IT biztonság és IT audit
best practice szemelvények:

a kiszervezés
- remélt előnyei
- nem várt hátrányai

Dr. Szenes Katalin, CISA, CISM, CGEIT, CISSP
Óbudai Egyetem, Neumann János Informatikai Kar
szenes.katalin@nik.uni-obuda.hu

tartalomjegyzék

tartalomjegyzék

- a COBIT 4 (4.0, 4.1) részei
- a COBIT 4 13 folyamata a kiszállításhoz és támogatáshoz

- DS1 - a szolgáltatási szintek meghatározása és kezelése
  [javasolt] részletes ellenőrzési célok
- DS1.1 A szolgáltatási szintek kezelése kereteinek kialakítása
  részlet Az Informatikai biztonság kézikönyvéből - Verlag Dashöfer
- DS2 - külső szolgáltatások kezelése
  [javasolt] részletes ellenőrzési célok

- best practice a tervezésben, és üzem közben - további COBIT 4, 4.1 példák

- javaslatok a szállítói kockázatok kezeléséhez
  "Az informatikai erőforrás-kihelyezés auditálási szempontjai" fejezet alapján
  Az Informatikai biztonság kézikönyve - Verlag Dashöfer

tartalomjegyzék

- COBIT® / CMM - érettségi szintek
  - az 1. szint fő jellemzői
  - a 3. szint fő jellemzői
  - tanácsok a DS2 - külső szolgáltatások kezelése
    3-as érettségi szintjéhez
    részlet "Az informatikai erőforrás-kihelyezés auditálási szempontjai"
    fejezetemből - Az Informatikai biztonság kézikönyve - Verlag Dashöfer

- IT szolgáltatás management - IT Service Mangement - ITSM
  ahogy az ISACA CISA Review Course-on tanítjuk
  - szolgáltatási jelentések

tartalomjegyzék

- a COBIT 5 messziről, csukott szemmel:
  - a COBIT domain-ek version 4.1-ig, és a COBIT 5 process-ei
  - egy kedvenc ábra az ISACA COBIT Focus-ából
  - best practice - COBIT 5 példák
- outsource best practice szemelvények - az ISO 27001-ből
- Infrastruktúrális elem definíciója
  ugyanazon kézikönyv ugyanazon fejezete
- irodalomjegyzék

egy lehetséges best practice lista - választott források

www.isaca.org
az USA-ban alapított ISACA
- Information Systems Audit and Control Association

- COBIT4, COBIT 5
- kézikönyvek a dezignációkhoz:
  - CISA – Certified Information Systems Auditor,
  - CISM - Certified Information Security Manager,
  - CGEIT - Certified in Governance Enterprise IT

www.isc2.org
ISC2: a szintén amerikai
- International Information Systems Security Certification Consortium

- Infosecurity Professional magazin
- kézikönyv: CISSP - Certified Information Security Professional

ISO szabványok

- ISO 27000 család, governance - 38500, egyéb risk: 73 Guide, **... ...**

miért érdemes a kiszervezéssel illusztrálni
az informatikai biztonsági / audit legjobb gyakorlatot?

kiszervezés:

- tervezés
  - erőforráskihelyezés, szolgáltatás kívülről, stb.
- mire, és hogyan kell felkészülni

egyéb + kiszervezés:

- a felújított és kiterjesztett kritériumok
- pilléreink,
  a szervezet, a szabályozás és a technika - a kiszervezés tükrében

- hasznos dolgok a best practice-ból:
  - COBIT 4 és 5
  - ISO, és
  - egyéb. pl. PCI DSS, NIST, stb.

követelmény, pl.
Requirements and Security Assessment Procedures
Version 3.0 November 2013

- "PCI DSS requirements apply to organizations and environments where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted.

- Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their CDE.

- Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party per the applicable PCI DSS requirements."

CDE: cardholder data environment

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

mit kell *okvetlenül* tudni?
- az örökzöld jelmondatom

ha akarom - vemhes
ha nem akarom - akkor is vemhes

akármit is helyezünk ki:
- feladatot
- az emberi / tárgyi erőforrásokat
- stb.

a felelősség bent marad

és kié?

mit kell még *okvetlenül* tudni?

