelő, folyamatosan változó külső környezete:
    1) új partnerekkel történő kapcsolatok kialakítása,
    2) új beszállítói kapcsolatokat alakít ki,
    3) újabb piaci területek felé nyit a szervezet,
    4) változnak a piaci körülmények,
    5) harmadik fél bevonása üzleti tevékenységének végrehajtásába,
    6) távoli munkavégzés engedélyezése;
b) változik a szervezeti struktúra az átszervezések, bővítések és leépítések következtében;
c) változhat a szervezet stratégiai célja;
d) A technológia követése, és az alkalmazásából fakadó változások;
e) a jogszabályi környezet változása.

Az előzőekben felsorolt, a szervezetet érintő változások mindegyike valamilyen új sebezhetőségi pontot jelenthet a szervezet számára, mely újabb fenyegetéseket, és azokon keresztül újabb kezelendő kockázatokat jelenthet a szervezet számára. Emiatt csak úgy biztosíthatja az Informatikai Biztonsági Irányítási Rendszer hatékony működését a szervezet,

ha ezeket az új kockázatokat rendszeres időközönként újraértékeli, és a meghatározott kockázatmenedzsment módszertanát alkalmazva kezeli azokat.

Ellenőrzési és mérési eljárásokat kell kialakítania és működtetnie a szervezetnek, hogy:

a) megfelel-e az Informatikai Biztonsági Irányítási Rendszer meghatározott hatóköre,
b) a meghatározott feladatok és felelősségek újraértékelése szükséges-e,
c) Azonnal észlelni tudja a biztonsági eseményeket az IBIR és az üzleti folyamatok működése és feldolgozások működése kapcsán;
d) A szervezet dolgozói által végrehajtott napi tevékenységek megfelelnek-e a szabályzókban megfogalmazottaknak, tehát a tevékenységeiket az elvárások szerint hajtják végre;
e) Elősegítse a biztonsági események észlelését, mely hatására lehetőség nyílik megelőzni a tényleges biztonsági esemény bekövetkezését, az elszenvedhető kár mértékét csökkenteni lehet;
f) Feltárásra kerüljön az, hogy a bevezetett védelmi intézkedések beváltották-e a hozzájuk fűzött reményeket.
g) Az elkészített katasztrófaelhárítási és üzletfolytonossági tervek aktuálisak-e, és biztosítják biztonsági esemény esetén az elvárt működést.
h) Meghatározott időközönként felül kell vizsgálni a kockázatfelméréseket és elemzéseket, maradványkockázatokat és a meghatározott elfogadható, a szervezet számára elviselhető kockázati szinteket, figyelembe véve:
    1) A szervezetben;
    2) A technológiában;
    3) A működési célokban és folyamatokban
    4) Az azonosított fenyegetésekben
    5) A bevezetett intézkedések hatékonyságában; és
    6) A külső környezetben, pl. a jogi, szabályozási környezetben, szerződéses kötelezettségekben. történő változásokat.

A szervezetnek meghatározott időközönként belső auditokat kell végrehajtania annak meghatározására, hogy az IBIR szabályozási céljai, intézkedései, folyamatai és eljárásai:

a) Megfelelnek-e a vonatkozó jogszabályoknak, szabályozásoknak, esetleg szabványoknak;
b) Megfelelnek-e az azonosított információbiztonsági követelményeknek;
c) Bevezetése eredményes volt-e, és a működtetése megfelelően történik-e;

A belső auditokat tervezni szükséges, melyhez szükség szerint figyelembe kell venni az auditálandó folyamatok és területek állapotát, fontosságát, illetve a korábbi auditok eredményeit.

Az auditok során az auditáló személyzetnek és a végrehajtási folyamatnak biztosítania kell az auditálási folyamat tárgyilagosságát és pártatlanságát. Tehát olyan személyeket kell kijelölni melyek a vizsgálandó területtől függetlenek, pártatlanul képesek véleményt nyilvánítani.

Az ellenőrzési és felülvizsgálati tevékenységek végrehajtása során rendszeresen el kell végezni a vezetőségi felülvizsgálatokat: biztonsági vizsgálatokat, rendszerteszteket, a biztonsági események jelentéseinek a vizsgálatát, a rendszergazdák, üzemeltetők javaslatainak figyelembevételét. Mindezek biztosítják, hogy az IBIR megfeleljen az üzleti követelményeknek, és az információbiztonsági kockázatok az elviselhető szinten maradjanak.

