# **9.b** Ismertesse az informatikai ellenőrzés feladatához és az ellátásához kapcsolódó alapfogalmakat (rendelkezésre állás, bizalmasság, sértetlenség), valamint a két kiegészítő követelményt (funkcionalitás, dokumentáció), mondjon példát a teljesítésük mérésére!

# Kockázatelemzés hasznossága

* Segítséget nyújt a rendszer leggyengébb pontjainak.
* Legnagyobb kockázatot jelentő fenyegető tényezők azonosítása.
* Ezek ismeretében költséghatékony, kockázatarányos védekezést lehet kialakítani.

# Kockázatmenedzsment

* Kockázatok, károk.
* Kockázatbecslés problémáit a kockázatmenedzsment módszerével szokás kezelni a gyakorlatban, ami a kockázatok értékeit nem határozza meg konkrét érték formájában.
  + Olyan összehasonlításra lehetőséget adó elemzést alkalmaz, ami alapján legcélszerűbb védelmi intézkedések meghatározhatóak.
* Egyes kockázati tényezőket egymáshoz hasonlítva határozzuk meg a gyenge láncszemeket, ahol a legcélszerűbb védekezni.

# Károk

* Hatás továbbterjedése = elsődleges, másodlagos, harmadlagos, stb. károk
* Veszélyforrás elbírálása meddig terjedhet ki, mivel a másodlagos, harmadlagos károk nagyobbak az elsődleges károknál.
* Elsődleges kár = Merevlemez meghibásodás
* Másodlagos kár = Nagy mennyiségű adat visszaállíthatatlanul megsemmisül.
* Harmadlagos kár = Üzleti haszon elmaradása a károk miatt

# Kockázatelemzés táblázatos módszere

* Alapja a veszélyforrások számbavétele és részletes elemzése, egy kockázatelemzési tábla szisztematikus, oszlopról-oszlopra haladó kitöltésével.

# Kockázatelemzés lépései

**1. Kategóriák felállítása:**

Bekövetkezési valószínűség, Kár, Kockázati, Kockázati szorzótábla meghatározása

1. **Veszélyforrások meghatározása**
2. **Bekövetkezési valószínűségek nagyságrendi meghatározása**
3. **Kárérték nagyságrendi meghatározása**
4. **Kockázati tényezők származtatása**
5. **Elviselhetetlen kockázatok kezelése**
6. **Védelmi intézkedések számbevétele és a megfelelő alternatívák kiválasztása**

# CIA

## **C**onfidendiality

* Adatok kiszivárgásának megakadályozása, vagyis titkosítás

## **I**ntegrity

* Sértetlenség, vagyis integritást védő algoritmusok

## **A**vailability

* Rendelkezésre állás, vagyis hálózati eszközök és adatok elérhetősége

# Példa

* Az áramszünet nem okozza a bizalmasság sérülését, de hatással van a rendelkezésre állásra és akár a tárolt adatok is sérülhetnek.
  + Ezt a hatásmechanizmust az **I** és **A** oszlopok megfelelő kitöltésével, a **C** oszlopban kihúzással jelölhetjük.

# Informatikai ellenőrzés

* Standardok, irányelvek alapján járnak el az ellenőrök.

## Funkcionalitás

* Azt vizsgáljuk, hogy a szoftver vagy rendszer megfelel-e a felhasználói igényeknek és elvárásoknak.
* Teszteket és vizsgálatokat végzünk a rendszer különböző részein.

## Dokumentáció

* Ellenőrizzük, hogy a rendszerhez vagy a szoftverhez készült dokumentáció megfelel-e és teljes.
* A dokumentáció magába foglalja a használati útmutatót, az implementációs dokumentációt, a tesztelési tervet és a működési dokumentációt is.
* Tehát ellenőrizzük, hogy a dokumentáció tartalmazza-e a szükséges információkat, például azokat a folyamatokat, amik segítségével a rendszer működik, a szükséges eszközöket, a szükséges konfigurációkat és azokat a paramétereket, amik befolyásolhatják a rendszer működését.