- „Ahhoz, hogy sikeres legyen az outsourcing, gondosan figyelnünk kell arra, hogy miért, mit, és hová helyezünk ki."
  (Wendell Jones, Digital Equipment Corporation, 1997.)

erőforráskihelyezés alapja:
- a kiszervezés egy **működés-támogató** folyamat
  ➔
- az intézmény ***üzleti céljaiból*** eredő szükségleteken kell, hogy alapuljon

- a szükségletek jellemzése:
  - a szerződésben szereplő szolgáltatások
  - azok elvárt szintje
    ➔
  - a munkatársak szerepe, felelőssége - Vevő / Szállító

a szolgáltatás biztosítás és támogatás audit feladatai-

a szolgáltatási szint kezelés módszereinek vizsgálata:

- a belső és a külső szolgáltatók szolgáltatási szintje
  - meg van határozva
  - felügyelt

az üzemeltetés vizsgálata:

- az üzleti szükségleteket kielégíti-e az informatikai támogatás?

- az adatadminisztráció módszereinek vizsgálata
  - az adatbázisok integritása
  - optimalizáltsága

a szolgáltatás biztosítás és támogatás audit feladatai-

a kapacitás- és teljesítménymonitorozási eszközök és módszerek használatának vizsgálata

- a szervezet céljait az informatikai szolgáltatások figyelembe veszik-e?

a dokumentáció mellett legfontosabb szempontok:
- változáskezelés
- konfigurációkezelés
- kiadáskezelés

gyakorlatának vizsgálata,
biztosítják-e, hogy az intézmény termelési környezetének változásait ***megfelelően***
- felügyelik-e
- dokumentálják-e?

intézmény - hiszen bármilyen szervezet lehet az audit tárgya

a szolgáltatás biztosítás és támogatás audit feladatai-

a probléma ➔ ? ← incidens, és
hibakezelés gyakorlatának vizsgálata

- dokumentálják
- kivizsgálják
- megoldják
- elvárható ? időre
- visszajelzés is legyen közben

úgy alakították-e ki az informatikai infrastruktúrát,
hogy "megfelelően" támogassa a szervezet céljait?

- eszközök
- alkalmazások
- ...

remélt előnyök

- költségcsökkentés
  avagy ? ● létszámcsökkentés - tőzsdei mutató javítása
- inkább valós - életszerűbb - kérdés:
  mikorra fog mindez megtérülni

megtérülési feltételek -
és itt jöhet az auditori / informatikai biztonsági bölcsesség:

- a költségek ellenőrizhetővé tétele ≠ költségcsökkentés!
  esély:
- ha a tevékenységekhez
  - pontosan meghatározzák
  - hozzá is rendelik
- a szükséges ember / anyagi erőforrásokat
  - minden infrastruktúrális elem + egyéb költség

vannak tényleges előnyök

végre !

- kötelezővé válik
  - a feladatok, elvárások pontos megfogalmazása
  - a szolgáltatások minőségi paramétereinek meghatározása
- ➔ definiálni kell valamiféle mérhető jellemzőket
- projekt alakuló ülés
- rendszerszervező moderálásával:
  - cédula,
  - táblázat,
  - mátrix

a vagyon, és az információrendszer - vigyázzunk rá!

- **a társasági vagyon:**
- stratégiai, védelmi és biztonsági szempontból:
  - az információrendszer
  - az értékrendszer
- **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

definíció forrása: részben ISACA, és IBM BSP Business System Planning

a teljesítendő követelményrendszer - vegyük figyelembe!

