IT biztonság
2020/2021 tanév ősz

Bemutatkozás

Giesz István
- okl. Gépészmérnök, okl. Rendszerszervező, Információbiztonsági menedzser, ISO27k1IA&LA
- KÖFÉM/ALCOA/ARCONIC, BUSZESZ, HUNGRANA, Csemege Julius_Meinl, SPAR, TESCO - IT vezető/ügyvezető
- GIRO Zrt – vezérigazgató helyettes
- Progadat - ügyvezető

Ismétlés

- … egy kis élet
- Irányítási és integrált irányítási rendszerek
- 2013. évi L. törvény (Ibtv.)
- GDPR és 2011. évi Információbiztonsági törvény (Infotv.)

Agenda

- Szabványok és ajánlások
- NIST SP 800-53r4
- ISO/IEC 27000-s szabványcsalád
- ITIL, COBIT, CC

Szabványok

Szabványok

Jogállás szerint
- De jure (regisztrált)
- Kvázi
- Ajánlás
- Legjobb gyakorlat

Elérhetőség szerint
- Nyílt
- Üzleti alapú

Használat szerint
- Alkalmazása kötelező
- Önkéntesen követhető

Bejegyzés szerint
- Magyar MSZ
- Európai MSZ EN
- Nemzetközi MSZ ISO
- Egyéb

MSzT - Magyar Szabványügyi Testület : „A szabványok figyelmen kívül hagyása súlyos gazdasági és jogi következménnyel járhat, mivel a szabványok - az Európai Unió műszaki jogalkotásának egyik legfontosabb alapelve szerint - a jogszabályokban meghatározott alapvető követelmények teljesítéséhez kínálnak **önkéntesen alkalmazható megoldásokat**. Ezek figyelembevétele esetében - ugyancsak európai uniós, de már jogkövetési alapelv szerint - vélelmezni kell a jogszabálynak való megfelelőséget és ezt **tilos vizsgálattal ellenőrizni**.”

Szervezetek

Nemzetközi, ajánlásokat és kvázi szabványokat kidolgozó szervezetek

- **IEEE** Institute of Electrical and Electronics Engineers
- **ITU** International Telecommunication Union
- **IEC** International Electrotechnical Commission
- **CEN** Comité Européen de Normalisation
- **CENELEC** European Committee for Electrotechnical Standardization
- **ETSI** European Telecommunications Standards Institute

Egyéb, USA szabványügyi szervezetek

- **NIST** National Institute of Standards and Technology
- **ASTM** American Society for Testing and Materials
- **ANSI** American National Standards Institute

USA kormányzati ajánlások

- **FIPS** Federal Information Processing Standards

Szabványok

ISO International Organization for Standardization

és szabványkatalógusa

https://www.iso.org/standards-catalogue/browse-by-ics.html

Szabványok

BSI Bundesamt für Sicherheit in der Informationstechnik
Német információbiztonsági szabvány és ajánláscsalád
(nyílt dokumentumok is vannak)

https://www.bsi.bund.de

IT biztonsági szabványok és egyéb ajánlások kereskedelme

https://www.itgovernance.co.uk/

Magyarországon bejegyzett szabványok elérhetősége

http://www.mszt.hu/

Szabványok

USA információbiztonsági szabvány-és ajánláscsalád (NYÍLT dokumentumok)

- **FIPS Publication 199**
  Standards for Security Categorization of Federal Information and Information Systems
- **FIPS Publication 200**
  Minimum Security Requirements for Federal Information and Information Systems
- **NIST Special Publication 800-53Revision 4**
  Security and Privacy Controls for Federal Information Systemsand Organizations

… (továbbá több tucatnyi érintőleges szabvány és ajánlás)

Ajánlások, cikkek…

NIST Information Technology Laboratory Divisions

- Advanced Network Technologies Division
- Applied and Computational Mathematics Division
- Applied Cybersecurity Division
- Computer Security Division
- Information Access Division
- Software and Systems Division
- Statistical Engineering Division

NIST 800-53r4 (Ibtv.)

NIST 800-53r4 felépítése

NIST - National Institute of Standards and Technology

NIST Special Publication 800-53Revision 4:
Security and Privacy Controls for Federal Information Systemsand Organizations

A **NIST Special Publication 800** információs technológiai dokumentumsorozata a NIST Információtechnológiai Laboratórium (ITL) kutatásairól, útmutatásairól és a számítógépes biztonsággal kapcsolatos ismeretterjesztő erőfeszítéseiről, valamint az iparral, a kormányzattal és az akadémiai szervezetekkel folytatott együttműködésről szól. Kiemelt területek közé tartozik a **kriptográfiai technológia és az alkalmazások, a fejlett hitelesítés, a nyilvános kulcsú infrastruktúra (PKI), az internetes biztonság, a kritériumok és a biztonság, valamint a biztonság kezelése és támogatása**.

https://nvd.nist.gov/800-53/Rev4
https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
NIST.SP.800-53r4
FIPS PUB 199