5.1 Mérőrendszer kialakítása

A mérés igénye abból a megfontolásból adódik, hogy amit nem tud mérni a szervezet, annak nem tudja a változását megfigyelni, így nem tudja, hogy mikor és milyen irányban kell beavatkoznia a céljai elérése érdekében. A mérőrendszer kialakítása során a szervezetnek javasolt a COBIT Vezetői útmutatóban meghatározott Monitoring domainban felsorolt 4 fő területhez rendelt mérőszámok megismerése és használata, mely segítséget nyújthat a szervezet számára az Informatikai Biztonsági Irányítási Rendszer ellenőrző mérőrendszerének kialakításában. A szervezet mérőrendszerét úgy kell kialakítania, hogy a mérések megismételhetőek legyenek, és a kapott eredmények összehasonlíthatósága biztosított legyen. A mérőrendszer kialakításának előfeltétele annak, hogy a szervezet meghatározza azokat célokat és mérési módszereket, melyekkel el tudja végezni a méréseit. Ezek ismeretében már képes lesz mérni a folyamatait, tevékenységeinek hatékonyságát és hatásosságát. Milyen területek esetén javasolt a mérőrendszer kialakítása, továbbá milyen mérőszámokat lehet alkalmazni és bevezetni?

Informatikai mérések esetében:

a) Biztonsági események száma;
b) Rendszer rendelkezésre állási mérések;
c) Informatikai válaszidő mérése a megkeresésekre;
d) Meghibásodások számossága;
e) Felhasználói panaszok számossága;

IBIR folyamatok működésének mérése:

a) Korrekciós intézkedések száma
b) Védelmi intézkedésekben meghatározott határidők betartása
c) Védelmi intézkedések számossága
d) Kritikus területek számossága
e) Harmadik fél szolgáltatásainak igénybe vétele esetén az SLA szintek teljesítésének mérése
f) Szabályok megsértésének számossága
g) Biztonsági események számossága

5.2 Az informatikai biztonság ellenőrzése

Az informatikai biztonság ellenőrzésének alapvető célja, hogy **objektív információkat** biztosításon a felelős vezetők számára az informatikai biztonság helyzetéről, amelyek alapján a kockázatok csökkenthetők, és a rendkívüli események elkerülhetővé válnak.

Az informatikai biztonsági ellenőrzés célja az, hogy teljeskörűen, azaz minden informatikai rendszerre és azok teljes életciklusára (az előkészítéstől, a bővítéseken és módosításokon át, a rendszerből történő kivonásig) rendszeresen vizsgálja, hogy:

a) az informatikai rendszerek biztonsága megfelel-e a Szervezet által elfogadott biztonságpolitikának,
b) érvényesülnek-e a jogszabályokban, a szervezeti és a rendszer szintű biztonságpolitikákban és szabályzatokban foglaltak,
c) történnek-e az informatikai rendszerek, illetve az általuk nyújtott szolgáltatások biztonságát sértő események, illetve mekkora ezek bekövetkezési valószínűsége.

Az ellenőrzések során feltárt hiányosságok (a megállapításokat mindig írásos jelentésbe kell foglalni!) képezik azon védelmi intézkedések (adott esetben szankciók) alapját, amelyek szükségesek ahhoz, hogy *minimális legyen a védelmi képességek kívánt és valós szintje közötti távolság, ezért az ellenőrzések során tapasztalt hiányosságok megszüntetésére intézkedési tervet (javaslatot) kell kidolgozni, és azt meg kell valósítani.*

5.3 Az informatikai biztonsági ellenőrzések formái

Az ellenőrzésekkel szemben alapvető követelmény, hogy az alkalmazott módszer biztosítsa a tárgyszerűséget, a valósághű képet és a valós helyzet feltárását, ennek megfelelően az

ellenőrzések különböző formában valósulnak meg. Az ellenőrzések formáját annak típusa, jellege és szintje határozza meg.

