Bevezetés az informatikai ellenőrzésbe

Dr. Szenes Katalin, CISA, CISM, CGEIT, CISSP, PhD

Óbudai Egyetem
Neumann János Informatikai Kar

szenes.katalin@nik.uni-obuda.hu

tartalomjegyzék

mi lesz, ha dolgozni kezdünk?
mi van a világban?
EU lép, USA ballag?, ma is ható fontos hírek

- átváltozott az ENISA
- (GDPR)
- (PSD2)
- (blockchain)

mi értelme az informatikai ellenőrzésnek?
folyamatok, szereplők, ellenőrzési célok / intézkedések
fontos források
- egy kis Amerika

audit / biztonság → kormányzás (governance)
kormányzás ← audit / biztonság

földhözragadt, egyszerű példák megoldandó feladatokra

tartalomjegyzék

mit kell megvédeni, és mivel? - alapszint, alapdefiníciók

MIT:

- társasági vagyon
- vállalati információ(s) rendszer
- egy biztonság definíció

MIVEL:

informatikai biztonsági / ellenőrzési alapdefiníciók

- ellenőrzési cél - működési cél
- ellenőrzési eljárás - működési intézkedés

tartalomjegyzék

FONTOS további SEGÉDLETEK:

alapkritériumok
- bizalmasság
- rendelkezésre állás
- integritás

középszint: a COBIT információkritériumai - és a COSO definíció

felső szint:
- **működési kiválósági kritériumok**
- az erőforrások kiváló kezelésének kritériumai

ebből kötelező lesz: !! funkcionalitás és dokumentáció

az intézményi működés 3 alappillére:
szervezet, szabályozás és technika

tartalomjegyzék

a biztonság és a stratégia kapcsolata
- stratégia - kockázat - kritérium - intézkedés

↓
stratégiai fontosság
↓
üzleti folyamat fontosság
↓
támogató folyamat fontosság
↓
IT alkatrészek fontossága

(rangsorolunk, kiválósági kritériumokat teljesítünk, néha elszúrjuk milyen a jó rendszerterv?)

(ellenőrzési) intézkedés / eljárás fajták
- megakadályozó, vizsgálati, javító

példa vállalati szemléletre
- vállalat információrendszerének felmérése IBM BSP módszerrel

Bevezetés az informatikai ellenőrzésbe - Szenes 5

tartalomjegyzék

az ellenőrzés és az informatikai ellenőrzés

egy kicsi a governance-ról

ellenőrzés fajták

az ellenőrzés vizsgálatának szempontjai - az ellenőrzés auditálása
- és a felső vezetés

felelőssége

példák

auditálási kockázatok

az audit fázisai - egy lehetséges verzió

Bevezetés az informatikai ellenőrzésbe - Szenes 6

tartalomjegyzék

néhány USA-ban indult minősítő szervezet és minősítés

hasznos források
- rengeteg segítség

nemzetközi és hazai szabványok

további támogató szabványok, módszertanok, irodalom

néhány magyar szakmai szervezet

mi less, ha dolgozni kezdünk?

informatikai ellenőrzés

➔ ➔

informatikai biztonság

➔ ➔

informatika

➔ ➔

üzleti szakterület

mi van a világban - EU lép

May 13, 2022 — The **Council** and **the European Parliament** have agreed on measures for a high common level of **cybersecurity** across the Union.

Jun 28, 2022 — The **Council** presidency and **the European Parliament** reached a political agreement on the **directive** on the resilience of critical entities.

Mi ez a NIS?

security of network and information systems

- bank, pénzügyek – nem újdonság
- de ezeken kívül még:
- egészségügy
- szállítmányozás
- gyártás
- szennyvízkezelés
- űrkutatás, stb.

mi van a világban – USA ballag?

kérdezem én:
NIST Cybersecurity Framework 2022
erre Google:
https://www.nist.gov/cyberframework/newsroom/latest-updates

2022. augusztus 17-én workshop, hogy felújítsák:
""Beginning our Journey to the NIST Cybersecurity Framework 2.0"

és mi van, pl.:

- Draft NISTIR 8286D, *Using Business Impact Analysis to Inform Risk Prioritization and Response*
- Draft NISTIR 8286C, *Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight*, is now available for public comment!
- a "new executive order on cybersecurity" mőgé nézve is 2021-est látok – lehet, rosszul látom

mi van a világban - amivel szerintem tele a padlás

MÁR UNJUK:

hacking
- személyi azonosító lopás
- DDOS támadások
- és egyéb, az IT üzemeltetés és fejlesztés hibáit kihasználó támadások

malware
- virus
- ransomware - zsarolóvírus
- ügyfelek hiszékenységének kihasználása
  valószínű, hogy nem nyugszik az öreg törzsfőnök,
  kincsekkel együtt, a tölgyfa alatt

social engineering
- Jancsi vagyok, a HelpDesk-től, karbantartunk, mondd meg a jelszavad

és mégse megyünk most rögtön haza **./.**

Bevezetés az informatikai ellenőrzésbe – Szenes 11

mi van a világban - ma is ható fontos hírek

átváltozott az ENISA

2004.
European Network and Information Security Agency.

az informatikai biztonság, és azon belül elsősorban a hálózati biztonság
[szakértői központja]

majd további névváltoztatás, most:
European Union Agency for Cybersecurity
https://www.enisa.europa.eu/news/enisa-news/the-eu-cybersecurity-act-a-new-era-dawns-on-enisa

2019. június 27-től hatályos:
EU Cybersecurity Act

(forrás: Az Európai Únió Hivatalos Lapja Magyar nyelvű kiadás Jogszabályok L151 62. évfolyam, 2019. június 7. ISSN 1977-0731)

Bevezetés az informatikai ellenőrzésbe – Szenes 12

"AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/881 RENDELETE(2019. április 17.)az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály)"

mindenki lesz szíves mindent megtenni,

az ENISA pedig ad:

- szakértelmet, tanácsadást
- támogatást, stb.

és itt a lényeg:

"az európai kiberbiztonsági tanúsítási rendszerek kidolgozása során az ENISA-nak rendszeresen konzultálnia kell a szabványügyi szervezetekkel, különösen az európai szabványügyi szervezetekkel"

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

(GDPR - EU General Data Protection Regulation**)**

A GDPR szerinti alapvető változások az EU adatvédelmében (2016 / 679 EU)

megjegyzés: Magyarországon már 1992. évi LXIII. tv.

de: NAIH elnökhelyettes: fontos a hatály

a személyes adatok **gyűjtéséhez való beleegyezés** szigorúbb követelményei

a belegyezés **korhatárának** emelése 13-ról 16 évesre

ha már nem használja az intézmény a gyűjtött adatot, ha a **gyűjtés oka megszűnik**,
törölnie kell

ha valaki **visszavonja a beleegyezését**, adatát törölni kell

(GDPR - EU General Data Protection Regulation**)**

az adatvédelmi incidensről 72 órán belül értesíteni kell az EU megfelelő hatóságát
(az MNB-nek a pénzintézetek jelentik)

nemzeti **hivatalt** kell alapítani a GDPR-rel kapcsolatos panaszok felügyeletére (monitor?) és kezelésére

a sok érzékeny adatot kezelő, vagy a sok ügyfél viselkedését figyelő intézményeknek **adatvédelmi felelőst** kell kinevezniök
€ 20m-ig, vagy a bevétel 4%-ig terjed a bírság a meg nem felelésért