2020.09.22. ELTE IT BIztonság Speci 13

ISO 27k

2020.09.22. ELTE IT Biztonság Speci 14

ISO 27k család

Kis történeti áttekintés

- BS7799-1 - Best practices for Information Security Management
- BS7799-2 - Information Security Management Systems - Specification with guidance for use
- ISO/IEC 17799 - Code of practice for information security management
- ISO/IEC 27001:2013 - Information security management systems – Requirements
- MSz ISO/IEC 27001:2014 – Biztonságtechnika. Információbiztonságirányítási rendszerek. Követelmények

ISO 27k család

Információbiztonsági szabványcsalád

- **ISO/IEC 27000** - Information security management systems Overview and vocabulary
- **ISO/IEC 27001** - Information security management systems Requirements
- **ISO/IEC 27002** - Code of practice for information security management
- **ISO/IEC 27003** - Information security management system implementation guidance
- **ISO/IEC 27004** - Information security management Measurement
- **ISO/IEC 27005** - Information security risk management

Hivatalos tájékoztatás az információbiztonsági szabványokról
http://mszt.hu/web/guest/az-informaciobiztonsag-iranyitas-szabvanyai

További ISO szabványok

Információbiztonsági szabványcsalád

- ISO/IEC19011:2018 - Guidelines for management systems auditing
- ISO/IEC 17021 - Management System Certification Bodies

Egységes ISO-struktúra

ISO.ORG kiadott (2012-ben) egy új, egységes követelmény-struktúrát minden újonnan megjelenő / megújuló ISO rendszerszabványra. Ez a koncepció (struktúra) a

HLS (High Level Structure)

- Egységes tartalomjegyzék és követelmény minden egyes ISO irányítási rendszerszabványban.
- Mindegyik szabvány menedzsment elemei ebben a struktúrában vannak meghatározva az adott szabványra értelmezve.
- Mindegyik szabvány egyedi, speciális területének követelményei vagy a szabványtörzsben (kiegészítésként, ha beilleszthető oda), vagy önálló mellékletként beillesztve.

Egységes ISO-struktúra

ISO.ORG kiadott (2012-ben) egy új, egységes követelmény-struktúrát minden újonnan megjelenő / megújuló ISO rendszerszabványra. Ez a koncepció (struktúra) a

HLS (High Level Structure)

1. Alkalmazási terület
2. Rendelkező hivatkozások
3. Szakkifejezések és meghatározások
4. A szervezet környezete
5. Vezetés
6. Tervezés
7. Támogatás
8. Működtetés
9. Teljesítményértékelés
10. Fejlesztés

Az IBIR és a MIR szabvány

MSZ ISO/IEC 27001:2014	MSZ EN ISO 9001:2015
4. A szervezet és környezete – (szervezet, érdekelt felek és IBIR-rel kapcsolatos igényei, IBIR alkalmazási területe és életbe léptetése	**4. A szervezet környezete –** (szervezet, érdekelt felek és MIR-rel kapcsolatos igényei, MIR alkalmazási területe és életbe léptetése)
5. Vezetés – (elkötelezettség, politika, szervezeti szerepek és felelősségek	**5. Vezetés –** (elkötelezettség, politika, szervezeti szerepek és felelősségek)
6. Tervezés – (IB kockázatok és lehetőségek, IB célok)	**6. Tervezés –** (kockázatok és lehetőségek, minőségcélok, változások tervezése)
7. Támogatás – *(erőforrások, felkészültség, tudatosság, kommunikáció, dokumentált információ)*	**7. Támogatás –** (erőforrások, felkészültség, tudatosság, kommunikáció, dokumentált információ
8. Működés – *(IBIR működéstervezés és felügyelet, IB kockázatok felmérése és kezelése)*	**8. Működés –** (termék előállítás / szolgáltatás nyújtás tervezése és szabályozása, tervezés és fejlesztés, outsourcing)
9. Teljesítményértékelés – *(mérés, elemzés, értékelés, belső audit, vezetőségi átvizsgálás)*	**9. Teljesítményértékelés –** (mérés, elemzés, értékelés, vevői elégedettség, belső audit, vezetőségi átvizsgálás)
10. Fejlesztés – *(nemmegfelelőség, helyesbítő tevékenység, folyamatos fejlesztés)*	**10. Fejlesztés** – (nemmegfelelőség, helyesbítő tevékenység, folyamatos fejlesztés)
A melléklet: Intézkedési célok és intézkedések	

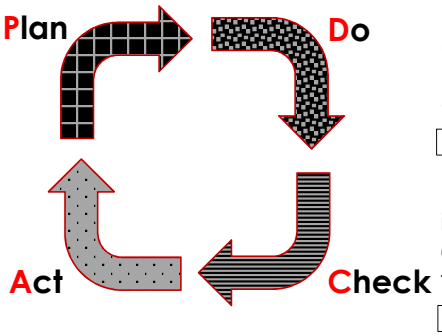
PDCA az irányítási rendszerekben

Irányítási rendszerek intézkedéseinek tervezése

4. A szervezet és környezete
5. Vezetés
6. Tervezés
7. Támogatás

Beavatkozási pont (pl. vezetőségi értékelés, politika, mérés, célok, ….

