MÁSODIK SZERDAI ELŐADÁS

Dombora Sándor: Működőképes információbiztonsági irányításrendszerek jellemzői

2018. November 14.

ISACA® Budapest Chapter

ISACA®

Trust in, and value from, information systems

Működőképes információbiztonsági irányításrendszerek jellemzői

Dombora Sándor

ISACA Budapest Chapter
2018. november 14.

Felelősség kizárása

Az elhangzott prezentációk tartalmát illetően az ISACA Magyarországi Egyesület nem vállal felelősséget az abban nyújtott információk aktualitásáért, helyességéért és teljességéért.

Az itt elhangzott információk nem feltétlenül egyeznek meg az ISACA Magyarországi Egyesület álláspontjával.

Miért van szüksége a szervezeteknek működőképes Információbiztonság Irányítási Rendszer kiépítésére

- A **GDPR betartása** feltételezi egy működőképes IBIR meglétét, a személyes adatok védelmének érdekében
- **Törvény írja elő** (pl. Ibtv., Infotv., GDPR, ágazati jogszabályok)
- **Piaci előny**, ha a szervezet rendelkezik **ISO 27001** tanúsítással
- A **szervezet saját érdeke** az általa kezelt **adatok védelme** az információszivárgás, adatsérülés ellen
- Az adatok **rendelkezésre állásának** biztosítása

Miért szükséges beszélni az Információbiztonság Irányítási Rendszerek működőképességéről

Az IBSZ gyakori problémái

- Szinte minden biztonsági szabályt az IBSZ tartalmaz
- Nincs a szervezetben kialakított szerepkörökre bontva a szabályozás
- Sok olyan leírást tartalmaz ami nem tartozik minden dolgozóra
- Nem világos, hogy az egyes dolgozókra mi vonatkozik
- A rosszul kialakított IBSZ minden dolgozó általi megismerése biztonsági kérdéseket vet fel

Az IBSZ gyakori problémái

- Nemcsak általános biztonsági szabályokat tartalmaz, hanem módszertanokat, leírásokat
- Túl hosszú, akár több 100 oldal
- Elolvasása sok időt igényel
- Sok rövidítést, szakkifejezést használ, sok dolgozó számára érthetetlen
- A dolgozók ha elolvassák is, nem emlékeznek a tartalmára
- Nincsenek meg a végrehajtáshoz szükséges feltételek

Az szabályozási rendszer gyakori problémái

- A szabályzat nem illeszkedik a munkakörnyezethez
- A szabályzatok nem felelnek meg a jogszabályi környezetnek
- Jogszabály/szabvány módosított másolata, megmarad elméleti szintem, nem épül be a munkafolyamatokba
- Átláthatatlan, kusza, átfedésben vannak a szabályzatok
- Ellentmondásos előírásokat tartalmazó szabályzatok
- Betarthatatlanság: ha betartjuk ellehetetlenül, megáll a munka

Hogyan keletkeznek a működésképtelen Információbiztonság Irányítási Rendszerek

Hogyan áll elő a végrehajthatatlan szabályozási rendszer

- Jogszabály írja elő, csinálunk valamit
- Szükség volt rá pályázat megnyeréséhez, gyorsan készítünk egyet
- Túl szoros határidőre kell elkészíteni
- Megrendeltük a tanácsadótól, leszállította
- Nem volt időnk, nem vettünk részt megfelelő mértékben a kialakításában, a tanácsadó úgyis tudja alapon

