12.b Határozza meg az informatikai biztonság szabályzási és dokumentációs rendszerét, adjon példát az egyes dokumentumok tartalmára intézményi környezetben!

BRD – Business Requirement Document

- Egy szerződés a vállalat és az ügyfél között egy product-ról.

DRP – Disaster Recovery Plan

- Leírja, hogy hogyan tud egy szervezet gyorsan munkába állni egy váratlan esemény után.

Mi a szabályozási rendszer?

- Fontos szerepet játszik az intézmények biztonságos és hatékony működésében, mivel biztosítja a szabályok és előírások betartását, megelőzve az esetleges jogi, biztonsági vagy reputációs kockázatokat.
- Az informatikai biztonság szabályzási és dokumentációs rendszere egy olyan strukturált módszer, ami segíti az intézményeket abban, hogy az információik biztonságosan legyenek kezelve és védelmezve legyenek.

ISO/IEC 27001 szabvány

- ISO/IEC 27000 szabványcsalád tagja, ami az information security management system követelményszabványa.
- A szabvány meghatározza azokat a rendszerkövetelményeket, amik célja, hogy az információbiztonság megfelelő felügyelet és ellenőrzés alatt álljon.

Mikre terjed ki a követelményrendszere?

- Szervezeti biztonság
- Alkalmazottakhoz kapcsolódó biztonság
- Külső személyekhez kapcsolódó biztonság
- Eszközök osztályozása és ellenőrzése
- Kommunikáció és üzemeltetés irányítás
- Hozzáférés ellenőrzés
- Működés folyamatosság irányítás
- Rendszerfejlesztés és karbantartás

Előnyei

- **Szabályozást ad**
  - Adatvesztés,
  - Jogosulatlan hozzáférés,
  - Vírustámadás,
  - Illetéktelen behatolás, Katasztrófa elhárítás
- Hozzájárul az információvagyon sérülésének megakadályozásához és a vállalkozás partnerei számára is biztosítékot ad arra, hogy az információkkal kapcsolatos kockázatok kezelése biztosított.

Dokumentumai (ezeken kívül még több is megtalálható, ezek a ténylegesen ajánlottak)

- Belső (Internal) Audit
- Information Security Policy
- Risk Assessment
- Statement of Applicability

Internal audit (9.2 Internal Audit)

- Szervezeten belüli auditálás, ellenőrzések.
- **Tartalma**
  - Executive summary
    - Szervezet megfelelősségi állapot
    - Kezelendő hiányosságok
  - Audit leírása
    - Információkat kell tartalmaznia az audit elvégzésének módjáról.
  - Hiányosságok és javítási lehetőségek
  - Javító (corrective) intézkedések meghatározása

Information Security Policy (5.2 Policy)

- Magas szintű áttekintést nyújt arról, hogy a szervezet hogyan közelíti meg az információbiztonságot.
- **Tartalma**
  - Cél (Purpose)
  - Követelmények (Requirements)
    - Jogi, szerződéses, szabályozási követelmények
  - Szerepek és felelősségi körök (Roles & responsibilities)
    - Ki felel a megvalósításért, karbantartásért, monitorozásért az ISMS-en belül.
  - Kommunikáció (Communication)
    - Szabályzatot kivel kell megosztani (belső vagy külső féllel)

Risk Assessment (6.1.2)

- Azonosítják a szervezeti kockázatokat, meghatározzák az egyes kockázatok valószínűségét és hatását, és felvázolják, hogy a szervezet hogyan fog reagálni az egyes kockázatokra.
- **Tartalma**
  - Kockázatok észlelése
  - Kockázatok elemzése
    - Veszélyességi szint hozzárendelése
  - Kockázatok értékelése és rangsorolása
  - Kockázatkezelési terv kitöltése
  - Kockázati jelentése készítése

Statement of Applicability (6.1.3)

- Az Annex A biztonsági ellenőrzések közül melyek alkalmazhatóak és melyek nem az ISMS-re.
- **Tartalma**
  - Kockázatkezelés végrehajtása
    - Risk assessment-ből kiindulva
  - Security kontrollok kiválasztása a kockázatok csökkentésére.
  - Lista azokról a kontrollokról, amiket nem fogunk használni és miért nem.
    - Nem akarunk nagy összeget költeni egy kis összegű problémára.
  - Dokumentáció naprakészen tartása.