10. Fejlesztés



Irányítási rendszerek működtetése, folyamatainak, intézkedéseinek végrehajtása

8. Működés

Folyamatok, termékek, irányítási rendszerek ellenőrzése, figyelemmel kisérése

9. Teljesítmény értékelés

Az információvédelmi eljárások megvalósítási területei

- **objektum, terület védelem** – Védi az adatokhoz, adathordozókhoz és azok területeihez való fizikai hozzáférést .
- **személy védelem** – Rendszerben a személy, mint információhordozó védelme, valamint a rendszer védelme az emberi jellegű támadásoktól, visszaélésektől.
- **hagyományos adatok, adathordozók védelme** – Pl. papíralapú információk (titkos ügyiratkezelés, …), analóg berendezések védelme.
- **informatikai védelem** – *Az informatikai rendszerben tárolt adatok védelme.*
- **elemi károk, természeti /társadalmi katasztrófahelyzetek elleni védelem** – Az információbiztonság szemszögéből, az üzletmenet – üzemmenet folytonosságának fenntartása.

ISO/IEC 27001 - „A” mellékletének területei

Hivatkozásul szolgáló intézkedési célkitűzések és intézkedések – „követelmények” vagy „kontrollok”
(Reference control objectives and controls)

A5. Információbiztonsági szabályok
A6. Az információbiztonság szervezete
A7. Az emberi erőforrások biztonsága
A8. Vagyonelemek kezelése
A9. Hozzáférés-felügyelet
A10. Titkosítás
A11. Fizikai és környezeti biztonság
A12. Az üzemelés biztonsága
A13. A kommunikáció biztonsága
A14. Rendszerek beszerzése, fejlesztése és karbantartása
A15. Szállítói kapcsolatok
A16. Az információbiztonsági incidensek kezelése
A17. A működésfolytonosság biztosításának információbiztonsági vonatkozásai
A18. Megfelelés

Összhangban az ISO/IEC 27002:2013 szabvány ajánlásaival

Információbiztonsági követelmények forrásai

- **Kockázatelemzés**, figyelembe véve a szervezet üzleti stratégiáját és célkitűzéseit. Kockázatelemzés során azonosítják az eszközöket fenyegető veszélyeket, értékelik a sérülékenységet és az előfordulás valószínűségét, és becsülik a lehetséges hatásokat.
- **Jogszabályi, szabályozási és szerződéses követelmények**, amelyeknek egy szervezetnek, kereskedelmi partnereinek, vállalkozóknak és szolgáltatóknak meg kell felelniük, valamint társadalmi-kulturális környezetük.
- **Információk kezelésére vonatkozó elvek, célkitűzések és üzleti követelmények**, amelyeket egy szervezet saját működésének támogatására fejlesztett ki.

ISO/IEC 27001 szabványban az IB gyakorlati területei

A5. Információbiztonsági szabályok
A6. Az információbiztonság szervezete
A7. Az emberi erőforrások biztonsága
A8. Vagyonelemek kezelése
A9. Hozzáférés-felügyelet
A10. Titkosítás
A11. Fizikai és környezeti biztonság
A12. Az üzemelés biztonsága
A13. A kommunikáció biztonsága
A14. Rendszerek beszerzése, fejlesztése és karbantartása
A15. Szállítói kapcsolatok
A16. Az információbiztonsági incidensek kezelése
A17. A működésfolytonosság biztosításának információbiztonsági vonatkozásai
A18. Megfelelés

Szabványtörzs:
4 – 10 fejezetek

Menedzsment rendszer követelmények

ISO/IEC 27001 szabványban az IB gyakorlati területei

A5. Információbiztonsági szabályok
A6. Az információbiztonság szervezete
A7. Az emberi erőforrások biztonsága
A8. Vagyonelemek kezelése
A9. Hozzáférés-felügyelet
A10. Titkosítás
A11. Fizikai és környezeti biztonság
A12. Az üzemelés biztonsága
A13. A kommunikáció biztonsága
A14. Rendszerek beszerzése, fejlesztése és karbantartása
A15. Szállítói kapcsolatok
A16. Az információbiztonsági incidensek kezelése
A17. A működésfolytonosság biztosításának információbiztonsági vonatkozásai
A18. Megfelelés

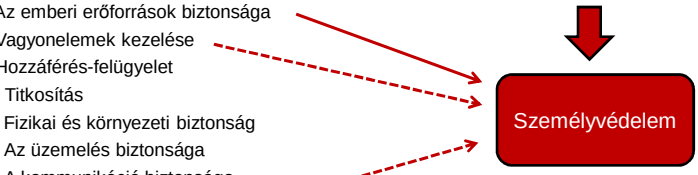
Szabványtörzs:
4 – 10 fejezetek

Terület és objektumvédelem

ISO/IEC 27001 szabványban az IB gyakorlati területei

A5. Információbiztonsági szabályok
A6. Az információbiztonság szervezete
A7. Az emberi erőforrások biztonsága
A8. Vagyonelemek kezelése
A9. Hozzáférés-felügyelet
A10. Titkosítás
A11. Fizikai és környezeti biztonság
A12. Az üzemelés biztonsága
A13. A kommunikáció biztonsága
A14. Rendszerek beszerzése, fejlesztése és karbantartása
A15. Szállítói kapcsolatok
A16. Az információbiztonsági incidensek kezelése
A17. A működésfolytonosság biztosításának információbiztonsági vonatkozásai
A18. Megfelelés

