# **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!

# Informatikai ellenőrzés

* **Auditálás == ellenőrzés**
* Standardok, irányelvek alapján járnak el az ellenőrök.
  + ISAE 3000, ISAE 3402, ISO27001, stb

## Audit célja

* Célja ellenőrizni, hogy megfelelően működik például az informatikai rendszer.
* Megfelelően dokumentált
* A dokumentációnak megfelelően működik
* Teljesíti az elvárásokat, mint például rendelkezésre állás, megbízhatóság.

## IT Audit felépítése

* **Tervezés (ellenőrzési terv)**
  + Célkitűzések meghatározása
  + Az audit tárgya
  + Részletes audit terv készítése
* **Lebonyolítás:** A vizsgálati bizonyítékok begyűjtése
* **Dokumentálás:** Vizsgálati jelentés készítése

## IT Audit tárgy

* IT rendszer, konfiguráció, működés-megfelelés
* Dokumentáció, szabályozás, folyamat
* IT rendszerhez kapcsolódó szerepkörök
* IT rendszer bevezetés, IT projektek
* **Gyakorlatilag ezek bármilyen kombinációja**

## Audit módszerek

* Az audithoz kapcsolódó bizonyítékokat több módon össze lehet gyűjteni
  + Dokumentáció, Interjú, tesztelés (mintavételes és analitikus)

## Audit dokumentáció

* Audit felkérés
* Részletes audit terv (felkérés alapján)
* Audit bizonyítékok: dokumentációk, jegyzetek, elemzések
* Audit jelentés

## Ki lehet IT Auditor?

* Az IT Auditor szerepköri megkötések
  + Objektív
  + Felkészült
  + Audit módszertanokat ismerő, nem kizárólag IT-s.
* **Összeférhetetlenség, tehát nem vizsgálhatja önmagát!**

## Belső audit

* Szervezeten belüli ellenőrzések.
* A belső ellenőrzés megállapításokat és ajánlásokat fogalmaz meg a szervezet vezetője részére.

## Külső audit

* Függetlenül ellenőrzi a belső auditálást, a belső ellenőrzési és irányítási rendszer működését, a vizsgált rendszer biztonsági állapotát.

## Törvények és az IT

* Állami és önkormányzati szervek információbiztonsága (2013/L.tv.)
* Létfontosságú létesítmények és rendszerek követelményei (2012/CLXVI.tv.)
* Pénzügyi szektor követelményei (hpt. – 2014/CCXXVII.tv.)

# CIA

* **Confidendiality:** Adatok kiszivárgásának megakadályozása, vagyis titkosítás.
* **Integrity:** Sértetlenség, vagyis integritást védő algoritmusok.
* **Availability:** 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.

# Követelmények

## Funkcionalitás

* **Mit kell kielégíteni a szoftvernek?**
* Megfelelőség
* Szolgáltatott outputok pontossága
* Más rendszerekkel való együttműködési képesség
* Vonatkozó szabványoknak, törvényi szabályozásnak és konvencióknak történő megfelelés
* Biztonság (védelem jogosulatlan, szándékos vagy véletlen hozzáférések ellen)

### Funckionalitás példák

* Az e-kereskedelmi weboldalnak lehetőséget kell biztosítani a felhasználóknak a termékek böngészésére, kosárba helyezésére és fizetésére.
* Egy ügyfélkapu rendszernek lehetőséget kell adnia a felhasználóknak a személyes adatok kezelésére, dokumentumok feltöltésére.

## 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.

### Dokumentáció példák

* **Felhasználói dokumentáció**, ami részletesen bemutatja az alkalmazás vagy rendszer használatát, tehát tartalmazza a funkciók leírását, útmutatókat, képernyőképeket.
* **Fejlesztői dokumentáció,** ami a fejlesztőknek a dolgát segíti, hogy az adott kódrészlet mit csinál, mik az inputok/outputok.