Működésképes

Információbiztonság Irányítási Rendszerek

jellemzői

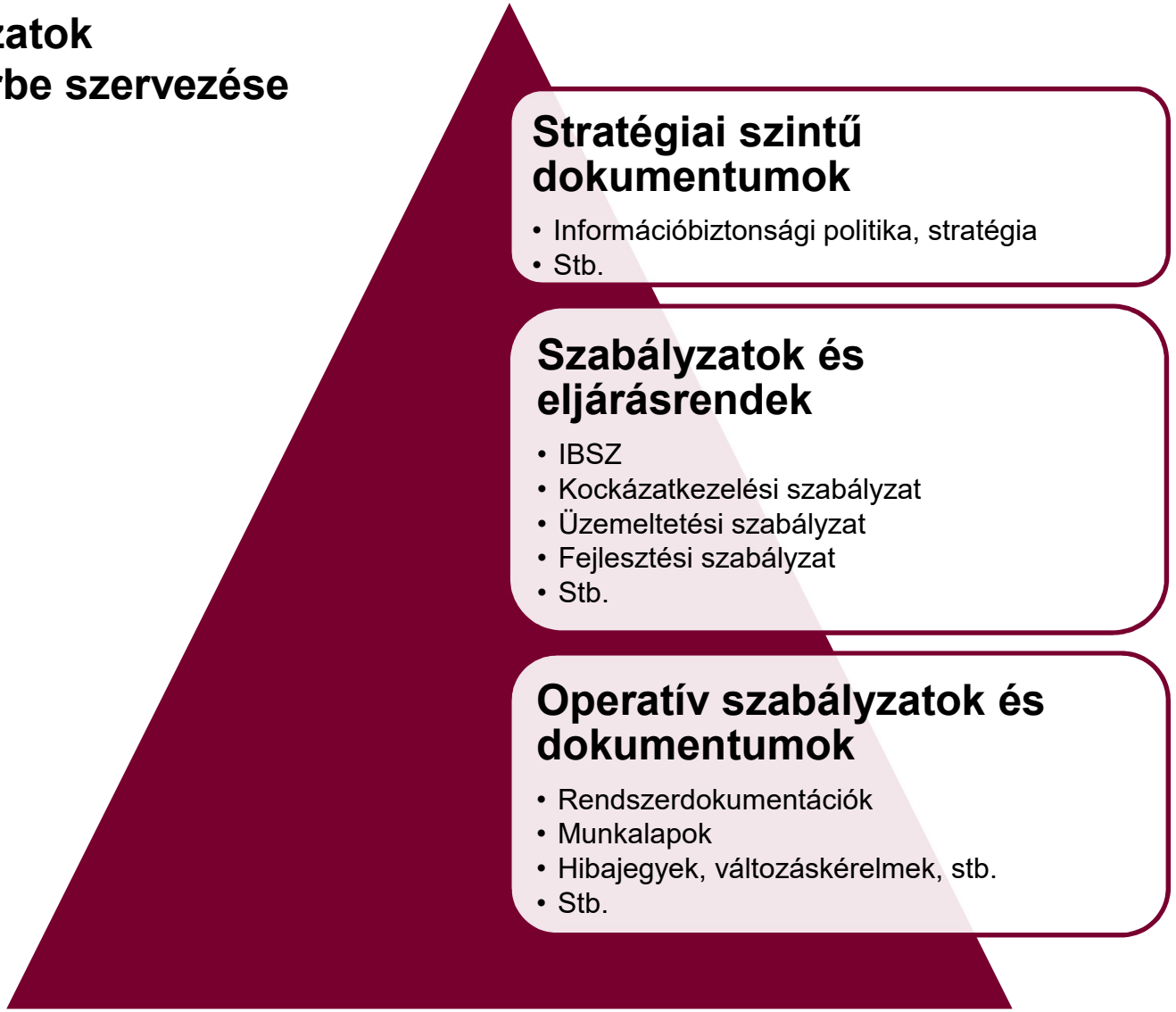
- Hierarchikus
- Konzisztens
- Betartható
- Végrehajtható
- Érthető és értelmezhető
- Minimálisan szükséges
- Teljes

Javasolt hierarchikus információbiztonsági szabályzatrendszer

- **Legfelső szint:** irányelvek, amelyek mentén a szervezet kialakítja az információbiztonságot
- **Középső szint:**
  - **Szabályzatok** – adott munkacsoportok által betartandó általános szabályok
  - **Eljárásrendek** - munkafolyamatok, információ-biztonsági előírásokkal
- **Alsó szint:** operatív szabályzatok és dokumentumok
  - Rendszerdokumentáció, munkafolyamatok
  - Munkalapok, Hibajegyek, Változáskérelmek, stb.