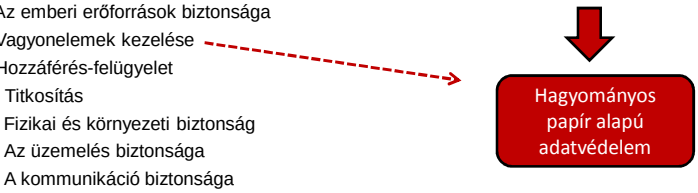
Szabványtörzs:
4 – 10 fejezetek



ISO/IEC 27001 szabványban az IB gyakorlati területei

A5. Információbiztonsági szabályok
A6. Az információbiztonság szervezete
A7. Az emberi erőforrások biztonsága
A8. Vagyonelemek kezelése
A9. Hozzáférés-felügyelet
A10. Titkosítás
A11. Fizikai és környezeti biztonság
A12. Az üzemelés biztonsága
A13. A kommunikáció biztonsága
A14. Rendszerek beszerzése, fejlesztése és karbantartása
A15. Szállítói kapcsolatok
A16. Az információbiztonsági incidensek kezelése
A17. A működésfolytonosság biztosításának információbiztonsági vonatkozásai
A18. Megfelelés

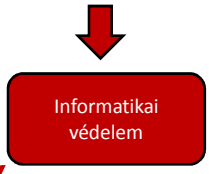
Szabványtörzs:
4 – 10 fejezetek



ISO/IEC 27001 szabványban az IB gyakorlati területei

A5. Információbiztonsági szabályok
A6. Az információbiztonság szervezete
A7. Az emberi erőforrások biztonsága
A8. Vagyonelemek kezelése
A9. Hozzáférés-felügyelet
A10. Titkosítás
A11. Fizikai és környezeti biztonság
A12. Az üzemelés biztonsága
A13. A kommunikáció biztonsága
A14. Rendszerek beszerzése, fejlesztése és karbantartása
A15. Szállítói kapcsolatok
A16. Az információbiztonsági incidensek kezelése
A17. A működésfolytonosság biztosításának információbiztonsági vonatkozásai
A18. Megfelelés

Szabványtörzs:
4 – 10 fejezetek



ISO/IEC 27001 szabványban az IB gyakorlati területei

A5. Információbiztonsági szabályok
A6. Az információbiztonság szervezete
A7. Az emberi erőforrások biztonsága
A8. Vagyonelemek kezelése
A9. Hozzáférés-felügyelet
A10. Titkosítás
A11. Fizikai és környezeti biztonság
A12. Az üzemelés biztonsága
A13. A kommunikáció biztonsága
A14. Rendszerek beszerzése, fejlesztése és karbantartása
A15. Szállítói kapcsolatok
A16. Az információbiztonsági incidensek kezelése
A17. A működésfolytonosság biztosításának információbiztonsági vonatkozásai
A18. Megfelelés

Szabványtörzs:
4 – 10 fejezetek

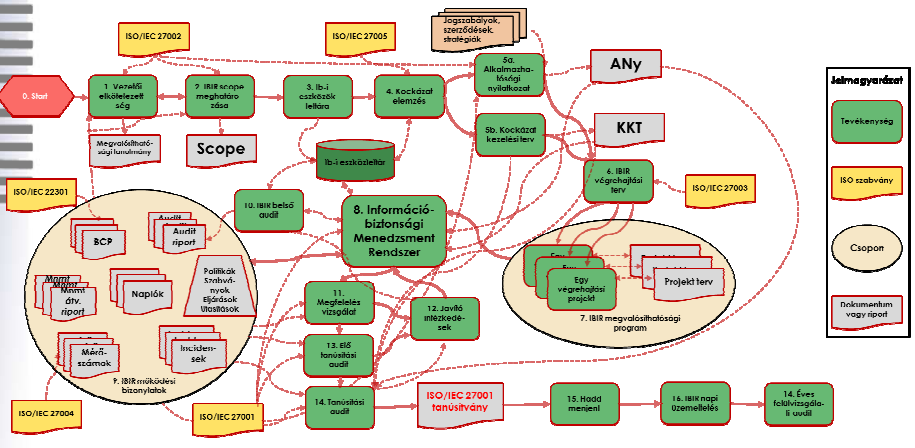
ISO/IEC 27002 Code of practice for information security controls

Szabvány célja:

- referencia eszköz a szervezetek számára a követelmények teljesítéséhez,
- útmutató az auditáló szervezetek számára a követelmények megvalósulásának ellenőrzéséhez,
- irányelveket tartalmaz ipar- és szervezetspecifikus IBIR irányelvek kidolgozásához.