💣 ennek az intézmények számítógépes rendszerére a hatása

(PSD2)

amivel nincs problémám:
a biztonsági követelmények - persze nem így

de amivel van:
AISP - Account information service providers- ezeknek elég, ha regisztrálnak, csomú kivétel pénzmosási, auditálási követelmények alól

TPP (third-party payment service providers) ➔➔ bank
- ha hiba van, az a bank kockázata,
- és a banké a bizonyítási kötelezettség,
- vevői panasznál a banknak kell meghiteleznie a kérdéses összeget

ha a TPP nem ismeri el hibáját, a banknak pechje van

ld.: EBA/GL/2017/09 11/07/2017 final report
szerintem egyetlen megoldás: csatlakozási app felkínálása

(a kripto és a blockchain
- ez lényegében gráfszerű, a szögpontokban a vagyonokkal)

bank:
- ismert: az ügyfél
- titok: az egyenleg

crypto:
- a vevőt egy privát kulcs "jelképezi"
- az egyenleget mindenki láthatja, sőt, látnia kell

ez az átláthatóság biztosítja, ha biztosítja, hogy megvan a pénzünk

az adat valódiságának elfogadása az ügyféltől függ, hiszi-e

EU: habozás és zűrzavar
szabályozni, vagy nem szabályozni, ez itt a kérdés
vannak tervek a szabályozásra, kell is, névtelenség ➜ pénzmosás, terrorizmus, stb.

egész EU-t árfogó blockchain adatbázis?
megbízhatóan kell szabályozni az adat, és a tranzakciók környezetét
https://www.coindesk.com

Bevezetés az informatikai ellenőrzésbe - Szenes 17

mi értelme az informatikai ellenőrzésnek?

adott: egy intézmény
szeretnénk: ha megmaradna
➜ muszáj: fenntarthatóan fejlődnie

első cselekvő: corporate management
(ez NEM enterprise management system)
intézményi stratégia, lehetőleg még indulás előtt
➜ stratégia megvalósítása: miből óhajtunk megélni? ➜ üzleti modell
➜ üzleti célok & folyamatok - ne maguktól alakuljanak
\+ működéstámogató folyamatok, pl. controlling,logisztikai, HR, IT, etc.

a folyamatok működése támogatására: intézményi információ(s?) rendszer
(ennek része lehet az enterprise information system)
⬇
és ennek támogatására: számítástechnikai rendszer
(jó, ha az üzleti modell architektúráját tükrözi)

Bevezetés az informatikai ellenőrzésbe - Szenes 18

folyamatok, szereplők, ellenőrzési célok / intézkedések

legfelső vezetés: mindent irányít & felügyel
(delegálhat, de a felelősség marad)
a felügyeletet támogatja: az ellenőrzési részleg HOGYAN?

üzleti szakterületek
- üzleti folyamatok ➜ üzleti célok / intézkedések
- vezetők
- beosztottak - (feladat - munkaköri leírás: U szerepkörök)

támogató szakterületek
- támogató folyamatok ➜ támogatási célok / intézkedések
- vezetők
- beosztottak - (feladat - munkaköri leírás: U szerepkörök)

IT eset - ráadásul az IT részleghez:
inf. biztonság: informatika strat. v. azt szolgáló céljait
gyakorlati célokra / intézkedésekre
informatikai ellenőrzés:
a stratégiai célokat gyakorlati "ellenőrzési" célokra / -intézkedésekre

fontos források

ISACA, COSO, ISC2, ISO, NIST, SEC, Cloud Security Alliance, Wi-Fi Alliance, Payment Card Industry Data Security Standard, Oasis-open, ...

www.isaca.org - Information Systems Audit and Control Association
CRM - CISA Review Technical Information Manual
COBIT: Control Objectives for Information Technology

- CISA – Certified Information Systems Auditor,
- CISM - Certified Information Security Manager,
- CGEIT - Certified in Governance Enterprise IT

www.isc2.org - International Information Systems Security Certification Consortium

- CISSP - Certified Information Security Professional
- CCSP - Certified Cloud Security Professional

www.coso.org

egy kis Amerika:

Securities Act of 1933, Securities Exchange Act of 1934
de a múlt században megint: Sarbanes-Oxley Act of 2002 - SOX

COSO: Committee of Sponsoring Organisations of the Treadway Commission

1985-ben alakult, a pénzügyi jelentésekkel kapcsolatos csalások nemzeti bizottságának (National Commission on Fraudulent Financial Reporting) támogatására. Ezt a bizottságot röviden gyakran csak "Treadway bizottságnak" nevezik, első elnökéről, James C. Treadway, Jr.-ról.

A Treadway bizottság a magánszektor kezdeményezésére alakult. Annak alapján készít ajánlásokat a tőzsdei társaságok, azok auditorai, a SEC (Security Exchange Committee), és más szabályozó szervezetek, és oktatási intézmények részére is, hogy tanulmányozzák a csaló pénzügyi jelentések sajátosságait.

ld. Informatikai biztonsági kézikönyv, Verlag Dashöfer, Budapest

audit / biztonság → kormányzás
kormányzás ← audit / biztonság
↓
informatikai biztonsági és ellenőrzési módszerek, módszertanok, ötletek kiterjesztése a vállalatirányítás, a működés, és a kockázatkezelés támogatására

a biztonság / audit alapdefinícióinak stratégiai szintre emelése

A vállalati információrendszer biztonságának követelményei
- **piaci érvényesülés**
- **biztonság szempontjából**

a rendszerszervezés kulcsszerepe
pl. módszereinek alkalmazása megfelelőség elérése / vizsgálata

- **kockázatkezelés ☞ osztályozás ☞ adattulajdonos ☞ …**
- **kötelességelhatárolás**
- **kiszervezés**

földhözragadt, egyszerű példák megoldandó feladatokra

biztonsági példa: rendszergazda otthonról
- hackeléssel
- social engineering-gel

gyógyszer lesz:
- biztonságos vállalati hálózati toplógia
- oktatás
- biztonsági - ellenőri segítség
- stb.

stratégiai példa: kiszervezés
- belsők több pénzért kimennek
- onnan aztán továbbállnak
- és most kell új partner - hogyan válasszunk, és
- milyen legyen az EGÉSZ folyamat ?

az állatorvos idei beteg lova:
- hogyan blamálja magát egyszerre vevő és szállító?

Bevezetés az informatikai ellenőrzésbe - Szenes 23

mit kell megvédenünk:

a társasági vagyon:

stratégiai, védelmi és biztonsági szempontból:
- az információrendszer
- az értékrendszer

+ mit kell elérnünk: fenntartható fejlődés

tehát
- a stratégiai célok elérését kell támogatnunk

mi most ezzel az eszközrendszerrel próbálkozunk elsősorban:

a vállalati információ(s ?) rendszer:
- a vállalat céljait szolgáló belső és külső kommunikációs kapcsolatok
- transzformációs eljárások
- eljárási szabályok, és
- az ezeket támogató

számítástechnikai rendszerek összessége

emlékszünk az integrált vállalati információs rendszerekre?

Bevezetés az informatikai ellenőrzésbe - Szenes 24

Mit jelent a biztonság - úgy "általában"?