- mit kell betartani?
  - üzleti célok, a nemzetközi "legjobb" gyakorlat alapján is!
  - törvények, iparági - főhatósági szabályozások
- a vállalati vagyon védelmének szempontjai
  - körülményekből eredő veszély
  - emberi eredetű veszély - ez a nehezebb
- és mik az alappillérek?
  - szervezet
  - szabályozás
  - technika

az ellenőrzési szempontok alapja

ellenőrzés alapja: a stratégia

- az Informatikának 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 bekövetkezés vsz.séggel
  - ez pedig a védelemre fordított erőfeszítéssel is

a COBIT 4 (4.0, 4.1) részei

- 34 informatikai folyamat
- 7 informatikai értékelési kritérium
- ellenőrzési célok
- ellenőrzési intézkedések / eljárások
- kiegyensúlyozott mutatószámrendszer
- az egyes informatikai folyamatokhoz illesztett képesség érettségi modell

ilyen állat, hogy "kontroll" nem létezik!
csak - esetleg - kontroll cél, vagy intézkedés / eljárás

a COBIT 4 13 folyamata a kiszállításhoz és támogatáshoz

- DS1 - a szolgáltatási szintek meghatározása és kezelése
- DS2 - külső szolgáltatások kezelése
- DS3 - a [megfelelő] teljesítmény és kapacitások biztosítása
- DS4 - a szolgáltatás folytonosságának biztosítása
- DS5 - a[z informatikai?] rendszer biztonságának biztosítása
- DS6 - a költségek azonosítása és szétosztása
- DS7 - a felhasználók képzése és betanítása
- DS8 - a helpdesk és az incidensek kezelése
- DS9 - a konfiguráció kezelése
- DS10 - problémakezelés
- DS11 - adatkezelés
- DS12 - a fizikai környezet felügyelete (kezelése)
- DS13 - az üzemeltetés? felügyelete (kezelése)

DS1 - a szolgáltatási szintek meghatározása és kezelése
[javasolt] részletes ellenőrzési célok

- DS1.1 A szolgáltatási szintek kezelése kereteinek kialakítása
- DS1.2 Az egyes szolgáltatások definiálása
- DS1.3 A szolgáltatási szintekre vonatkozó megállapodások
- DS1.4 A működési szintekre vonatkozó megállapodások
  - a szolgáltatási szintekre vonatkozó teljesítmény kritériumok megadása
  - a kockázatviselők számára érthető jelentések
  - monitorozó statisztikák és ezek vizsgálata ➔ teendők
- DS1.5 A szolgáltatási megállapodások teljesítésének felügyeletéről, és a helyzetjelentésekről szóló rendelkezések
- DS1.6 A szolgáltatási szerződések, és klauzuláik felülvizsgálata

DS1.1 A szolgáltatási szintek kezelése kereteinek kialakítása
részlet "Az informatikai erőforrás-kihelyezés auditálási szempontjai"
fejezetemből - Az Informatikai biztonság kézikönyve - Verlag Dashöfer

a szolgáltatás Vevőjének és Szállítójának, együtt, olyan, pontosan és részletesen definiált kereteket kell kialakítaniok, amely egyértelműen meghatározza,

- **kinek, mikor, mi a feladata,**
- **ennek végrehajtásáért ki a felelős,**
- **mi az a - pontosan megadható tulajdonságokkal jellemezhető - termék, amiről egyértelműen megállapítható kell legyen, hogy megfelel-e az előzetes specifikációknak,**
- **és ki, mikor, hogyan fogja ellenőrizni, hogy ezek az elvárások milyen mértékben teljesültek;**
- **az ennek a teljesülési mértéknek az alapján megítélt teljesítés minőségi paraméterei visszacsatolásának a módját, és**
- **ezeknek a paramétereknek a felhasználását a:**
  - **jelen teljesítés díjazásában**
  - **a jövőbeli együttműködés javításában, és**
  - **esetleges kiterjesztésében**

DS2 - külső szolgáltatások kezelése
[javasolt] részletes ellenőrzési célok

- DS2.1 Az összes szállítóval való kapcsolat azonosítása
- DS2.2 A szállítókkal való kapcsolat kezelése
- DS2.3 A szállítókkal kapcsolatos kockázatok kezelése
- DS2.4 A szállító teljesítményének monitorozása

best practice a tervezésben, és üzem közben - további COBIT 4, 4.1 példák

a teljesség mindenféle igénye nélkül:

- PO9 Az informatikai kockázatok becslése és kezelése
- AI3 A technológiai infrastruktúra beszerzése és karbantartása
- PO10 Projektirányítás
- AI3 A technológiai infrastruktúra beszerzése és karbantartása
- AI5 IT erőforrások vásárlása
- DS4 A folyamatos szolgáltatás biztosítása
- DS5 A rendszerbiztonság biztosítása
- ME1 Az IT teljesítményének monitorozása és értékelése
- ME2 A belső ellenőrzés megfelelésének vizsgálata és értékelése
- AI6 Változáskezelés
- DS9 Konfigurációkezelés

javaslatok a szállítói kockázatok kezeléséhez
"Az informatikai erőforrás-kihelyezés auditálási szempontjai" fejezet alapján

javasolt kiegészítések a COBIT módszertanhoz:

- a szerződés teljesítése közben a külső fél tudomására jutott információ diszkrét, bizalmas kezelése
  (non-disclosure)
- ha rendszert, fejlesztési eredményt veszünk valahonnan, akkor, a szállítónak való kiszolgáltatottság csökkentése érdekében azoknak az információknak a letétbe helyezése, amelyeket közvetlenül egy szállító általában nem szívesen adna át, de amelyekre, az ő esetleges megszűnése esetén, szükség lehet - ilyen például a forráskód
  (escrow agreement)
- a szállítók életképessége:
  - a piacon való megmaradás valószínűsége
  - legalább a szerződéses kapcsolat tartama alatt, lehetőleg tovább is

javaslatok a szállítói kockázatok kezeléséhez
"Az informatikai erőforrás-kihelyezés auditálási szempontjai" fejezet alapján

további javaslatok:

- felkészülés esetlegesen helyettesítő Szállító bevonásának lehetőségére a
  - kapcsolatot előkészítés esetleg
- a Szállító a Vevőnél teljesítendő biztonsági követelményeknek való megfelelése
  - úgyis a Vevő a felelős
- szankciók arra az esetre, ha a Szerződő Felek valamelyike a Szerződés valamely előírását nem teljesítené, és
- a jó teljesítésért esetleg járó bónusz.

COBIT 4 ® / CMM - érettségi szintek

COBIT 4 ® / CMM
SEI: Carnegie Mellon Software Engineering Institute

0 semmiféle érettséget nem mutató
1 kezdeti, ad-hoc
2 ismételhető, de intuitív
3 definiált folyamat
4 irányított és mérhető
5 optimalizált

COBIT 4 ® / CMM - az 1. szint fő jellemzői

1. szint - kezdeti / ad-hoc

- kell foglalkozni az informatikai irányítással
- nincsenek standard folyamatok – ad-hoc
- vezetés - informatikai irányítás - kaotikus
- informatika jelentősége az üzleti folyamatokban (néha)
- nincs szabvány mérésekre
- informatika felügyelet csak, ha történik valami

COBIT 4 ® / CMM - a 3. szint fő jellemzői

3. szint - definiált folyamat

- elfogadták, kell informatikai irányítás – vannak elvek
- kezdeti szintnek megfelelő mérőszámkészlet
- -> de az eltéréseket mindenki egyénileg kezeli...
- kimeneti értékek definiálása és dokumentálása
- szabványosított és dokumentált eljárások
- ezek bekerültek a vezetőség kommunikációjába is
- -> informálisan már oktatják is ezeket
- BSC (Balanced ScoreCard) kialakítása,
- elemeinek felhasználása az értékelésben ●●●

tanácsok a DS2 (külső szolgáltatások kezelése) 3-as érettségi szintjéhez
részlet "Az informatikai erőforrás-kihelyezés auditálási szempontjai"
fejezetemből - Az Informatikai biztonság kézikönyve - Verlag Dashöfer