ISO_IEC_27002_2013

ISO/IEC 27003 – IBIR tervezése és bevezetése



Szabványok vs. Tematika fejezetek

Tematika	ISO/IEC 27001	NIST 800-53r4	41/2015 BM
Sérülékenység elemzés és kezelés	A12.6 A műszaki sebezhetőségek felügyelete	SA - System and Services Acquisition	3.1.3. - Rendszer és szolgáltatás beszerzés
Kriptográfiai protokollok	A10. Titkosítás	SC - System and Communications Protection	3.3.13. - Rendszer- és kommunikáció védelem
Határvédelmi technológiák	A13. A kommunikáció biztonsága	SC - System and Communications Protection	3.3.13. - Rendszer- és kommunikáció védelem
Behatolásvédelem	A13. A kommunikáció biztonsága	SC - System and Communications Protection	3.3.13. - Rendszer- és kommunikáció védelem
Üzemeltelés biztonság	A12. Az üzemelés biztonsága	AU - Audit and Accountability CM - Configuration Management CP - Contingency Planning	3.3.12. - Naplózás és elszámoltathatóság 3.3.6. – Konfigurációkezelés 3.1.4. - Üzletmenet (ügymenet) folytonosság tervezése
Fizikai biztonság	A11. Fizikai és környezeti biztonság	PE- Physical and Environmental Protection	3.2. – Fizikai védelem
Dokumentum-védelem	A8 Vagyonelemek kezelése	MP - Media Protection	3.3.8. - Adathordozók védelme

ITIL

ITIL első pillantásra

ITIL - Information Technology Infrastructure Library

bevált gyakorlatot leíró kiadvány az IT szolgáltatás-menedzsment (ITSM) terén

- világszerte a legszélesebb körben elismert **keretrendszer az ITSM számára**
- sok száz szervezet használja

nem szabvány, amelyet be kell tartani

- ajánlott tanulmányozni és **megérteni**, hogy
- **érték keletkezzen** a szolgáltató és ügyfelei számára, és hogy
- **testre lehessen szabni**, hogy konkrét környezetekben működni tudjon

az **ISO/IEC 20000 formális és általános szabvány**

- azon szolgáltatók számára, akik **demonstrálni** szeretnék a **képességeiket** a szolgáltatásmenedzsment terén

az **ITIL-nek együtt kell fejlődnie** azzal, ahogy a technológiák és az üzleti gyakorlat fejlődnek (1987 óta)

ITIL első pillantásra

2007 – az ITIL **második nagy frissítése**, hogy

- feleljen meg a **kiszervezés**, **osztott szolgáltatások**, **közműszerű számítástechnika**, **szerverpark-alapú számítástechnika**, **virtualizáció**, **webszolgáltatások** és **mobilkereskedelem** kihívásainak
- a folyamatalapú megközelítés kiegészüljön a **szolgáltatási életciklussal**

2011 – az alapkiadványok aktualizálása, hogy még **egységesebbek legyenek**

Újra megújuló ITIL

- **2019**: **ITIL alapszintű útmutató**
- **2020: ITIL részletes útmutatók** amely kiterjed (többek közt)
- **Ipar 4.0 forradalom** követelményei
- **globális felhőszolgáltatások**
- **IoT/blokklánc technológiák**
- **agilis / karcsú megközelítések** nemcsak egyszerű, de komplex környezetekben is

ITIL előnyei

Olyan gyakorlatot alakít ki, amely lehetővé teszi a szervezetek számára, hogy **hasznot** termelhessenek, a befektetéseik **megtérüljenek** és **fenntartható sikereket** érhessenek el

- **érték** teremtése az ügyfeleknek szolgáltatásokon keresztül
- a szolgáltatásra irányuló stratégia **integrálása** az üzleti stratégiával és ügyféligényekkel
- az IT-szolgáltatások és a szolgáltató **teljesítményének** a mérése, megfigyelése és optimalizálása
- az IT-**befektetések és -költségvetés** kezelése
- a **kockázatok** kezelése
- az **ismeretek** kezelése
- a **képességek és erőforrások** kezelése az eredményes és hatékony szolgáltatásnyújtás érdekében
- **standard megközelítések** befogadásának elősegítése a szolgáltatásmenedzsment terén az egész szervezetben
- a **szervezeti kultúra** megváltoztatása fenntartható sikerek elérése érdekében
- az **ügyfelekkel** való kapcsolattartás és az egész viszony javítása
- a **javak és szolgáltatások** nyújtásának koordinálása az értékhálózaton keresztül
- a **költségek** optimalizálása és csökkentése

A szolgáltatásmenedzsment fogalma

Szolgáltató: olyan szervezet, amely egy vagy több, belső vagy külső ügyfélnek nyújt szolgáltatást

Szolgáltatásmenedzsment: olyan speciális **szervezeti képességek** létrehozása és fenntartása, amelyek szolgáltatások formájában **értéket adnak az ügyfelek számára**

A szolgáltatásmenedzsmentet elősegítő tényezők:

- hagyományos **szolgáltatási (üzleti) területek** megléte, működése
- a **szolgáltatás-orientált megközelítés** IT-szervezetek általi befogadása
- **üzleti modellek**, stratégiák és tevékenységek **támogatása** szolgáltatásokkal
- a **megosztott szolgáltatások** és a **kiszervezés** terjedése