Az informatikai biztonsági ellenőrzések típusai:

a) *informatikai biztonsági vizsgálat* (fenyegetettség, védelmi képesség elemzés kockázatelemzéssel),
b) *auditálás* (meghatározott követelményeknek való megfelelés vizsgálata),
c) *informatikai biztonsági tanúsítás és minősítés* (pl.: a Common Criteria, ISO 27001 követelményeinek való tanúsított megfelelés).

Az ellenőrzés eszközei:

a) személyes ellenőrzés,
b) megfigyelés,
c) információ bekérés,
d) dokumentumok vizsgálata,
e) technikai berendezések által rögzített adatok elemzése,
f) sebezhetőség-vizsgálat (vulnerability analysis)
g) behatolási tesztek (penetration testing) végzése
h) feladatlap kitöltése,
i) Folyamatelemzés.

Az ellenőrzések munkaszakaszai:

a) előkészítés,
b) felkészülés, helyszíni vizsgálat,
c) írásba foglalás,
d) hasznosítás, javaslatok (realizálás),

Az ellenőrzések jellegük szerint felosztatók:

a) tervezett és rendszeres ellenőrzésekre,
b) eseti vizsgálatokra,
c) biztonsági esemény kivizsgálásokra.

5.4 Az Informatikai Biztonsági Irányítási Rendszer vezetőségi vizsgálata

A vezetésnek felül kell vizsgálnia a szervezet Informatikai Biztonsági Irányítási Rendszerét a megvalósított ellenőrzési terv alapján. A felülvizsgálat lehetővé teszi a szervezet számára, hogy eldöntse, milyen javító változtatásokra van szükség az Informatikai Biztonsági Irányítási Rendszert illetően. Az ellenőrzési szakaszban kiemelten fontos az üzleti, a termelő

környezetet érintő változások figyelése és felülvizsgálata, valamint meg kell győződni arról, hogy az IBIR megfelelő védelmet biztosít ezekkel a változásokkal szemben. A helyzet felülvizsgálata után szükség lehet a biztonsági szabályok, eljárások, valamint technikai intézkedések hozzáadására, cseréjére és tökéletesítésére. Felülvizsgálat nélkül az Informatikai Biztonsági Irányítási Rendszer elavul, és hatástalanná válik az új kockázatok kezelésére.

Sokféle vizsgálati és felülvizsgálati módszer áll a szervezetek rendelkezésére, melyeket meg kell fontolni: az Informatikai Biztonsági Irányítási Rendszer belső auditja, külső szakértő által végrehajtott audit, vagy tanúsító szervezet által végrehajtott audit (ha a szervezetnek nem (üzleti) érdeke az informatikai biztonság tanúsítása, akkor az nem kötelező).

Fontos, hogy a vezetés megfelelő és helyes vizsgálati adatokkal rendelkezzen, és helyes döntéseket hozzon a megfelelő intézkedések foganatosításáról, mert ezek nélkül a vizsgálat hatástalan. Fontos, hogy a vezetés kísérje figyelemmel az Informatikai Biztonsági Irányítási Rendszer belső ellenőrzése során az informatikai biztonsági követelmények érvényre jutását.

A vezetőségi vizsgálat során, ahhoz hogy a döntéshozó testület megfelelő döntéseket hozzon, az alábbi információkkal kell minimálisan rendelkezni az IBIR hatékony irányítása érdekében:

a) a bevezetett IBIR-t érintő auditok eredményeiről;
b) a szakmai szervezetek, érintett felek visszajelzéseiről;
c) a bevezetett megelőző és korrektív védelmi intézkedések aktuális állapotáról, azok bevezetésének hatásosságáról;
d) a kockázatfelmérés során felvállalt, vagy maradványkockázatként feltárt kockázatokat, továbbá a kockázatkezelés során nem kezelt sebezhetőségi pontok és releváns fenyegetések listájáról;
e) a mérési és ellenőrzési rendszer eredményeiről;
f) a korábbi vezetőségi átvilágítás során tett intézkedésekről;
g) bármilyen az IBIR-t érintő változásról;
h) és a fejlesztésre vonatkozó javaslatokról.