Egy ***lehetséges*** biztonság definíció Vasvári Györgytől:

A követelmények
előre meghatározott szinten
teljesülnek,

ettől a szinttől csak
előre meghatározható,
előre jelezhető
- mértékű
- valószínűségű

eltérés engedélyezett.

HF.: Mondjunk erre példát!

biztonság ☞☜ stratégia

Alapszint - alapdefiníciók

az ***információrendszer*** biztonsága ALAPSZINTEN
a számítástechnikai, ***és !*** a manuálisan
kezelt üzleti és működési információ

- mérhető mértékű és
  ismert kockázatú rendelkezésre állása
- integritása
- bizalmassága.

ezek az ISACA és az ISO/IEC szabványok közös követelményei

„alapszintű pótfeltételek": funkcionalitás, dokumentáció

működési */ IT* "**ellenőrzési" cél** *(már a COBIT 5-ből kihagyták, 2019-ben sincs)*
saját értelmezésem:
stratégiai célból levezetett/ támogatására alkalmas
➜ a kiváló (akár informatikai) működést **támogató** cél.

nem az ellenőr célja! (ő csak segít, akár az IT biztonság)

Alapszint - alapdefiníciók

működési / "ellenőrzési" intézkedés:
saját értelmezésem:

a működési / "ellenőrzési" cél eléréséhez ***hozzájáruló***
intéskedés, másnéven tevékenység

működési / "ellenőrzési" eljárás:
saját definíció + értelmezés:
működési / ellenőrzési intézkedések sorozata

stratégiai célokhoz, mint gyökérhez tartozó GRÁFok szögpontjai:
célok - részcélok - tevékenységek (ellenőrzési intézkedések)

a működési kiválóság

a biztonságot és az intézményi stratégiát egyaránt szolgálja !

az alap kritériumok jelentése

The information (or any kind of asset)
is ***confidentially*** *handled*,
if those, and only those have *access* to it, who have job to do with it.

az információ (vagy bármilyen vagyontárgy) ***bizalmas*** kezelése:
annak van hozzáférése, akinek dolga van vele

általában a jogosultságkezelésre szűkítik le
annak van jogosultsága ...
félrevihet

gyakran keverik az integritással

Hf.: mondjanak példát

az alap kritériumok jelentése

Availability of the information means, that
if it concerns a *given matter*,
then
it is available to every *competent* employee, who is competent in this matter,
in a *planned*, *predictable,* and *documented* way
according to the *preliminary* agreements on its availability.

az információ akkor **áll rendelkezésre**,
egy adott ügy szempontjából:
ha mindegyik dolgozónak, aki az adott ügyben kompetens, rendelkezésére áll,

- előre tervezett,
- előre jelezhető [mértékben, időben, stb.]
- dokumentált módon,
- az előzetes megegyezés(ek) szerint.

Hf.: mondjanak példát

az alap kritériumok jelentése

integritás:

The *integrity of the information* is preserved,
if its handling or processing *does not change it inadvertently*.

a vagyonelem (pl. információ) ***integritása*** akkor marad meg, ha
- kezelése
- feldolgozása

véletlen módon
nem változtatja meg.

gyakran összekeverik a bizalmassággal

Hf.: mondjanak példát

Középszint - COBIT

ISACA COBIT módszertana szerinti
(Control Objective for Information Technology)
információ kritériumok (a magyar neveket én adtam):

- a célnak való megfelelés - célravezető információ - effectiveness
- eredményesség, hatékonyság - efficiency
- bizalmasság - confidentiality
- integritás, sértetlenség - integrity
- rendelkezésre állás - availability
- külső követelményeknek való megfelelés - compliance
- megbízhatóság - reliability

COSO: (itt is kevert az adat és a feldolgozás, a cél, és elérése)

Effectiveness and efficiency of operations.
Reliability of financial reporting.
Compliance with applicable laws and regulations.

Felső szint: kiterjesztés értelmezésben és hatókörben - saját

működési kiválósági kritériumok
jellemzik:
- az intézményi kormányzás minőségét
- a működési kiválóságot

a működési / működés
- hatékonysággal,
- intézkedések célravezető jellegével,
- (mindenkinek - stakeholder + all) megfelelő funkcionalitásával,
- megbízhatóságával
- külső és belső előírásoknak való megfeleléssel,
- kockázatkezelés kiválóságával,
- *renddel*

a rend alkotóelemeiből:
- *dokumentáltság*
- változás kezelés
- üzletmenet folytonosság tervezés / spec.: informatikai
- stb.

Felső szint: kiterjesztés értelmezésben és hatókörben - saját

az erőforrások kiváló kezelését jellemző
kritériumok:

- az intézményi kormányzás minőségét (szintén)
- a működési kiválóságot (szintén)
- a vagyontárgyak (pl. információ) kezelésének kiválóságát

ezek a régi CCTA (Central Computer and Telecommunications Agency), BSI (British Standards Institution), ISO (International Organization for Standardization), stb. követelmények

- rendelkezésre állás - availability
- bizalmasság - confidentiality
- integritás, sértetlenség - integrity

szintén kiterjeszthetőek
- értelmezési tartományban és
- hatókörben

hogyan definiáljuk ezeket, milyen alapzaton működjenek?

saját definícók, de lehet használni

hasznos szögpontok
a problémamegoldási erdő gráfjaiban

működési kiválósági kritériumok

- hatékonyság, eredményesség - efficiency
  az 1 vagy több adott cél / intézkedés / esetleg folyamat
  - javításához, továbbfejlesztéséhez
  - az emberi, anyagi erőforrásokat optimálisan használjuk ki,
    - pl. termelékenyen, gazdaságosan
      - előre tervezett
      - dokumentált módon

- megfelelés, célravezető intézkedések - effectivity, effectiveness
  az 1 vagy több adott célhoz / intézkedéshez / esetleg folyamathoz
  - releváns információ,
  - a megfelelő időben áll rendelkezésre,
  - korrekt,
  - konzisztens,
  - használható

működési kiválósági kritériumok

- funkcionalitás - functionality - saját kritérium
  az 1 vagy több adott célhoz / intézkedéshez / esetleg folyamathoz
  - adekvát cél / intézkedés / esetleg folyamat

- megbízhatóság - reliability
  az 1 vagy több adott célhoz / intézkedéshez / esetleg folyamathoz

egy információ, ill., egy intézmény teljes információS rendszere megbízható, ha

- az információ feldolgozása úgy van szervezve, hogy
  - az előzetes megegyezés szerinti adatkészletet úgy biztosítja, hogy
  - az a legjobb szakmai gyakorlat szerint
  - támogassa a személyzet munkáját

működési kiválósági kritériumok

- külső és belső előírásoknak való megfelelés - compliance
  ezt a kritériumot 1 vagy több adott cél / intézkedés / esetleg folyamat akkor szolgálja,
  ha:
  - dokumentált módon megfelel
  - valamely olyan követelménynek, amelyet
    - egy olyan hatóság, szerv, állít,
    - amelynek joga van intézményünkkel szemben követelményt állítani, illetve valamely tevékenységét szabályozni

- kockázatkezelés kiválósága - risk management excellence

erről később lesz szó

működési kiválósági kritériumok

- rend - order - saját kritérium

egy intézmény rendezett módon működik, vagy:
a működés rendje adekvát,

ha

- a működés megfelel a legjobb szakmai gyakorlatnak
- a legfelső vezetés vállalja a zintémény jólétéért a felelősséget