Az IT-szolgáltatásmenedzsment fogalma

Az informatika különböző nézőpontokból

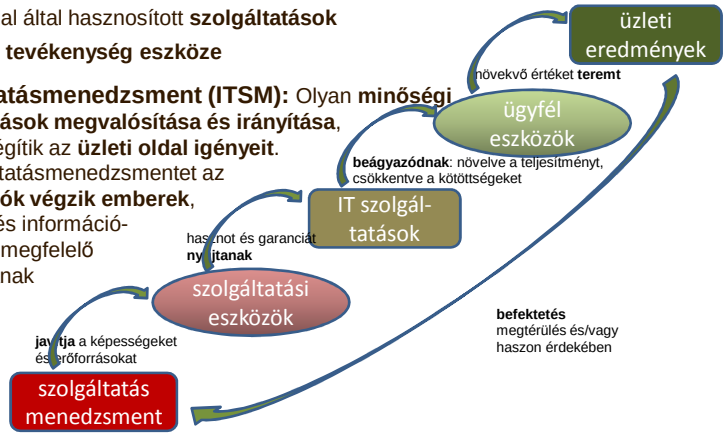
rendszerek, alkalmazások és infrastruktúrák **összessége**

szervezet, amely **képességek és erőforrások** adott körével rendelkezik

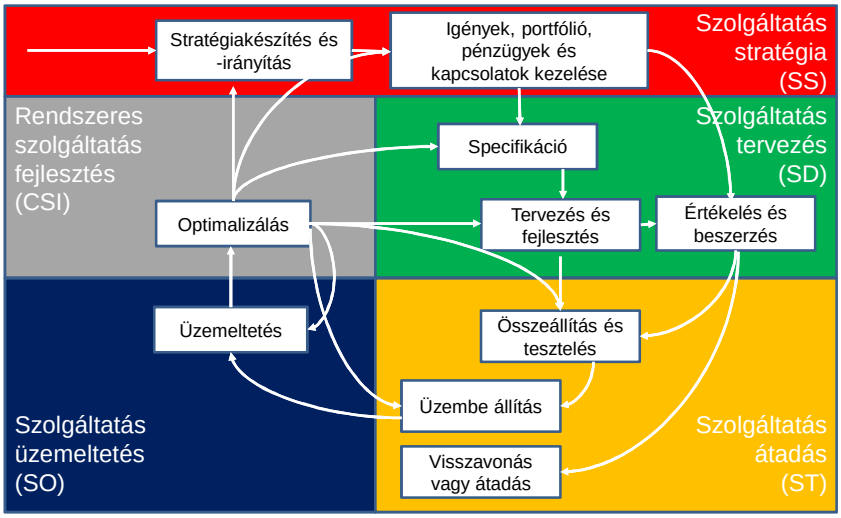
üzleti oldal által hasznosított **szolgáltatások**

az üzleti tevékenység eszköze

IT-szolgáltatásmenedzsment (ITSM): Olyan **minőségi IT-szolgáltatások megvalósítása és irányítása**, amelyek kielégítik az **üzleti oldal igényeit**. Az IT-szolgáltatásmenedzsmentet az **IT-szolgáltatók végzik emberek**, **folyamatok** és információ-**technológia** megfelelő kombinációjának segítségével.



Az életciklus-megközelítés



COBIT

ISACA: https://engage.isaca.org/budapestchapter/aboutchapter/about

COBIT

ISACA (Information **S**ystems **A**udit and **C**ontrol **A**ssociation**) (www.isaca.org):** nemzetközi szakmai szövetség, amely az IT irányításával foglalkozik..

COBIT (Control **Ob**jectives for **I**nformation and Related **T**echnology**):** vállalati IT irányítás és menedzsment üzleti keretrendszere

Az ISACA a COBIT® 5 kiadványt **elsődlegesen oktatási anyagnak** szánja vállalati IT irányítási, bizonyosságnyújtási, kockázatkezelési és biztonsági szakemberek számára. Az ISACA nem állítja, hogy a módszertan bármely részének felhasználása pozitív eredményekhez vezet.

Információ

Az információ és a technológia által hordozott előnyök a vállalkozások számára:

- az információ minden vállalkozás számára kulcsfontosságú erőforrás,
- az információ létrehozása, felhasználása, megőrzése, elosztása és megsemmisítése,
- a technológiának kulcsszerepe van ezen tevékenységekben,
- a technológia az üzleti és a személyes élet minden területén elterjedt.

Control **Ob**jectives for **I**nformation and Related **T**echnology

Vállalati előnyök

A vállalkozások és vezetőik arra törekszenek, hogy:

- **jó minőségű információt** biztosítsanak üzleti döntések támogatásához,
- **üzleti értékeket teremtsenek** az IT támogatásával megvalósuló befektetések által, azaz elérjék stratégiai céljaikat, valamint üzleti hasznot hajtsanak az IT eredményes és innovatív felhasználásával,
- **működési kiválóságot érjenek** el a technológia megbízható és hatékony alkalmazásával,
- **elfogadható szinten** tartsák az IT használatából eredő **kockázatokat**,
- **optimalizálják** az IT szolgáltatások és a technológia **költségeit**,
- **betartsák** az egyre nagyobb számú **jogszabályt, szabályozást, szerződéses kötelezettséget és szabályzatot**.