A fent felsorolt információk birtokában a vezetés képes értékelni a működtetett IBIR jelenlegi állapotát, megismeri a kezelendő pontokat és területeket, melyek gyakorlati kezelésére meg tudja hozni a megfelelő döntéseket. Ezen információk birtokában a vezetés képes az IBIR:

a) hatásosságának fejlesztésére
b) a kockázatfelmérési, elemzési, kezelési tervek frissítésére

c) módosíthatja a működési eljárásokat, bevezetett kontrollokat;
d) biztosíthatja a szükséges erőforrásokat;
e) fejlesztheti a mérési és ellenőrzési folyamatokat.

5.5 Az informatikai biztonság független felülvizsgálata

Az informatikai biztonságpolitika megvalósulását ajánlatos időközönként független módon is felülvizsgálni annak érdekében, hogy megismerjük, hogy a szervezet gyakorlata hogyan képzi le az informatikai biztonságpolitikát, illetve annak hatékonyságát. Az informatikai biztonság megvalósulását független szakértőnek kell értékelnie. Ez lehet a Biztonsági Vezetőtől és az Informatikai Vezetőtől független belső ellenőrzés, vagy egy ilyen vizsgálatokra szakosodott független külső szervezet is.

Az informatikai biztonságpolitikában, informatikai biztonsági stratégiában, valamint az Informatikai Biztonsági Szabályzatban rögzítettek megvalósulását az Informatikai Biztonsági Vezető ellenőrzi. Ez az általános ellenőrzési jogkör nem mentesíti a szakterületek (projektek vagy rendszerek) vezetőit az alól, hogy az informatikai biztonság megvalósulását a beosztottaik munkavégzésének folyamatos vizsgálata során ellenőrizzék.

5.6 Megfontolások a rendszerek biztonsági ellenőrzésére

Cél maximalizálni a rendszert átvilágító auditálás hatékonyságát, és minimalizálni az általa vagy benne okozott zavarokat. Intézkedéseket kell alkalmazni az üzemelő rendszer védelmére, és hogy megóvjuk az auditálás alatt az auditáló eszközöket. Ugyancsak védelmet szükséges alkalmazni ahhoz, hogy megóvjuk az auditáló eszközök sértetlenségét, és megelőzzük a velük való visszaélést.

Az ellenőrzés egy folyamatos tevékenység, amely azt vizsgálja, hogy a rendszer és felhasználói, valamint a környezet fenntartja-e az informatikai biztonsági tervben meghatározott biztonsági szintet. Napi rendszerességű ellenőrzési tervet kell készíteni kiegészítő iránymutatásokkal és eljárásokkal a folyamatos biztonságos működés támogatására. A felhasználóknak, az üzemletetési személyzetnek és a biztonsági tervezőknek rendszeresen konzultálniuk kell annak érdekében, hogy az összes biztonsági célkitűzést kielégítsék, és az informatikai biztonsági terv naprakész maradjon.

Azon okok egyike, amelyek miatt az ellenőrzés olyan fontos az informatikai biztonság fenntartásában az, hogy ez egy út a biztonságot érintő változások érzékelésére. Néhány

szempont, amit ellenőrizni kell: az eszközök és értékük, az eszközökre irányuló fenyegetések és azok sérülékenységei és az eszközöket védő biztosítékok.

Az eszközöket az értékükben és az informatikai rendszerek biztonsági céljai változásának észlelése érdekében kell ellenőrizni. Ezeknek a változásoknak a lehetséges okai a következők: a szervezet céljai, az informatikai rendszerben működő alkalmazások, az informatikai rendszerben feldogozott információk és maguk az informatikai eszközök.

A fenyegetéseket és sérülékenységeket azért ellenőrizzük, hogy érzékeljük a változásokat súlyosságukban (például az infrastruktúrában, környezetben bekövetkezett változások okozhatják ezeket vagy technikai lehetőségek), és hogy korai szakaszban tudjunk érzékelni új fenyegetéseket vagy sérülékenységeket. Az eszközök változásai befolyásolhatják a fenyegetések és sérülékenységek változásait.

A biztosítékokat teljesítményük és hatékonyságuk vizsgálata érdekében ellenőrizzük időnként. Biztosítani kell, hogy megfelelőek legyenek, és az informatikai rendszert a szükséges védelmi szinten védjék. Lehetséges, hogy az eszközök, fenyegetések és sérülékenységek változásai befolyásolják a biztosítékok hatékonyságát és megfelelősségét.