Dokumentumok típus szerinti hierarchiája

Szabályzatok rendszerbe szervezése



Dokumentumok szakterület szerinti hierarchia

- Informatikai biztonsági politika, stratégia
  - Informatikai biztonsági szabályzat
    - Kockázatkezelési szabályzat
      - Kockázatkezelési eljárásrend
        - Kitöltött kockázatkezelési űrlapok
        - Kockázatelemzés eredménye
    - Biztonságtervezési eljárásrend

Dokumentumok szakterület szerinti hierarchia

- Informatikai Stratégia
  - Informatikai üzemeltetési szabályzat
    - Eseménykezelés
      - Biztonsági események kezelése
    - Incidenskezelési eljárásrend
    - Konfigurációkezelési eljárásrend
    - …
  - Informatikai fejlesztési szabályzat
    - Fejlesztési eljárásrend

Látható az átfedés az informatikai biztonsági területtel

Ezeket kezeljük hivatkozással

Konzisztencia biztosítása
Dokumentációs rend kialakítása

- Szabályzatok **hatókörének és terjedelmének rögzítése**, karbantartás – minek hol a helye
- Minden **szabály, biztonsági követelmény egy helyen szerepel**, máshol csak hivatkozunk rá
- Dokumentumok közötti **kapcsolati térkép**
- A **szabályzatok követelményeket fogalmaznak** meg
- Az **eljárásrendek munkafolyamatokat** írnak le.
- Az **igazoló dokumentumok a munka elvégzését**, szabályok betartását dokumentálják

Megfelelés az üzleti, jogszabályi és szabvány elvárásoknak

- **Szisztematikus tervezés**
- **Üzleti követelményekből** származó követelmények beépítése
- **Iparági és információbiztonsági szabványokból** származó követelmények beépítése
- **Jogszabályokból és végrehajtási rendeletetekből** származó követelmények beépítése
- **Összefüggések azonosítása kezelése**

Betarthatóság és végrehajthatóság

- Az általános **mindenkire vonatkozó** információbiztonsági szabályokat építsük az **IBSZ-be**
- A **szakterületekre vonatkozó** általános szabályokat építsük a **szakterület biztonsági szabályzatába**
- A **tevékenységekhez kapcsolható** biztonsági **előírásokat** építsük be a **munkafolyamatokba**, **eljárásrendekbe**
- A szabályzatok hierarchiájában haladjunk az általánostól a specifikus felé

Betarthatóság és végrehajthatóság

- A szabályzatokat **a szakterület bevonásával** készítsük
- Az **elméleti szabályokhoz** tartozzon **végrehajtási eljárásrend,** ha lehet **épüljenek be munkafolyamatokba**
- **Világítsuk át és aktualizáljuk** a már **meglévő munkafolyamatokat** a szabályzatrendszer mentén
- **Az informatikai rendszerekbe kockázatoktól függően építsük be a szükséges kontrollokat**, ez kikényszeríti a biztonságos működést és a szabályzatok betartását

Iránymutatás a dokumentációs rend kialakításához

- **A teljesség érdekében: jogszabály vagy szabvány alapú szerkezet** a szervezet igényeihez igazítva
- A szervezet számra **legmeghatározóbb jogszabály vagy szabvány mentén** építkezzünk
- Irányelvek szabályzatok és eljárásrendek hatókörének meghatározásához:
  - **Átláthatóság és kezelhetőség** biztosítása érdekében **minél kevesebb és kisebb szabályzat**
  - **Szabályok szerepkörönkénti szétválasztása**

Iránymutatás a dokumentációs rend kialakításához

- **Érthetőség és értelmezhetőség**
  - A célterületen dolgozók által használt terminológia használata
- **Minimalizálás**
  - Csak üzleti, jogszabályi vagy szabvány követelmények teljesülését biztosító szabályok kerüljenek be a rendszerbe
- **Frissítés**
  - Konzisztencia megtartása
  - Kapcsolódó dokumentumok frissítése

Köszönöm a figyelmet!

Kérdések?

dombora.sandor@kvk.uni-obuda.hu