Döntéshozói érték

- A döntéshozói értékének megteremtéséhez **megfelelő irányításra** és az információs és technológiai (IT) eszközök **kezelésére** van szükség.
- Az **IT-nak részének kell lennie az** igazgatóságnak és a felsővezetésnek, ugyanúgy mint a vállalkozás bármely más jelentős területének.
- Az információ és technológia vállalati felhasználásával kapcsolatos külső **jogi, szabályozási és szerződéses követelmények** növekszenek, és megsértésük fenyegetést jelentenek.
- **A COBIT 5 átfogó keretet nyújt, amely segíti a vállalkozásokat céljaik elérésében és az értéknövelésben a vállalati informatika hatékony irányítása és menedzselése révén.**

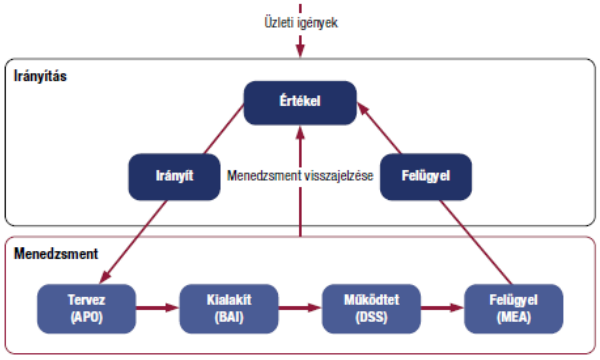
COBIT 5 keretrendszer

A COBIT 5 **általános érvényű** és hasznos bármilyen méretű szervezet számára, az üzleti, a nonprofit és az állami szektorban egyaránt.

A COBIT 5 a vállalati IT irányítás és menedzselés **öt alapelvén** nyugszik:

1. alapelv: **Az érdekelt felek igényeinek kielégítése**
2. alapelv: **Kiterjesztés a teljes vállalatra**
3. alapelv: **Egységes, integrált keretrendszer alkalmazása**
4. alapelv: **Átfogó megközelítés megvalósítása**
5. alapelv: **Az irányítás és menedzsment szétválasztása**

Az irányítás és menedzsment kulcsfontosságú területei



COBIT 5 célhierarchia használata

A célhierarchia azért **fontos**, mert segítségével meghatározhatjuk a vállalat (stratégiai) célkitűzéseire, és a kapcsolódó kockázatokra alapozott vállalati IT irányítás megvalósításának, fejlesztésének, és bizonyosságnyújtásának prioritásait.

7 megvalósítási tényező

1. Az **alapelvek, szabályzatok és keretrendszerek** gyakorlatias útmutatást nyújtanak a mindennapi menedzsment tevékenységekhez
2. Az **eljárások** meghatározása, amelyek az átfogó célok megvalósulását elősegítő egyedi eredmények és célok megvalósításához szükségesek.
3. A **szervezeti struktúrák** határozzák meg a szervezeti egységeket a vállalati döntéshozatalhoz.
4. Az egyéni és vállalati **kultúra, etika és viselkedés** irányítási és menedzsment sikertényező.

7 megvalósítási tényező

5. Az **információ** a szervezet minden részében jelen van és kiterjed minden, a vállalat által előállított és a felhasznált információra.
6. A **szolgáltatások, infrastruktúra és alkalmazások** magukba foglalják az információfeldolgozást és IT-szolgáltatásokat biztosító vállalati infrastruktúrát, technológiát és alkalmazásokat.
7. Az **emberi erőforrás, készségek és képességek** az emberekhez kötődnek, és elengedhetetlenek a tevékenységek sikeres végrehajtásához, a helyes döntések meghozatalához és a korrekciós folyamatok végrehajtásához.

COMMON CRITERIA (ISO/IEC 15408)

Mi az a Common Criteria?

Common Criteria:

- egy nemzetközileg elfogadott informatikai biztonsági követelményrendszer
  - közös struktúra és nyelv a termékek/rendszerek az IT követelmények kifejezésére
  - szabványos IT biztonsági követelmény összetevők és csomagok gyűjteménye
- nemzetközileg elfogadott értékelési módszertan, besorolási rendszer,
- ISO szabvány (ISO / IEC 15408)

https://www.commoncriteriaportal.org

Mire használható a Common Criteria?

Common Criteria:

- olyan IT rendszerek és termékek **biztonsági tulajdonságainak a specifikációja**, melyek a következőket valósítják meg: bizalmasság, sértetlenség, rendelkezésre állás,
- független értékelések **eredményeinek az összehasonlíthatóságára**,
- hardverben, szoftverben és förmverben implementált **védelmi intézkedésekre** vonatkozó
  - technológia független,
  - és a fejlesztő által kívánt kombinációk **meghatározására**.