↓

- a rend alkotóelemeiből:
  - *dokumentáltság*
  - változás kezelés
  - üzletmenet folytonosság tervezés / speciális eset: informatikai
  - stb.

ezt a kritériumot 1 vagy több adott cél / intézkedés / esetleg folyamat
akkor szolgálja,

ha:

- hozzájárul valamelyik alkotóelemhez

az erőforrások kiváló kezelése kritériumai - néhol pontosítva, általánosítva

- rendelkezésre állás - availability
  egy erőforrás akkor áll rendelkezésre,
  1 vagy több adott cél / intézkedés / esetleg folyamat számára,

ha:

- mindegyik, az adott célban / intézkedésben / folyamatban illetékes alkalmazott rendelkezésére áll,
  - az előre tervezett
  - és megegyezés szerinti,
  - előre jelezhető mértékben, és
  - dokumentált módon

- bizalmasság - confidentiality
  egy erőforrás kezelése akkor bizalmas,
  1 vagy több adott
  céllal kapcsolatban / intézkedés során / esetleg folyamatban

ha:

- azoknak áll rendelkezésére, akiknek dolga van vele →

az erőforrások kiváló kezelése kritériumai - néhol pontosítva, általánosítva

tehát, kapcsolat van a rendelkezésre állás, és a bizalmasság között!
általában is súlyozhatunk, mi a fontos az adott helyzetben?

- rendelkezésre állás?
- bizalmasság?

pl. hatékonyság szerint

- integritás, sértetlenség - integrity

egy erőforrás kezelése akkor felel meg az integritás követelményének,
1 vagy több adott
céllal kapcsolatban / intézkedés során / esetleg folyamatban
ha:

- azt kezelése, feldolgozása *véletlenül* nem változtatja meg
- szokás megkövetelni:
  - pontosságot
  - teljességet
  - üzleti [jobb: stratégiai] értékeknek, elvárásoknak megfelelő érvényességet

az intézményi működés 3 alappillére:
szervezet, szabályozás és technika

a működési kiválósági, és
az erőforrások kiváló kezelését jellemző 10 kritérium legalább egyike
eléréséhez ***hozzájáruló***

részcélokat - operational objective, hivatalosan: control objective, és
tevékenységeket - operational activity , hivatalosan: control measure
vagy tevékenységsorozatokat - procedure, vagy
control procedure, hivatalos neve nincs

az intézményi működés 3 alappillére valamelyikén, vagy egyszerre többükön
biztos, hogy lehet értelmezni

a stratégiai célok eléréséhez vagy a kiválósági kritériumokon keresztül, vagy
valamely, ezeket szolgáló tevékenységgel járulhat hozzá
az intézmény személyzete

miről is van szó ?? hogy jön ide a pillér ??

az intézményi működés 3 alappillére:
szervezet, szabályozás és technika

annak érdekében, hogy a módszertanom felhasználója

➔ mind a legjobb szakmai gyakorlat receptjeiben, mind saját tapasztalataiban könnyebben *azonosíthassa és rendezhesse,* hogy a működés mely területén van teendő,

➔ mely területén kell valamilyen részcélt kitűzni, ez a teendő / részcél a működés milyen részén fog változtatni,

➔ a működés mely eszközeivel,

"önkényesen" kijelölök dimenziókat az intézményi működéshez, *legyen* három:
szervezet,
szabályozás,
technika

az intézményi működés 3 alappillére:
szervezet, szabályozás és technika

operational activity - működési tevékenység
az ISACA régi control measure-ének,
ún. ellenőrzési intézkedésének az általánosítása

valamilyen környezetben / helyzetben kell végrehajtani

a kiválósági kritériumok részcélok lesznek a stratégiai célok elérésében
- intézkedéseinkkel ezek teljesüléséhez szeretnénk hozzájárulni
- vagy: valami kellemetlenséget elhárítani

igaz az egész vállalati működésre, itt speciális eset: az IT

az intézményi működés 3 alappillére:
szervezet, szabályozás és technika

szervezeti pillér elem, pl.:
az egész szervezeti struktúra, és annak részei

szervezeti intézkedés pl.:
szervezeti egységek, munkaköri leírások, szerepkörök definiálása
úgy, hogy hozzájáruljunk célunk teljesüléséhez

szabályozási pillér elem, pl.:
a szabályzatok, szerep- és munkaköri leírások
de ezek készítése szervezeti intézkedés és szabályozási is egyszerre

szabályozási intézkedés megfogalmazás:
a definíciók szabályzatba foglalása, a szabályzat kiadása
"írok egy szabályzatot"

az intézményi működés 3 alappillére:
szervezet, szabályozás és technika

technikai pillér elem, pl.:

a működési tevékenységek ellátásához szükséges
összes fizikai / infrastruktúrális erőforrás
a használatukat meghatározó / lehetővé tévő technikai feltételekkel együtt

technikai intézkedés pl.: mindezek technikai támogatása

az intézményi működés 3 alappillére:
szervezet, szabályozás és technika

készítsünk példákat:

a vírusvédelemhez hozzárendelhető
- stratégiai célok
- kiválósági kritéiumok
- intézkedések
  - értelmezési tartomány - melyik pillér
  - értékkészlet (hatás helye) - melyik pillér

Hf.: egy Informatikai biztonsági szabályzat részei hova illenek?

Hf.: a kötelességelhatárolás megvalósításának mely pillérek lehetnek *pl.*
- az értelmezési tartománya, ill. értékkészlete?

a kritériumok a stratégiát célzó kiterjesztése:
értelmezési tartomány:
- az intézményi működés legalább egy alappillére, vagy erőforrás

hatókör:
- vagy ugyanez, de eshet az intézményen kívülre is

a "valódi" cél tehát:
a stratégiai célok eléréséhez ***hozzájáruló*** kiváló működés

de itt főleg
informatikáról - informatikai ellenőrről - informatikai biztonságról
lesz szó

(speciális eset:
bank, és a többi, már elismerten is kritikus infrastruktúra
inkább ez a macera, mint a bírság, ugye?)

amit szoktam mondani:
olyan régen foglalkozom
- számítástechnikával és
- távközléssel, hogy ...

node a kőbalta már nem segít, hanem

már megint:

biztonság ☞☜ stratégia

a biztonság és a stratégia kapcsolata

stratégia - kockázat - kritérium - intézkedés
↓
stratégiai fontosság
↓
üzleti folyamat fontosság
↓
támogató folyamat fontosság
↓
IT alkatrészek fontossága

módszerek kellenek az információrendszer biztonsága eléréséhez:
- módszertanok
- szabványok

A cél:
a megfelelés – mihez képest?
támogatása – józan ész.

A szabványoknak való megfelelést is
a mindennapokra kell alkalmazni.