Továbbá, ha új informatikai rendszereket vezetnek be, vagy megváltoztatják a meglevőket, akkor igény keletkezik, hogy a hasonló változások ne befolyásolják a meglévő biztosítékokat, és az új rendszerek számára megfelelő biztosítékok álljanak rendelkezésre.

Ha biztonsági rendellenességet találunk, akkor azt ki kell vizsgálni, és a megállapításokat jelenteni kell a felsővezetésnek a biztosítékok lehetséges felülvizsgálatához, vagy komolyabb körülmények között az informatikai rendszerszintű biztonsági politika felülvizsgálatához és kockázat-felmérési tevékenységhez.

A biztonsági politikához való kapcsolódás érdekében megfelelő erőforrásokat kell rendelni a következők megfelelő napi szintű ellenőrzésének biztosítására:

a) Létező biztosítékok,
b) Új rendszerek és szolgáltatások bevezetése, és
c) Tervezett változtatások a létező rendszerekben és szolgáltatásokban.

Sok biztosíték készít napló formájú kimenetet az eseményekről. Ezeket a naplókat statisztikai technikák használatával kell ellenőrizni a trendváltozások és az ismétlődő események előfordulásainak korai érzékelése érdekében. Ki kell jelölni, hogy ki a felelős a naplók elemzéséért.

Elosztott rendszerekben a naplók csak egy adott környezetre vonatkozó információkat rögzítenek. Egy összetett esemény valós megértéséhez egyetlen eseményrekorddá kell

egyesíteni a különböző naplókat. Ezután ezt az eseményrekordot kell elemezni. Az eseményrekord egyesítés egy összetett feladat és a legfontosabb szempontja azon paraméterek azonosítása, melyek segítségével a különböző naplóbejegyzéseket biztonságosan össze lehet fűzni.

A napi rendszerességű ellenőrzés szervezéséhez szükséges vezetési technika a biztonsági műveleti eljárások dokumentálása. Ez a dokumentum leírja az összes műveletet, ami ahhoz szükséges, hogy biztosítjuk minden rendszer és szolgáltatás biztonsági szintjének hosszabb távon való fenntartását.

A biztonsági konfiguráció frissítéséhez szükséges tevékenységeket dokumentálni kell. Tartalmazniuk kell a változtatott biztonsági paramétereket, és frissíteniük kell minden biztonsági szervezési információt. Ezeket a változásokat rögzíteni kell, és jóvá kell hagyni a konfigurációkezelési folyamat során. A rendszeres karbantartás folyamán biztosítani kell, hogy a biztonság ne sérüljön. Megbízható elosztási eljárásokat kell leírni minden biztonsági összetevőre, ahol ez alkalmazható.

A biztosítékok ellenőrzési folyamatát írásba kell foglalni. Rögzíteni kell a biztonsági naplók vizsgálatának gyakoriságát és annak megközelítését. Meg kell jeleníteni a statisztikai eszközök és módszerek használatát. Útmutatást kell adni arról, hogy különböző működési körülmények között milyen vizsgálati küszöbértékeket alkalmazunk.

5.6.1 Rendszerauditálási óvintézkedések

Az üzemelő rendszer átvilágító auditálásának a követelményeit, valamint az ellenőrzést is magában foglaló tevékenységeket ajánlatos gondosan megtervezni és egyeztetni, hogy ezzel minimalizálni lehessen az üzleti folyamatok megszakadásának a kockázatát. Az alábbiakat ajánlatos megfigyelni:

a) Az átvilágító auditálás követelményeit ajánlatos egyeztetni az illetékes vezetőséggel.
b) Az ellenőrzés tárgyát ajánlatos egyeztetni és ellenőrizni.
c) A szoftverek és az adatok ellenőrzése a „csak olvasás” jellegű hozzáférésre legyen korlátozva.
d) A „csak olvasás”-on kívüli hozzáférést csak akkor szabad engedélyezni, ha az a rendszerállományok (rendszerfájlok) elkülönített másolatán történik, és akkor is az átvilágító auditálás befejezésével ezeket az állományokat ajánlatos megsemmisíteni.

e) Az ellenőrzéseket végző informatikai eszközöket pontosan azonosítani kell, és rendelkezésre kell bocsátani.
f) A különleges vagy kiegészítő feldolgozás követelményeit ajánlatos azonosítani és egyeztetni.
g) A hivatkozási napló (reference trail) készítéséhez ajánlatos minden egyes hozzáférést megfigyelni és naplózni (log).
h) Valamennyi eljárást, követelményt és felelősséget ajánlatos írásba foglalni (dokumentálni).