Minősített termék típusok

- hozzáférés-vezérlő eszközök és rendszerek (pl. SSO)
- határvédelmi eszközök és rendszerek (pl. tűzfalak)
- adatbázis kezelők
- adatvédelmi eszközök (pl. kriptográfiai titkosító eszközök)
- észlelő eszközök és rendszerek (pl. IDS)
- IC-k, intelligens kártyák, és ezekhez kapcsolódó rendszerek
- kulcs menedzsment rendszerek (pl. PKI) rendszerek
- hálózati és hálózathoz kapcsolódó eszközök és rendszerk (pl. VPN rendszerek)
- operációs rendszerek
- elektronikus aláíró rendszerek
- egyéb eszközök és rendszerek

Koncepció

Védelmi profil (Protection Profiles - PP)

Egy adott kiértékelési céltárgy (TOE - Target of Evaluation) kategóriájára vonatkozó megvalósítás független biztonsági követelmények halmaza, amelyek kielégítik a felhasználó igényeit.

Biztonsági cél (Security Target – ST)

A biztonsági követelményeknek és specifikációnak egy olyan halmaza, amely egy meghatározott vizsgálati céltárgy kiértékelésének alapjául használandó.

CC felépítése

Biztonsági funkcionális követelmény (Security Functional Requirements) osztályok:

- naplózás,
- azonosítás és hitelesítés,
- erőforrás-felhasználás,
- kriptográfiai támogatás,
- biztonságkezelés,
- TOE hozzáférés,
- kommunikáció,
- adatvédelem,
- megbízható útvonal / csatornák,
- felhasználói adatok védelme,
- TOE biztonsági funkcióinak védelme.

CC felépítése

Biztonsági garancia követelmény (Security Assurance Requirements) osztályok:

- konfigurációkezelés
- használati útmutatók
- sérülékenység értékelése
- szállítás és üzemeltetés
- élettartam-támogatás
- biztosítékok karbantartása
- fejlesztés és teszt

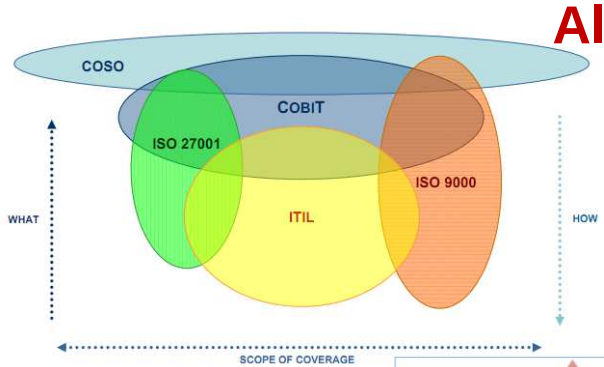
CC felépítése

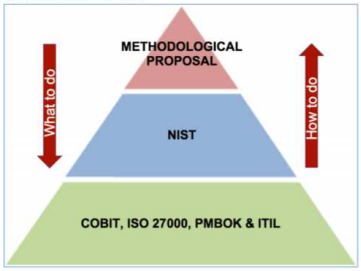
Garanciális szint (Evaluation Assurance Level - EAL) osztályok, fejlesztés biztonságára vonatkoznak:

- EAL 1: Funkcionálisan tesztelve
- EAL 2: Strukturálisan tesztelve
- EAL 3: Módszeresen tesztelve és ellenőrizve
- EAL 4: Tervszerűen tervezve, tesztelve és átnézve
- EAL 5: Félformálisan tervezve és tesztelve
- EAL 6: Félformálisan igazolt módon tervezve és tesztelve
- EAL 7: Formálisan igazolt módon tervezve és tesztelve

IRÁNYÍTÁSI RENDSZEREK HASZNÁLATA

Alkalmazás





COSO - Committee of Sponsoring Organisations

Alkalmazás

- A COBIT akkor jó jelölt, ha egy szervezet az egész szervezetre kiterjedő keretet kíván létrehozni a menedzsment számára, amelynek nem része az információbiztonság. Noha nem nyújt közvetlen tanúsíttatást.
- Az ITIL az ISO szabványokra épül, mint keretekre a megoldás megvalósításához. Igy alkalmas azoknak a szervezeteknek, amelyek a járatos ISO-szabványokat akarják használni, anélkül, hogy szükségszerűen el kellene érniük az ISO 27001 tanúsítványt.
- Az ISO 27002 (ISO 27001) társított tanúsítása világszerte elismerést és elfogadást nyújt, ezért a nemzetközi határokon átnyúlóan működni kívánó szervezetek előnyösnek találhatják a bevezetést és a tanúsítást. Ezenkívül néhány ISO 27001 tanúsítvánnyal rendelkező vállalat megköveteli a partnerek tanúsítását is.

Alkalmazás

- Az amerikai kormányzati szervezetek kötelesek a NIST-t használni a szövetségi törvények betartása érdekében. Ezenkívül **nem szövetségi szervezetek is használhatják a NIST szabványt**, de más szabványok, például az ISO 27002 vagy az ITIL alkalmasabbak lehetnek, mivel a NIST-t egyes szervezeteknél nehéz lehet bevezetni.

NIST használata még:

NIST – IoT
NIST - Cloud

Olvasnivalók

Célszerű a hivatkozott honlapokon körülnézni és a dokumentumokba belenézni.