3-as érettségi szint: definiált

- A külső szolgáltatókkal való tárgyalásra és ellenőrzésükre, sőt, már a szolgáltatások menedzselésére is vannak *jól dokumentált* eljárások. Szabványosították, hogyan kell leírni a szerződéses feltételeket. A szerződések *pontosan lefedik* a megállapodásokat, és részletezik bennük:
  - milyen szolgáltatásokat nyújt a harmadik fél
  - mik a jogi,
  - működési, és
  - ellenőrzési követelmények.
- Ki van jelölve, hogy ki fogja, a Vevő részéről, *felelősen* figyelemmel kísérni a szolgáltatások teljesítését. Megvan(nak) a Vevőnél az(ok) az illetékes munkatárs(ak) is, aki(k)nek felelőssége, illetve feladata a kiszervezésből eredő kockázatok becslése, és az eredmények a megfelelő helyekre való továbbítása.

IT szolgáltatás management - IT Service Mangement - ITSM
ahogy az ISACA CISA Review Course-on tanítjuk

az ITSM folyamatok és eljárások célja:
az informatikai feladatok, és -támogatás

- hatékony
- a megállapodásoknak minőségben és
- teljesítési időpont szerint megfelelő ellátása

legfontosabb követelmények:
- az informatikai szolgáltatásokat a vállalati követelményekhez kell igazítani
- az informatikai szolgáltatások minőségét
  - mérni,
  - javulását kimutatni
  - a költségek csökkentése mellett

végülis ezekre való a COBIT is !

IT szolgáltatás management - IT Service Mangement - ITSM
ahogy az ISACA CISA Review Course-on tanítjuk

szolgáltatási jelentések - néhány mainframe szót változtatva ma is jó!!

- job-ok szabálytalan befejeződése
- operátori problémák
- output szétosztás
- konzol log-ok
- operátori műszakbeosztás

a COBIT domain-ek version 4.1-ig, és a COBIT 5 process-ei

COBIT 1998 - COBIT 4.1 2007 DOMAINS:

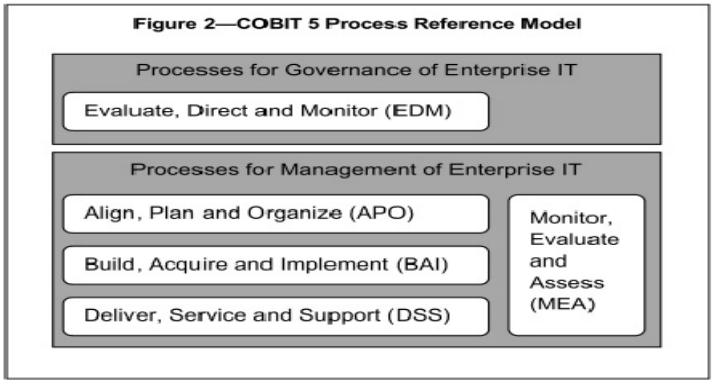
- Plan and Organise (PO)
- Acquire and Implement (AI)
- Deliver and Support (DS)
- Monitor and Evaluate (ME)

COBIT 5 [process types] for the management of enterprise IT:

- Evaluate, Direct and Monitor (EDM)
- Align, Plan and Organise (APO)
- Build, Acquire and Implement (BAI)
- Deliver, Service and Support (DSS)
- Monitor, Evaluate and Assess (MEA)

egy kedvenc ábra az ISACA COBIT Focus-ából

forrás: Stefan Beissel, Ph.D., CISA, CISSP
Supporting PCI DSS 3.0 Compliance With COBIT 5



best practice - COBIT 5 példák

APO01.06 Define information (data) and system ownership.
Acitivies között:

- "Create and maintain an inventory of information (systems and data) that includes a listing of owners, custodians and classifications. Include systems that are outsourced and those for which ownership should stay within the enterprise."

APO12.03 Maintain a risk profile.
Acitivies között:

- "Inventory business processes, including supporting personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers and
  outsourcers, and document the dependency on IT service management processes and IT infrastructure resources."

inventory, document - ugye !

best practice - COBIT 5 példák

"DSS01.02 Manage outsourced IT services.
Manage the operation of outsourced IT services to

- maintain the protection of enterprise information and
- reliability of service delivery."

