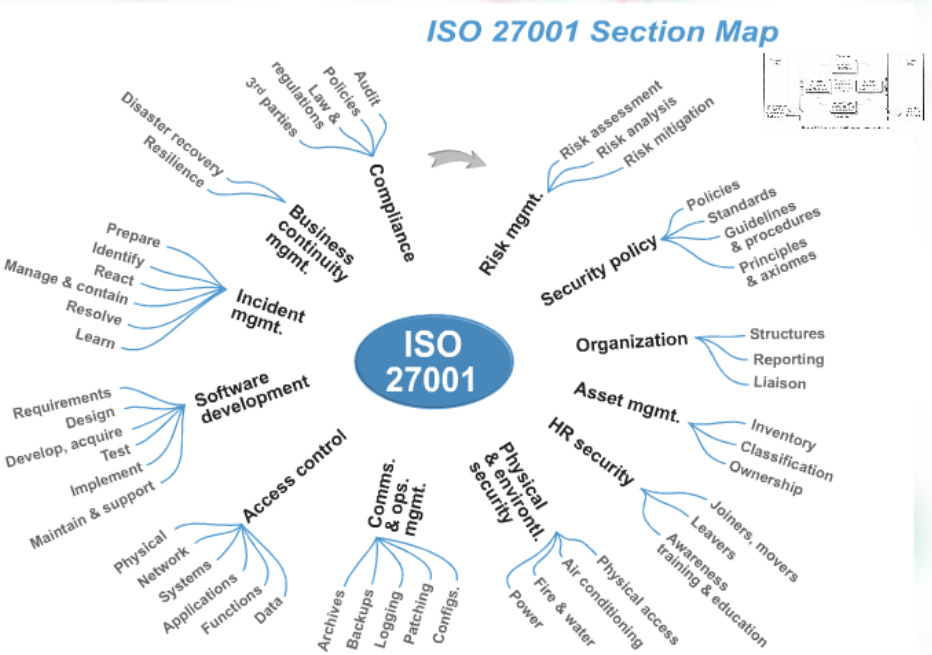
Információbiztonság



ISMS/IBIR bevezetési tapasztalatok

Rónaszéki Péter, CISA, CISM, ISO27001LA

peter.ronaszeki@isaca.hu
peter.ronaszeki@secure-it.hu
(30) 222 5585

Napirend

- Rövid bemutatkozás
- Az ISO27k szabványcsalád, az ISO27001:2005 felépítése
- Merre tart a szabvány fejlődése? ISO/IEC 27001:2013
- Bevezetési tapasztalatok
- Kiszervezett IT és a 27001...
- Hová van "telepítve" a CISO?
- Tévhitek és szakmai hitviták

Rónaszéki Péter, CISA, CISM, ISO 27001 LA

Szakmai tapasztalat:

BISO, Citibank, (1998-2000)
CISO, Budapest Bank, GE Germany, GE USA, (2000-2006)
OISRM, ING Bank (2006-2008)
CISO, Lufthansa Systems (2008-2012)
Secure-IT Hungary (2012-)

Magyar Bankszövetség IB munkacsoport szakértő
ISACA elnökségi tag
„KIBEV" alapító tag
NBF külső szakértő

About the ISO27k standards

ISO 27001 security

At least 32 "ISO27k" standards are planned, more than half of which have been published and are on sale from various official ISO/IEC outlets (not us!):

1. ISO/IEC 27000:2012 - provides an **overview/introduction** to the ISO27k standards plus a glossary for the specialist **vocabulary**. Changed
2. ISO/IEC 27001:2013 is the **Information Security Management System (ISMS) requirements standard,** a formal specification for an ISMS. New
3. ISO/IEC 27002:2013 is the **code of practice for information security controls** describing good practice information security control objectives and controls. New
4. ISO/IEC 27003:2010 provides **guidance on implementing ISO/IEC 27001.** Changed
5. ISO/IEC 27004:2009 covers **information security management measurement** (metrics). Changed
6. ISO/IEC 27005:2011 covers **information security risk management**.
7. ISO/IEC 27006:2011 is a guide to the **certification or registration process** for accredited ISMS certification or registration bodies. Changed
8. ISO/IEC 27007:2011 is a guide to **auditing Information Security Management Systems.**
9. ISO/IEC TR 27008:2011 concerns the **auditing of technical security controls.**
10. ISO/IEC 27009 will cover certified **compliance to sector- or service-specific versions of**