*munka*módszer:

- stratégiai célok – top down egyre mindennapibb célok
- az alacsonyabb szintű célok mindig hozzájárulnak a magasabb szintűek teljesítéséhez

az intézkedések ***is "csak" hozzájárulnak*** a célok teljesítéséhez
biztos módszer nincs

Az informatikai biztonság céljai, és
az ellenőr ellenőrzési szempontjai a stratégián alapulnak,
az egész személyzetnek,
az Informatikának, biztonságinak, ellenőrnek
a cég boldogulását kell szolgálnia:

a vállalkozás / intézmény piaci boldogulása ->

vállalati / intézményi stratégia
stratégiai – üzleti célok, üzleti követelmények ->

informatikai stratégia
az üzleti követelményeket teljesítő informatikai folyamatok

kockázat - stratégia kapcsolat alapja:
az üzleti fontosság adja meg a fenyegetett vagyonelem értékét
kockázat ~ ezzel az értékkel, és a veszély bekövetkezése valószínűségével

ez a valószínűség pedig ~ a dolog statégiai értékével, viszont
fordítottan ~ a védelemre fordított erőfeszítéssel
%

Bevezetés az informatikai ellenőrzésbe - Szenes 53

az üzleti folyamatokat az Informatika
a felső vezetés szerinti rangsoruk
az egész szeméyzet, az IT is, e rangsor szerint kell, hogy támogassa

- folyamatok fontossága ➔
- adatok / rendszerek fontossága

ez határozza meg

- az infrastruktúrális elemek fontosságát

a jogosultságokat az üzleti szerepek kell, hogy meghatározzák

az adatok tulajdonosa a felhasználó ➔ ő engedélyez
(az üzleti szakterület vezető, vagy *delegáltja*)

rangsor - osztályozás, és
adattulajdonos: - ld. banki felügyeleti követelményeket

Bevezetés az informatikai ellenőrzésbe - Szenes 54

TEHÁT:

az Informatika meg kell, hogy feleljen /1

- az informatikai stratégiának
  ↓
  tehát az ÜZLETNEK
  ↓
  a rendszerek súlyozása
  azaz a fontosabb üzleti célt
  szolgáló számítástechnikai rendszer a fontosabb

volt : a kiválósági kritériumok teljesítésének súlyozása
hiszen minden egyszerre, egyformán jól nem teljesíthető,
itt is az üzleti megfelelés a lényeg

az ÜZLET érdekében meg kell felelni:
- a törvényeknek,
- ágazati, hatósági szabályozásoknak

A KÖVETELMÉNYEK TELJESÍTÉSÉNEK MÓDJA PEDIG AZ, HOGY:

az Informatika meg kell, hogy feleljen / 2

- az informatikai biztonsági követelményeknek:
  - a rendszerek rendelkezésre állása
  - az adatok bizalmassága
  - az adatok sértetlensége
  - + a többi COBIT kritérium
  - !! funkcionalitás és dokumentáció

(ez a szűkített követelmény verzió
- bővebb: a 10 kiválósági kritérium)

no, és hogy lehet elszúrni?
sokféleképpen
pl. nincs, vagy rossz rendszerfejlesztési módszertan

milyen a jó rendszerfejlesztés?

megkérdezem a Google-t:
"advanced programming principles"
about 121,000,000 results (0.37 seconds)

megkérdezem a Google-t:
"apply effective problem solving techniques"
511,000,000 találat, és:

Here are seven-steps for an effective problem-solving process.
Identify the **issues**. Be clear about what the **problem** is. ...
Understand everyone's interests. ...
List the possible solutions (options) ...
Evaluate the options. ...
Select an option or options. ...
Document the agreement(s). ...
Agree on contingencies, monitoring, and evaluation.

milyen a jó rendszerfejlesztés? - SZERINTEM

FELMÉRÉS

RENDSZERTERV

TESZTELÉSI TERV

PROGRAMDOKUMENTÁCIÓ

ÜZEMELTETÉSI KÉZIKÖNYV

FELHASZNÁLÓI KÉZIKÖNYV

Teendők:
control measure / procedure
ellenőrzési célokhoz ellenőrzési intézkedések / eljárások

pontatlan: "kontroll" =
control measure / procedure
"ellenőrzési" intézkedés / eljárás

példa belső ellenőrzési intézkedésre:
- informatikai (szervezési, SW, HW, ...!!!) eljárások
- szabályzatok,
- munkaköri leírások készítése - ez a
- **KÖTELESSÉGELHATÁROLÁS** - segregation / separation of duties elveinek figyelembe vételével
- adat / program elérési előírások - jogosultságkezelésfi
- **dokumentáció!**

Hf.: mi, melyik pillér(ek)hez tartozik?
további példák?

Bevezetés az informatikai ellenőrzésbe - Szenes 59

(ellenőrzési) intézkedés / eljárás fajták

a probléma szempontjából:

preventive	–	megakadályozó
detective	–	vizsgálati
corrective	–	javító

melyik fajtát válasszuk?

mi legyen a választás alapja:
a szükséges
(becsült – minek alapján?)
ember, pénz, stb. ráfordítás

és ki választ :
a legfelső vezetés ← mert mindenről ők tehetnek
ők a felelősek a tulajdonosok, ügyfelek, mindenki előtt

Bevezetés az informatikai ellenőrzésbe - Szenes 60

(ellenőrzési) intézkedés / eljárás fajták

az, hogy melyik intézkedés melyik fajta
az értelmezéstől - "kiszereléstől" - nagyon függ!!

preventive - megakadályozó ellenőrzési intézkedés pl.:
- eszközökhöz fizikai hozzáférés - ennek mije legyen itt?
- **dokumentáció!**
- **REND!!**

detective - vizsgálati ellenőrzési intézkedés pl.:
- már megtörtént hiba,
- mulasztás
- rosszindulatú cselekedet

UTÓLAGOS észrevételére alkalmas
eszköz pl.:

Hf. :hozzáférési napló (access log) - ez vajjon mindig vizsgálati?

(ellenőrzési) intézkedés / eljárás fajták

detective versus preventive:

hozzáférési napló
szabályzat
jogosultságkezelés
vírusvédelem nos, mi, melyik?

corrective - javító ellenőrzési intézkedéegy hiba miatti baj bekövetkezéséből eredő káros hatások következményének felszámolása, pl.:
- szabályozott restart / recovery - a megszakadt szolgáltatás folytatása
- még a dokumentáció is lehet eső után köpönyeg - példa?
- szervezet - szabályozás - technika - van példa!

detective versus preventive versus corrective

példa vállalati szemléletre
avagy: min alapul a kockázatbecslés
avagy: éljenek a rendszerszervezők!

Vállalat információrendszerének felmérése IBM BSP módszerrel

régen:
IBM BSP versus SSADM:
alap: a folyamat ill. az adat

ma is, évente hitvita, csak más nevekkel:
mi az, hogy információ(s)rendszer?

Információrendszer adatközpontú definíciója
egy régi, az SSADM:

Egy szervezet valamely alaptevékenysége művelésében szükséges infok egy adott körét
előállító és rendelkezésre bocsátó rendszer

Vállalat információrendszerének felmérése IBM BSP módszerrel

IBM BSP értelmezések:

Folyamat:
A vállalat céljaiból levezethető, szükséges, elhatárolható tevékenységek sorozata.

Stratégiai cél:
A vállalat hosszútávú elképzelései
a vállalat jövőbeni belső és külső körülmények által meghatározott állapotáról.

Vállalat információrendszerének felmérése IBM BSP módszerrel

IBM BSP értelmezések:

Döntéselőkészítés, információszolgáltatás:
Adott funkció ellátására adatok, hírek összeállítása.