"Activities:

- 1. Ensure that the enterprise's requirements for security of information processes are adhered to in accordance with contracts and SLAs with third parties hosting or providing services.

- 2. Ensure that the enterprise's operational business and IT processing requirements and priorities for service delivery are adhered to in accordance with contracts and SLAs with third parties hosting or providing services."

az idézet innen van: COBIT ® 5: Enabling Processes - ld. referenciák

best practice - COBIT 5 példák

DSS01.02 Manage outsourced IT services. - folyt.

"Activities:

- 3. Integrate critical internal IT management processes with those of outsourced service providers, covering, e.g., performance and capacity planning,
  change management, configuration management, service request and incident management, problem management, security management, business continuity, and the monitoring of process performance and reporting.
- 4. Plan for independent audit and assurance of the operational environments of outsourced providers to confirm that agreed-on requirements are being adequately addressed."

az idézet innen van: COBIT ® 5: Enabling Processes - ld. referenciák

outsource best practice szemelvények - az ISO 27001-ből

- **8 Operation**
  8.1 Operational planning and control

...

The organization shall ensure that outsourced processes are determined and controlled.

- **A.13 Communications security**
  A.13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

A.13.1.2 Security of network services

control [measure]:

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

outsource best practice szemelvények - az ISO 27001-ből

- **A.14.2.7 Outsourced development control [measure]:**
  The organization shall supervise and monitor the activity of outsourced system development.

Infrastruktúrális elem definíciója
Szenes Katalin: Az informatikai erőforrás-kihelyezés auditálási szempontjai (Az Informatikai biztonság kézikönyve)

Infrastruktúrális elemnek
nevezzük az informatikai infrastruktúra komponenseit.

- Maga a számítógép is infrastruktúrális elem,
- a rajta futó szoftverrel,
- az adatbázis kezelő rendszerrel,
- a számítógépes kommunikációt biztosító hálózati elemekkel,
- az informatikai szolgáltatás megfelelő minőségét, sértetlenségét és bizalmasságát biztosító védelmi elemekkel és persze
- az ezek segítségével működő, az üzleti folyamatot szolgáló alkalmazói programrendszerekkel együtt.

Megj.: a gépen futó SW-be számít az operációs rendszer, és a utility-k is!
Ez - többek között - egy sérülékenységi lehetőség szerinti bontás.

irodalomjegyzék - ISACA

- ***CRM*** 20xx CISA Review Technical Information Manual
  editor: Information Systems Audit and Control Association
  Rolling Meadows, Illinois, USA, 20xx

(1999. óta vagyok: Quality Assurance Team tag)

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

- ***COBIT*** ® 4.1
  Framework, Management Guidelines, Maturity Models
  Copyright © IT Governance Institute®, 2007

- **COBIT** ® 5: Enabling Processes
  Copyright © 2012 ISACA., ISBN 978-1-60420-241-0

(COBIT 5 - 2010, 11, 12 - 2010-11.: Subject Matter Expert Team tag voltam)

irodalomjegyzék - ISO

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

- CRAMM – CCTA Risk Analysis and Management Methodolology
- BS 7799 - BSI
- ISO/IEC 17799
  International Standard ISO/IEC 17799
  First edition 2000-12-01

- International Standard ISO/IEC 27001
  First edition 2005-10-15
  International Standard ISO/IEC 27002 First edition 2005-06-15
  Information technology — Security techniques — Code of practice for information security management

most: 27001, 2 - 2013
+ a 27000-es biztonsági család többi tagja: 27005, 27000

irodalomjegyzék

Szenes Katalin: Az informatikai erőforrás-kihelyezés auditálási szempontjai
Az Informatikai biztonság kézikönyve
I. rész: 36. aktualizálás, 8.10. 1. old. – 26. old. (26 oldal)
Verlag Dashöfer, Budapest, 2010. február
II. rész: 39. aktualizálás, 2010. december
8.10. 27. old. – 158. old.