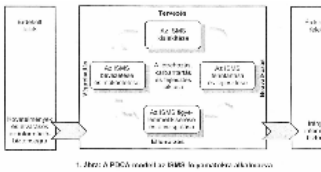
6. ISO/IEC 27005:2011 covers **information security risk management**.
7. ISO/IEC 27006:2011 is a guide to the **certification or registration process** for accredited ISMS certification or registration bodies. Changed
8. ISO/IEC 27007:2011 is a guide to **auditing Information Security Management Systems.**
9. ISO/IEC TR 27008:2011 concerns the **auditing of technical security controls.**
10. ISO/IEC 27009 will cover certified **compliance to sector- or service-specific versions of ISO/IEC 27001**.
11. ISO/IEC 27010:2012 provides guidance on **information security management for inter-sector and inter-organisational communications.**
12. ISO/IEC 27011:2008 is the **information security management guideline for telecommunications organizations** (dual-numbered as ITU X.1051).
13. ISO/IEC 27013:2012 provides guidance on the **integrated/joint implementation of both ISO/IEC 27001** (ISMS) **and ISO/IEC 20000-1** (service management, derived from ITIL).
14. ISO/IEC 27014:2013 offers guidance on the **governance of information security.**
15. ISO/IEC TR 27015 provides **information security management guidelines for financial services.**
16. ISO/IEC TR 27016 will cover the **economics of information security management.** Changed
17. ISO/IEC 27017 will cover **information security controls for cloud computing.**
18. ISO/IEC 27018 will cover **privacy aspects of cloud computing.** Changed
19. ISO/IEC TR 27019 will cover information security for **process control** [mostly?] in the energy industry.
20. ISO/IEC 27031:2011 is an ICT-focused standard on **business continuity.**
21. ISO/IEC 27032:2012 covers **cybersecurity.**

17. ISO/IEC 27017 will cover **information security controls for cloud computing.**
18. ISO/IEC 27018 will cover **privacy aspects of cloud computing.** Changed
19. ISO/IEC TR 27019 will cover information security for **process control** [mostly?] in the energy industry.
20. ISO/IEC 27031:2011 is an ICT-focused standard on **business continuity.**
21. ISO/IEC 27032:2012 covers **cybersecurity.**
22. ISO/IEC 27033 is replacing the multi-part ISO/IEC 18028 standard on **IT network security** (parts 1, 2 & 3 are published, the others are in preparation).
23. ISO/IEC 27034 is providing guidelines for **application security** (part 1 was released in 2011, the others are in preparation).
24. ISO/IEC 27035:2011 on **information security incident management.** Changed
25. ISO/IEC 27036 will be a security guideline for **supplier relationships** including the relationship management aspects of cloud computing. Changed
26. ISO/IEC 27037:2012 covers identifying, gathering and preserving **digital evidence.**
27. ISO/IEC 27038 will be a specification for **digital redaction.**
28. ISO/IEC 27039 concerns **intrusion detection and prevention systems.**
29. ISO/IEC 27040 guideline on **storage security.** Changed
30. ISO/IEC 27041 guideline on **assurance for digital evidence investigation methods.**
31. ISO/IEC 27042 guideline on **analysis and interpretation of digital evidence.**
32. ISO/IEC 27043 guideline on **digital evidence investigation principles and processes.**
33. ISO/IEC 27044 guideline on **SIEM (Security Incident and Event Management)** Changed
34. ISO 27799:2008 provides **health sector specific ISMS implementation guidance** based on ISO/IEC 27002.

Mi is az ISO 27001?