Stratégiai tervezés:
A vállalat hosszútávú célkitűzéseinek meghatározása, a célok eléréséhez
szükséges és lehetséges műszaki - gazdasági fejlődési tendenciák felvázolása.

Vállalat információrendszerének felmérése IBM BSP módszerrel

A BSP alapelvei

Felülről lefelé haladó tervezés:
- a vállalati célkitűzések lefordítása információ igényekre
- átvilágítás a vállalat felső vezetése szempontjából
- fokozatosan az átfogótól a részletes felé;

Alulról-felfelé történő megvalósítás - indulás:
- alapadatok felmérése
- alapnyilvántartások kidolgozása

↓

integrált irányítási rendszerek megvalósítása

Vállalat információrendszerének felmérése
IBM BSP módszerrel

A CHEMIMAS esete:

A munka folyamatos irányítását
a vállalat felső vezetőiből alakult team végezte.

A BSP mellett mi, a külsők döntöttünk,
a vezérigazgató egyetértésével.

A BSP lépései:

1. A vállalati célok meghatározása
2. A vállalati folyamatok meghatározása
3. Az adatosztályok meghatározása
4. Az információrendszer szerkezetének meghatározása

Vállalat információrendszerének felmérése
IBM BSP módszerrel

1. A vállalati célok meghatározása

Célja, hogy a felső vezetés egyetértésre jusson abban,
hogy merre halad a vállalat,
ezt kell az információrendszernek támogatnia.

Partnerünk: az Igazgatótanács

ülések, cédulák, tábla

Vállalat információrendszerének felmérése
IBM BSP módszerrel

2. A vállalati folyamatok meghatározása

Ez adja a vállalati információrendszer
nyújtotta támogatás hosszútávú alapját.
(A folyamatok állandóságára alapoz.)

Partnerünk:
Igazgatótanáccsal a főfolyamatokat
és azok nagybani tartalmát, majd a folyamatok rangsorát, aztán u.ezt tisztázzuk alsóbb szinteken is.

Vállalat információrendszerének felmérése
IBM BSP módszerrel

3. Az adatosztályok meghatározása

Meghatározzuk
az egy, vagy több folyamatot támogató átfogó adatokat.

Partnerünk:
Külön interjúk a megfelelő igazgatótanácsi tagokkal, majd lefelé az egyes ágazatokban.

4. Most már készülhetnek mátrixok !

folyamat - szervezet - adatok, stb.

ugyanolyan, mint a kockázatbecslés, amin aztán alapul az IT BCP !

Vállalat információrendszerének felmérése
IBM BSP módszerrel

5. Az információrendszer szerkezetének meghatározása
itt nem információs !

Ez lényegében az információrendszer hosszútávú céljainak megadása, kidolgozása,
Ezt mi csináljuk, a Vevővel egyeztetünk, és ennek alapján felvázoljuk az IR nagyvonalú szerkezetét.
Majd a fontossági sorrendek meghatározása,
fontosabb alrendszerek részletezése,
akcióterv,

végtermék: TANULMÁNY.

az ellenőrzés egy értelmezése:

- az üzleti célok elérésére,
- a nemkívánatos események
- megakadályozására, vagy
- feltárására, és
- a már bekövetkezett hiba kijavítására tervezett

  - irányelvek,
  - eljárások,
  - szabályozás,
  - gyakorlat, és
  - szervezeti struktúrák

  komplex összessége

Az informatikai ellenőrzés hivatalos célja:

biztosítja az információrendszer számítástechnikai támogatásának
- biztonságát – valamelyik definíció szerint, és
- megfelelő minőségét
  mihez képest megfelelő??

Mit ellenőrzünk?
- a termelést
- a működést

biztosító és támogató információrendszert
➔
Ez folyamatokat, adatokat is jelent,
nemcsak technikát!

(cél: IT Governance)

egy kicsi a governance-ról

Az intézmény kormányzása:

annak piaci versenyképességét szolgáló irányítása,
- a környezethez
- lehető legjobban alkalmazkodó
- stratégia alapján,

amelynek
- meghatározása, és
- rendszeres karbantartása

az első számú vezető felelőssége

egy kicsi a governance-ról

az intézmény
(vállalat, közintézmény, akármi)

sikeres informatikai kormányzása:

a sikeres vállalati kormányzás egyik szükséges feltétele

az IT (részleg + tevékenységek + ▪▪▪)
olyan irányítása,
amely
- a vállalati kormányzást
- a felső vezetés szándékai szerint szolgálja

ellenőrzés fajták - az ellenőrzési szempontok csoportosítási lehetőségei:

- működés
- működés támogatása
  - informatikai
  - pénzügyi
- (közvetlen termelés)
- (termelés támogatása, pl. projekt)

az ellenőrzés vizsgálatának szempontjairól:

- miért ellenőrzünk,

mi a cél, milyen előnye van az ellenőrzésből az ellenőrzöttnek, vagy bárki / bármi másnak

- mit ellenőrzünk,

mit kell vizsgálni, mit nézünk meg az ellenőrzés során

- hogyan ellenőrzünk,

milyen vizsgálati módszereket lehet alkalmazni

az ellenőrzés felülvizsgálata, auditálása
tanusítja:

- az ellenőrzés megfelel a legjobb szakmai gyakorlatnak
- a menedzsment irányelvei **dokumentáltan** érvényesülnek

  - az információt nyújtók
  - az információt fogadók
  - az információáramlást számítástechnikával támogatók

  kapcsolatrendszerében.

fontosabb informatikai biztonsági követelményeinket felsoroltuk már:
rendelkezésre állás - ha ez nincs, nincs miről beszélni
bizalmasság
integritás (sértetetlenség)

Zavartalan" **rendelkezésre állás:**
milyen hibák,
milyen okokból következnek be,

mi e hibák üzleti kockázata,

hogyan, és
mennyi ráfordítással lehet ezeket kivédeni

és egyáltalán:
súlyozni a különféle kiválósági kritériumok között ./.

a legfelső vezetésnek ***felelőssége és joga*** dönteni

- *megéri-e* a ráfordítás, vagy
  inkább érdemes-e kockáztatni, hogy
  esetleg bekövetkezzenek a hibák,

és felkészülni
  a következményeik elhárítására

a kockázatot arányosként definiáltuk:
  veszély bekövetkezésének valószínűsége *
  fenyegetett vagyonelem értéke

- mi legyen?

„vállalja-e a kockázatot"
szleng
– pontosan:

  a kockázat mértéke
  - megéri-e a veszély
  - elhárításának költségét?

ha nem: jön a kockázat elfogadó nyilatkozat

példák

az ellenőrzési munka lehet kis falat / nagy falat

jelenthet átfogó vizsgálatot is.
pl.
működés ellenőrzési „nagy falatok":

A vállalati stratégia elkészítésének
  folyamata **dokumentáltan**
  megfelel-e a tulajdonosok érdekeinek?