5.6.2 Rendszerauditáló eszközök védelme

A hozzáférést a rendszerauditáló, átvilágító eszközökhöz, azaz szoftverekhez és adatállományokhoz (fájlokhoz) védeni kell annak érdekében, hogy kizárjuk a lehetséges visszaéléseket és a veszélyeztetést. Ezeket az eszközöket el kell különíteni az üzemeltető és a fejlesztő eszközöktől, és nem szabad azokat a szalagtárakban vagy a használói körzetekben tárolni, hacsak nincsenek ellátva alkalmas szintű kiegészítő védelemmel.

6. Információbiztonsági Irányítási Rendszer továbbfejlesztése és karbantartása

A szervezetnek folyamatosan javítania kell az IBIR hatékonyságát, tekintettel arra, hogy a technológiai és szervezeti környezet a szervezet életében folyamatosan változik, ami új biztonsági kihívásokat támaszthat az adott szervezettel szemben. A szervezetnek az IBIR javítását az információbiztonsági szabályzat, biztonságpolitika, az audit eredmények, az ellenőrzések visszajelzései, a helyesbítő és megelőző tevékenységek valamint a vezetőségi átvilágításon keresztül kell végrehajtania.

Az IBIR rendszer továbbfejlesztése és karbantartása során a szervezetnek biztosítania kell a működtetési periódusban bevezetett eljárások karbantartását, javítását, valamint az ellenőrzési folyamatok kapcsán kapott eredményeket felhasználva meg kell kezdeni az IBIR rendszer módosítását és hozzáigazítását a változó körülményekhez. Az ellenőrzések kapcsán feltárt hiányosságok miatt szükség van a bevezetett biztonsági folyamatok javítására, tekintettel arra, hogy csak így kezelhetők megfelelő szinten az azonosított IBIR-t érintő kockázatok. A változó technológiai szervezeti és környezeti hatások miatt az IBIR-t érintő kockázatok, fenyegetések is folyamatos változásokon mennek keresztül, melyek érinthetik a rendszerbiztonságot belülről és kívülről is egyaránt. Ezt figyelembe véve szükséges az Informatikai Biztonsági Irányítási Rendszer folyamatosan felülvizsgálata, és a vizsgálatok eredményeinek ismeretében a szükséges akciók meghozatala. A szervezet által kialakított monitorozó rendszer és a feltárt biztonsági eseményeket kezelő eljárások segítségével a szervezet képes a gyors és hatékony reagálásra. A folyamatos kockázatelemzés végrehajtásával, és monitorozó rendszer működtetésével képes a szervezet megelőző és helyesbítő tevékenységek meghozatalára, mellyel biztosítja a biztonságos IBIR működését.

Az IBIR fejlesztése és karbantartása során fontos, hogy a szervezet minden helyesbítő és megelőző védelmi intézkedésének dokumentálása megtörténjen, továbbá biztosított legyen a rendszer módosítása esetén megváltozott feladatok és felelősségek megfelelő szintű kommunikációja, tekintettel arra, hogy ez elengedhetetlen fontosságú az IBIR működtetése szempontjából. A védelmi intézkedések kidolgozása és bevezetése esetén a szervezetnek biztosítania kell, hogy a Biztonsági politikában lefektetett irányelvek ne sérüljenek, és biztosítsák a vezetés által meghatározott biztonsági célokat.

6.1 Mérések szükségessége

Ahhoz, hogy az IBIR-t működtető szervezet képes legyen az IBIR rendszerének fejlesztésére, a működési folyamatokról visszajelzésekkel kell rendelkeznie az IBIR-t irányító vezetésnek. A mérésekről és ellenőrzésekről az előző szakaszban ismertetett átvizsgálási és ellenőrzési módszereket kell következetesen és rendszeresen végrehajtani ahhoz, hogy a döntéshozó testület birtokában legyen mindazon információnak, mellyel biztosítani tudja az IBIR folyamatos fejlődését, és a változó környezethez való alkalmazkodás lehetőségét.