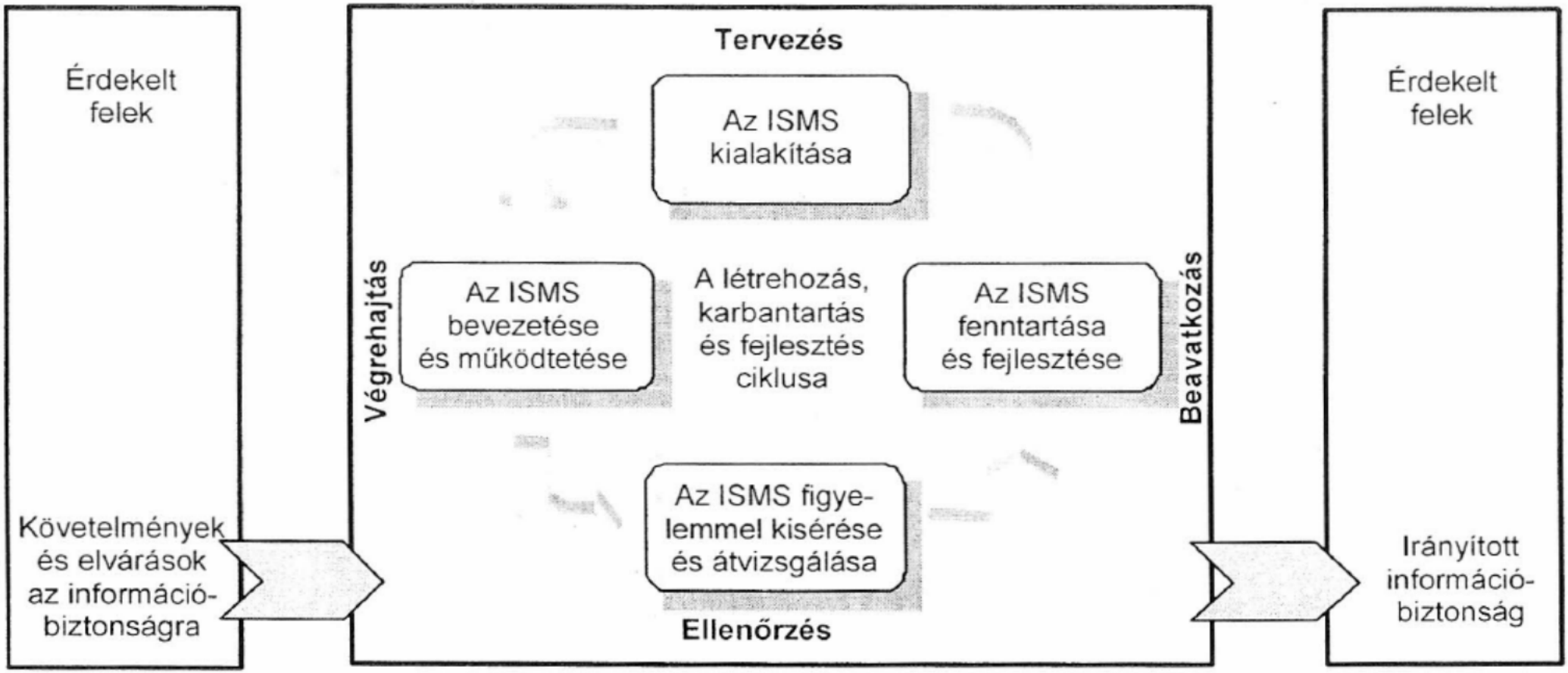
- Nemzetközi információbiztonság-irányítási rendszerszabvány (tanúsítható...)
- Kockázatelemzés 'alapú'
  - Támogatja a folyamatos fejlődést: Plan – Do – Check – Act
- NEM technikai szabvány !
  - Információbiztonsági szabályzat
  - Információbiztonsági szervezet
  - Információs vagyon kezelése
  - Emberi erőforrás biztonsága
  - Fizikai és környezeti biztonság
  - Kommunikáció és működés irányítás
  - Hozzáférés szabályozás
  - Rendszerek beszerzése, fejlesztése, karbantartása
  - Információbiztonsági incidensek kezelése
  - Üzletmenet-folytonosság menedzselése
  - Megfelelőség

