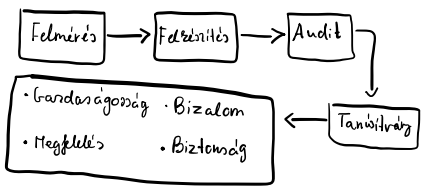
Informatizai biztonság szabályzási és dokumentációs rendszer

- **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.
- **Szabályzási rendszer**
  - Fontos szerepet játszik az intézmények biztonságos és hatékony működésben, mivel biztosítja a szabályok és előírások betartását, megelőzve az esetleges jogi, biztonsági vagy reputációs kockázatokat.
  - Az informatizai 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. (ISMS)
  - A szabvány meghatározza azokat a rendszerkövetelményeket, amik célja, hogy az információbiztonság megfelelő felügyelet és ellenőrzés alatt álljon.
- **Miket fejed ki a követelményrendszer?**
  - Szervezeti biztonság
  - Alkalmazottakhoz / 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 vállalati partnerek számára is biztosítékot ad arra, hogy az információval kapcsolatos kockázatok kezelése biztosított.
- Dokumentumai
  - Belső audit
  - Information Security Policy
  - Risk Assessment
  - Statement of Applicability
- Internal audit (9.2)
  - Szervezeten belüli auditálás/ellenőrzések.
  - Tartalma
    - Executive Summary
      - Szervezet megfelelőségi állapot
      - Kezelendő hiányosságok
    - Audit leírása
      - Információkat kell tartalmazzon az audit elvégzésének módjáról
    - Hiányosságok és javítási lehetőségek
    - Javító (corrective) kontrollok meghatározása

- **Information Security Policy (5.2)**
  - Magas szintű áttekintést nyújt arról, hogy a szervezet hogyan közelíti meg az információbiztonságot.
  - Tartalma
    - Cél (Purpose)
    - Követelmények (Requirements) -> Jogi, szerződés, szabályozási követelmények
    - Szerepek és felelősségi körök (Roles & responsibilities) -> Ki felel a megvalósításért, karbantartásért, monitorozásért az ISMS-en belül.
    - Kommunikáció -> 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 kockázatokkal.
  - Tartalma
    - Kockázatok észlelése
    - Kockázatok elemzése -> Veszélyességi szint hozzárendelése
    - Kockázatok értékelése és rangsorolása
    - Kockázatkezelési terv kitöltése
    - Kockázati jelentés készítése
- **Statement of Applicability (6.1.3)**
  - Az Annex A biztonsági ellenőrzések közül melyik alkalmazhatóak és melyek nem az ISMS-re.
    - Tartalma
      - Kockázatkezelés végrehajtása -> Risk assessment-ből kiindulva.
      - Security Controllok kiválasztása a kockázatok csökkentésére.
      - Lista arról a controllokról, amiket nem fogunk használni és miért nem.
        - Nem akarunk nagy összeget költeni egy kis összegű problémára.
      - Dokumentáció naprakészen tartása.