6.2 Helyesbítő tevékenységek

Az ellenőrzések kapcsán feltárt hiányosságok, sebezhetőségi pontok, felmerülő újabb és újabb sebezhetőségek hatására a szervezetnek beavatkozásokat kell végrehajtania azok kiküszöbölésének érdekében, hogy megelőzze az ismételt előfordulásokat. Ezen intézkedések sorozatát nevezik helyesbítő intézkedéseknek. Ahhoz, hogy ezt a szervezet hatékonyan el tudja végezni, szükséges egy megfelelő ellenőrző és megfigyelő rendszer kialakítása. A rendszer kiépítésének célja az IBIR bevezetésével és/vagy működtetésével kapcsolatos nemmegfelelőségek azonosítása, és a kiváltó okok meghatározása.

A felmerült nemmegfelelőség kezelése érdekében első körben fel kell mérni azt, hogy a kapcsolódó fenyegetések, azok bekövetkezési valószínűsége és az érintett szervezeti információs vagyon indokolja-e egyáltalán külön védelmi intézkedés foganatosítását, vagy a felmerülő kockázat nem éri el a kockázatkezelés szintjét. Ennek érdekében a vezetés, az érintett szakmai területtel együtt konzultálva értékeli a helyesbítő tevékenység bevezetésének szükségességét. A szervezetnek dokumentálnia kell a döntését elutasítás, vagy további kezelés esetében egyaránt.

Amennyiben a szervezet a helyesbítő tevékenység bevezetése mellett döntött, a szervezetnek ki kell dolgoznia azokat a forgatókönyveket, melyek megszűntetik a nemmegfelelőségeket. Ezt jellemzően az érintett terület szakmai személyzetének kell kidolgoznia. Természetesen a nemmegfelelőség kezelésére számos lehetőség adódhat, melyek mindegyikét számba kell venni. A szakmai csoport által elkészített kezelési terveket fel kell terjeszteni a döntéshozók felé, akik az alternatívák közül kiválasztják azt, melyhez biztosítják a szükséges erőforrásokat a megvalósítás érdekében.

Az elfogadott kezelési terv alapján a bevezetést tervezetten kell végrehajtani, dokumentálni kell a bevezetés lépéseit, a bevezetésért felelős személyek körét, a bevezetés

időpontját, és ha szükséges például technológiai módosítások esetén a hibákra felkészülve a visszaállás lépéseit.

A helyesbítő tevékenységek bevezetése során a fent említett lépéseket dokumentálni szükséges, továbbá biztosítani kell a feljegyzések döntések visszakereshetőségét az esetleges ellenőrzések auditok kapcsán. Fontos a dokumentációk megléte, tekintettel arra, hogy a szervezet így tudja bizonyítani a vizsgálatot folytató felé, hogy az IBIR rendszerét a változó környezet és a felmerülő nemmegfelelőségek érdekében folyamatosan fejleszti, törekszik az optimális állapot eléréséért.

A bevezetett helyesbítő tevékenység gyakorlati működése során ellenőrizni szükséges, hogy teljesíti a feltárt nemmegfelelőség elvárt szinten történő kezelését, és a kapott mérési eredményeknek megfelelően meg kell hozni a szükséges javító vagy módosítandó lépéseket annak érdekében, hogy a felmerült nemmegfelelőség kezelése az elvárt szinten megtörténjen.

6.3 Megelőző tevékenységek

Az IBIR fejlesztésének egyik módszere az ún. megelőző tevékenységek használata, védelmi intézkedések bevezetése és érvényesítése. A megelőző tevékenységek érvényesítésének alapfeltétele az előzetes kockázatfelmérés és elemzés végrehajtása, tekintettel arra, hogy magának a biztonsági esemény bekövetkezését megelőzendően a szervezet meghozza azon intézkedéseit, melyekkel el kívánja kerülni az adott fenyegetés bekövetkezését, és annak hatására realizálható veszteség elkerülését.