A vállalati stratégiából (a fő stratégiai célokból)
  vezették-e le az informatikai stratégiát, és
  dokumentáltan tették-e ezt?

adatvédelmi törvények, előírások betartása, pl.
- adatok sorsának követése

pláne most, GDPR és PSD2 idején (ld. Európai Únió)

példák

működés támogatási nagy falatok

- egy stratégiai jelentőségű alkalmazói rendszer auditja
  mint projekt – a fejlesztésének menete
  mint eredmény – a rsz. biztonsági jellemzői
- egy stratégiai jelentőségű folyamat auditja, pl.
  - üzemeltetés
  - fejlesztés
    – a fejlesztésről lesz még szó!
- pénzügy, pl.:
  - mérlegkészítés átvilágítása
  - jelentésszolgálat megfelelése
  - értékcsökkentés könyvelés

példák

mik is tartoznak a működés *támogatáshoz*?

informatika
pénzügy
- tevékenységek elszámolása
- eredmények kiszámítása valamilyen módon
- tevékenységek finanszírozása vagy
  már meglévők hatékonysága
- stb.

emberi erőforrás
jog
...
és persze a vezetés

a működés pedig: amiből élünk

példa működés támogatási kis falatra:

- audit a közvetlen termelésben:

MEO, törvények,munkavédelem
(néhai ISO 9000 család)

- közvetlen termelés támogatási audit - kis falat, és nagy is lehet:

pl. projektirányítás

számítástechnikai kis falat:

- mentések ellenőrzése egy számítóközpontban:

az üzemeltetési ügyrendhez illeszkedik-e – ha van!

- kinek a felelőssége
- milyen időközönként történik
- nyilvántartás
- tárolás, hozzáférés,
- stb.

auditálási kockázatok

ún. jelentős (substantive) hiba, amely:
a vizsgált célterület bármely komponense vizsgálatának helyességét *jelentősen* veszélyezteti
(vs. substantive audit)

auditálási kockázat:
(informatikai / pénzügyi jelentés jelentős hibát tartalmaz)
a vizsgálatban hiba történt, de az auditor nem veszi észre

ún. öröklött kockázat:
a tévedés

- a célterület természete miatt
- a feltárandó összefüggések bonyolultsága miatt
  pl. egy bonyolult számítás

auditálási kockázatok

ún. ellenőrzési kockázat:
- a belső ellenőrzési rendszer nem alkalmas
  valamely *jelentős* hiba *időben* történő feltárására

ún. detektálási kockázat:
- nem megfelelő tesztelési eljárások miatt
  az auditor egy jelentős hibát nem vesz észre

az auditálás teljes kockázata:
kombináció
- szakterületre,
- ellenőrzési célpontokra
- hibalehetőségekre

az audit fázisai
az ISACA CRM , COBIT®, ISO, ... és főleg a józan ész alapján

ez csak egy verzió a sok lehetséges közül ***!***

1 az audit scope meghatározása, együttműködve
- a megrendelővel / az auditált terület menedzsmentjével

ide tartozik
az adott tevékenységet szolgáló informatikai folyamatok és
intézményi ellenőrzési mechanizmusok azonosítása

az audit fázisai
az ISACA CRM , COBIT®, ISO, ... és főleg a józan ész alapján

2 az intézmény megismerése, és
a feladat pozícionálása az intézményben:

- az intézmény helyzetének felmérése,
- a siker szempontjából kritikus tevékenységeknek, és
- annak a mértéknek a meghatározása, hogy
  e tevékenységek mennyire járulnak hozzá
  az intézmény stratégiai céljai eléréséhez
- ha résztevékenység az audit hatókör,
  annak viszonya a kritikus tevékenységekhez
- az adott esetben szerepet játszó üzleti célkitűzések
  kijelölése, pl. COBIT®
  vagy bármi más, ami alkalmas

az audit fázisai
az ISACA CRM , COBIT®, ISO, ... és főleg a józan ész alapján

3 a célszervezet körülményei az audit előtt:

- az auditálandó célterület áttekintése,
- pozícionálása az intézményen belül
- előző évi auditálások
- jelenlegi pénzügyi helyzet
- törvények, rendeletek
- esetleg: ismert külső forrású kockázatok összegyűjtése

az audit fázisai
az ISACA CRM , COBIT®, ISO, ... és főleg a józan ész alapján

4 az audit hatóköre pontosításához és
a lefolytatás előkészítéséhez

a következőket kell azonosítani, kiválasztani,
és ***egyeztetni*** a megrendelővel:

- alkalmazandó kiválósági kritériumok
- ezek súlyozása(i)
- control objectives
- auditálási eljárások
- ütemezésük
- szükséges emberi / anyagi / egyéb erőforrások – az auditált részéről
- ...

Bevezetés az informatikai ellenőrzésbe - Szenes 89

az audit fázisai
az ISACA CRM , COBIT®, ISO, ... és főleg a józan ész alapján

5 felkészülés az auditra - helyzetfeltárás
a terep és az összefüggések megismerésére:
- o BPR – Business Process Reengineering
- o ISACA ajánlások
- o rendszerszervezés + ...
- o COBIT
- o bármi más

folyamat < - > üzleti követelmény
folyamat < - > megvalósítási feltételek
folyamat < - > ellenőrzési célok

A megvalósítási feltételeknek és az ellenőrzési céloknak való megfelelés ellenőrzése érdekében ezekből, és
az adott folyamattal kapcsolatos további kérdésekből
ellenőrzési listákat , mátrixokat lehet készíteni

Bevezetés az informatikai ellenőrzésbe - Szenes 90

az audit fázisai
az ISACA CRM , COBIT®, ISO, ... és főleg a józan ész alapján

6 az audit módszereinek meghatározása
tulajdonképpen a receptek kiválasztása
az adott helyzet szerint

felhasználjuk:
- a legjobb szakmai gyakorlatnak megfelelő módszertanokat
- saját tapasztalatot + józan észt

szaktudomány - best practice ↗

azaz: 27001 Appendix A? vagy?
COBIT üzleti követelmények, mérések, stb.?

az audit fázisai
az ISACA CRM , COBIT®, ISO, ... és főleg a józan ész alapján

7 kockázat becslés fázis

7.1 a vizsgálandó terület kockázatai

7.2 a belső ellenőrzési helyzet – ha kell
- az ellenőrzési környezet, és
- az ellenőrzési eljárások
- detektálási kockázatok becslése
- ellenőrzési kockázatok becslése
- teljes kockázat becslése

az audit fázisai
az ISACA CRM , COBIT®, ISO, ... és főleg a józan ész alapján

8 az audit lefolytatása

- jelenlegi ellenőrzés vizsgálata és tesztelése – ha kell
- irányelvek, szabályzatok vizsgálata, és
- betartásuk*, azaz eljárások, stb. vizsgálata
- (munkaköri) kötelességelhatárolások
  ehhez tartozó jogosultság, stb. vizsgálatok
- konkrét bizonyítékok gyűjtése,
  naplózás vizsgálata, stb.
- esetleg analítikus eljárásokkal egyenlegek, és / vagy
- más, lényegi összefüggések lényegi tesztelése
- stb.

* "nosza, írjunk egy szabályzatot!"

az audit fázisai
az ISACA CRM , COBIT®, ISO, ... és főleg a józan ész alapján

9 befejezési munkálatok

- dokumentációk, pl.
  következtetések, ajánlások, javaslatok
- auditori jelentés
  - ISACA Code of Ethics
  - best practice

! follow-up review
azaz: GOTO STEP 1

néhány USA-ban indult minősítő szervezet és minősítés

Information Systems Audit and Control Association
ISACA - www.isaca.org

alapítás: 1969. EDP Auditors Association

Certified Information Systems Auditor – CISA
Certified Information Security Manager - CISM
Certified in Governance Enterprise IT - CGEIT

Information Systems Audit and Control Foundation – ISACF
az IS audit és ellenőrzés K+F támogatására

Information Systems Security Certification Consortium
(ISC)2 - www.isc2.org

CISSP - Certified Information Security Professional

hasznos források

<u>ISACA könyvek</u>

ebből készülnek mind az 5 földrészen a CISA vizsgára:
CISA Review Technical Information Manual
ed.: Information Systems Audit and
Control Association
Rolling Meadows, Illinois, USA
(1 kivétellel évenként kiadják - 1998. óta vagyok Expert Reviewer)

COBIT könyvek ./.

és a Bookstore

<u>ISACA folyóirat:</u>

IS Control Journal, majd Control Journal, most ISACA Journal

rengeteg segítség:

COBIT®
Control OBjectives for Information Technology

egy fejlődési folyamat, néha rossz döntésekkel
de alapjában óriási:

a kezdet:
COBIT - 1998

CMM és Balanced ScoreCard:
COBIT 2000 – COBIT 3rd edition

COBIT 4.0 - 2005
Control Objectives, Management Guidelines, Maturity Models
2005, IT Governance Institute®

rengeteg segítség:

COBIT 4.1 - 2007
IT Governance Institute®; editor: ISACA

a COBIT 5 indulása:
COBIT ® 5 Design Paper Exposure Draft © 2010 ISACA, working paper

2011-ben meghívnak az Expert Reviewer csoportba,
és ettől kezdve a COBIT könyvek elején is ott van a nevemmel:
University Obuda

itt a COBIT 5 és 2019 könyvekhez látható
- szakdolgozathoz
- diplomamunkához
- cikkhez

egy célszerű hivatkozás gyűjtési módszer . / .

rengeteg segítség:

[COBIT 5, 2012, Proc.] Enabling Processes COBIT 5® An ISACA Framework
Copyright © 2012 ISACA
ISBN 978-1-60420-239-7

[COBIT 5, 2012, Gov.] COBIT 5 A Business Framework for the Governance and Management of Enterprise IT
Copyright © 2013 ISACA
ISBN 978-1-60420- **xxxxxxxxxxxx** ezt még pótolom

[COBIT 5, 2013] COBIT® 5: Enabling Information COBIT 5® An ISACA® Framework
Copyright © 2013 ISACA
ISBN 978-1-60420-350-9

rengeteg segítség:

[COBIT 2019, 2018, Gov]

COBIT 2019 Framework: Governance and Management Objectives
ISBN 978-1-60420-728-6
Copyright © 2018 ISACA

[COBIT 2019, 2018, Gov] COBIT® 2019 Framework: Introduction and Methodology
ISBN 978-1-60420-644-9
Copyright © 2018 ISACA

nemzetközi és hazai szabványok

ISO/IEC =
International Organization for Standardization /
International Electrotechnical Commission

sokáig volt:
ISO/IEC 17799
International Standard ISO/IEC 17799
First edition 2000-12-01
Information technology —
Code of practice for information security management
Reference number: ISO/IEC 17799:2000(E)

elődei:
CRAMM – CCTA Risk Analysis and Management Methodolology
BS 7799, majd 17799

nemzetközi és hazai szabványok

a 27000-es családból az elsők:

ISO/IEC 27001
International Standard ISO/IEC 27001
First edition 2005-10-15
Information technology - Security techniques - Information security management systems - Requirements
Reference number: ISO/IEC 27001:2005 (E) © ISO/IEC 2005
ez a 27000-es család első eleme, az 17799 ismételve,
most: 2013

az 17799 másik darabja: 27002
International Standard ISO/IEC 27002 First edition 2005-06-15
Information technology — Security techniques — Code of practice for information security management
Reference number: ISO/IEC 27002:2005(E) Copyright © ISO/IEC 2005
most: 2013

nemzetközi és hazai szabványok

a 27001, 27002 útmutatása:

hogyan kell az informatikai biztonság
alapkövetelményeit,
a rendelkezésre állást,
a bizalmasságot, és az
integritást teljesíteni.

Az informatikai szakterületet részterületekre bontja, és az egyes részekhez leírja, milyen *veszélyek* fenyegetik, és *ellenőrzési célokat* javasol a követelmények teljesítéséhez.

27005 - risk,
27018 - cloud,
27034 - application security
stb.

nemzetközi és hazai szabványok

ISO/IEC 15408
Information technology — Security techniques
— Evaluation criteria for IT security
(Common Criteria)
(ITCSEC, majd ITSEC, majd CC)

Magyar Szabvány MSZ ISO/IEC 12207:2000
Magyar Szabványügyi Testület
Informatika. Szoftveréletciklus-folyamatok
Information technology. Software life cycle processes
megfelel: az ISO/IEC 12207:1995 verziónak
de már van a 27034!

International Standard First edition 2008-06-01
Corporate governance of information technology
Gouvernance des technologies de l'information par l'entreprise
Reference number: ISO/IEC 38500:2008(E) Copyright © ISO/IEC 2008

további támogató szabványok, módszertanok, irodalom

Szenes Katalin - fejezetek Az Informatikai biztonság kézikönyvéből
Verlag Dashöfer, Budapest

- Informatikai biztonsági megfontolások a Sarbanes - Oxley törvény ürügyén

(A 2002-es Sarbanes - Oxley törvény hatásai az informatikai biztonsági rendszerekre és az informatikai ellenőrök feladataira. A jelentésszolgálat és a többi kulcsfontosságú alkalmazás felügyeletének kérdései)
22. aktualizálás, 2006. október

- A szolgáltatás - orientált architektúrák biztonsági kérdései
23. aktualizálás, 2006. december

- A COBIT 4.0 és 4.1 újdonságai
27. aktualizálás, 2007. november

- A számítógéphálózatok biztonságának felülvizsgálata
28. aktualizálás, 2008. február

stb.

Bevezetés az informatikai ellenőrzésbe – Szenes

105

további támogató szabványok, módszertanok, irodalom

- **NIST** - National Institute of Standards and Technology nist.org
(US Dept. Commerce)
pl. http://web.nvd.nist.gov/view/vuln

- ISC2., pl. https://vulnerability.ISC2.org

- CERT Hungary, pl.
http://www.cert-hungary.hu/sites/default/files/press
http://tech.cert-hungary.hu/vulnerabilities

- Wifi Alliance

- PCI DSS - Payment Card Industry Security Standards
https://www.pcisecuritystandards.org/security_standards/

- OWASP - Open Web Application Security Project

- OASIS-OPEN - advancing open standards for the information society
https://www.oasis-open.org/

ős: SGML (Standard Generalized Markup Language) Open, 1993.

- stb., stb.

Bevezetés az informatikai ellenőrzésbe – Szenes

106

néhány magyar szakmai szervezet

- az European Organization for Quality - EOQ
  Magyar Nemzeti Bizottság Informatikai Szakbizottsága

www.eoq.hu

- a Hírközlési és Informatikai Tudományos Egyesület Számítástechnikai Szakosztálya

www.hte.hu

- az (ISC)2 Hungary Chapter

www.isc2.org

- az ISACA Magyar Fejezete

https://isaca.hu/