Ahhoz, hogy a szervezet megelőző védelmi intézkedéseket tudjon bevezetni, a „0. 3. Az Információbiztonsági Irányítási Rendszer létrehozása” fejezetben meghatározott sebezhetőségi vizsgálatot, fenyegetettség-elemzést, kockázatelemzést kell végrehajtania. Ennek eredményeképpen a vezetésnek meg kell határoznia a megelőző tevékenységek fontossági sorrendjét, és annak alapján elkészítenie a bevezetési tervét.

A megelőző védelmi intézkedések kivitelezése és tervezése kapcsán a helyesbítő tevékenységeknél említetteknek megfelelően biztosítani kell ebben az esetben a megfelelő dokumentálást, mellyel a szervezet bizonyítani tudja a felülvizsgálatok és ellenőrzések kapcsán az IBIR fejlesztésére, módosítására tett lépéseit.

A megelőző védelmi intézkedések a tapasztalatok szerint gazdaságosabbak a helyesbítő védelmi intézkedéseknél, tekintettel arra, hogy ilyen esetekben a tényleges biztonsági esemény még nem következett be, tehát az akkor realizált kár megelőző védelmi intézkedések alkalmazásakor nem jelenik meg, csak a bevezetéssel járó költségek. Ezt figyelembe véve

javasolt a folyamatos kockázatelemzés végrehajtása, és annak eredményeinek megfelelően a megelőző védelmi intézkedések meghozatala.

A megelőző védelmi intézkedések esetében is szükséges végrehajtani a bevezetést követő hatékonyság és hatásosság elemzést, mellyel a szervezet megbizonyosodik arról, hogy a bevezetett intézkedés elérte a célját, vagy szükséges esetleges további módosító vagy új intézkedések meghozatala a kezelendő sebezhetőséget kihasználó fenyegetések elkerülése érdekében.

6.4 Dokumentációk karbantartása, frissítése

A megelőző és helyesbítő védelmi intézkedések bevezetésével párhuzamosan, amennyiben nem adminisztratív védelmi intézkedés került bevezetésre, abban az esetben szükséges végrehajtani a szabályozási környezetet alkotó dokumentációk frissítését. Ennek érdekében a szervezetnek ki kell alakítania egy dokumentált eljárást, melyben szabályozza a szabályzó környezet frissítését és karbantartását. Az eljárásnak tartalmaznia kell a karbantartással kapcsolatos feladatokat és felelősségeket, továbbá az alábbi követelményeket:

a) Az adott szabályzat kiadása előtti jóváhagyási folyamat szabályozását
b) A dokumentum felülvizsgálatát, szükség esetén frissítését és újbóli jóváhagyási folyamatát
c) Annak biztosítását, hogy a dokumentumok változásai aktuális állapotai nyomonkövethetők legyenek
d) A dokumentumok aktuális és hatályos verziói az érintettek számára elérhetők legyenek
e) A dokumentumok megsemmisítésének szabályait
f) A dokumentumok biztonsági besorolásának, és címkézési szabályait
g) A dokumentumok elosztásának szabályait, azaz az elosztás ellenőrzött legyen
h) A nem hatályos dokumentumok visszavételének eljárását, továbbá ilyen esetekben a megfelelő azonosítás alkalmazását a további megőrzés és azonosítás érdekében.

Felhasznált irodalom

[1] *Muha Lajos*: Az Informatikai Biztonsági Irányítási Rendszer, In: IKT 2010 (Informatika Korszerű Technikái). Dunaújváros, Magyarország, 2010.03.05-2010.03.06.

[2] *Berkes Zoltán, Déri Zoltán, Krasznay Csaba, Muha Lajos*: Informatikai Biztonsági Irányítási Rendszer (IBIR), Budapest: Miniszterelnöki Hivatal, 2008.

[3] *Muha Lajos*: Szabványok és ajánlások, In. Az informatikai biztonság kézikönyve (szerk. Muha L.), Verlag Dashöfer Szakkiadó, 2005., 1. kötet 2.3.

Szabványok

[1] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements

[2] ISO 9000:2005 Quality management systems. Fundamentals and vocabulary.

[3] ISO 9001:2008 Quality management systems. Requirements.

[4] ISO 9004:2009 Managing for the sustained success of an organization. A quality management approach.

[5] ISO 14001:1996 Environmental management systems—Requirements with guidance for use.

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.