ISO 27001 Section Map



ISO 27001

- Compliance
  - Audit
  - Policies
  - Law & regulations
  - 3rd parties
- Business continuity mgmt.
  - Disaster recovery
  - Resilience
- Incident mgmt.
  - Prepare
  - Identify
  - React
  - Manage & contain
  - Resolve
  - Learn
- Software development
  - Requirements
  - Design
  - Develop, acquire
  - Test
  - Implement
  - Maintain & support
- Access control
  - Physical
  - Network
  - Systems
  - Applications
  - Functions
  - Data
- Comms. & ops. mgmt.
  - Archives
  - Backups
  - Logging
  - Patching
  - Configs.
- Physical & environtl. security
  - Power
  - Fire & water
  - Air conditioning
  - Physical access
- HR security
  - Joiners, movers
  - Leavers
  - Awareness training & education
- Asset mgmt.
  - Inventory
  - Classification
  - Ownership
- Organization
  - Structures
  - Reporting
  - Liaison
- Security policy
  - Policies
  - Standards
  - Guidelines & procedures
  - Principles & axiomes
- Risk mgmt.
  - Risk assessment
  - Risk analysis
  - Risk mitigation



1. ábra: A PDCA-modell az ISMS-folyamatokra alkalmazva

ISO 27001:2005

5. BIZTONSÁGI POLITIKA
5.1. Információbiztonsági politika
5.1.1. Információbiztonsági politika dokumentuma
5.1.2.Információbiztonsági politika átvizsgálása

6. AZ INFORMÁCIÓBIZTONSÁG SZERVEZETE
6.1. Belső szervezet
6.1.1. Vezetőség információbiztonsági elkötelezettsége
6.1.2. Információbiztonság irányítási koordináció
6.1.3. Információbiztonsági felelősségek meghatározása
6.1.4. Jóváhagyási folyamat az információkezelés eszközeinek használatára
6.1.5. Titoktartási megállapodások
6.1.6. Kapcsolattartás a hatóságokkal
6.1.7. Kapcsolattartás érdekképviseleti fórumokkal
6.1.8. Információbiztonság független átvizsgálása
6.2. Külső felek
6.2.1. Külső fél általi hozzáférésből adódó kockázatok azonosítása
6.2.2. Biztonsági követelmények az ügyfélkapcsolatban
6.2.3. Biztonsági követelmények a harmadik féllel kötött szerződésekben

7. INFORMÁCIÓS VAGYON KEZELÉSE
7.1. Az eszközökkel kapcsolatos felelősségek
7.1.1. Vagyonleltár
7.1.2. A vagyontárgyak tulajdonlása
7.1.3. Megfelelő eszközhasználat
7.2. Információ osztályozás
7.2.1. Osztályozási irányelvek
7.2.2. Információ jelölés és kezelés

8. AZ EMBERI ERŐFORRÁS BIZTONSÁGA
8.1. Munkába lépés előtt
8.1.1. Szerepek és felelősségek
8.1.2. Szűrés
8.1.3. Alkalmazási feltételek
8.2. Az alkalmazás alatt
8.2.1. A vezetőség felelőssége
8.2.2. Információbiztonsági tudatosság, oktatás és képzés
8.2.3. Fegyelmi eljárás
8.3. Alkalmazás megszűnése vagy megváltozása
8.3.1. A megszűnéssel kapcsolatos felelősségek
8.3.2. Eszközök visszaszolgáltatása
8.3.3. Hozzáférési jogok megvonása

9. FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG
9.1. Védett területek
9.1.1. Védett területek körülhatárolása
9.1.2. Beléptetés szabályozása
9.1.3. Irodák, helyiségek és eszközök védelme
9.1.4. Külső és környezeti fenyegetések elleni védelem
9.1.5. Munkavégzés védett területen
9.1.6. Nyilvánosan hozzáférhető kiszállítási és rakodási terület
9.2. Berendezések védelme
9.2.1. Berendezések elhelyezése és védelme
9.2.2. Támogató közművek
9.2.3. Kábelezés védelme
9.2.4. Berendezések karbantartása
9.2.5. Berendezések szervezeten kívüli biztonsága
9.2.6. Berendezések biztonságos megsemmisítése és újrahasznosítása
9.2.7. Eszközök elvitele

10. A KOMMUNIKÁCIÓ ÉS A MŰKÖDÉS IRÁNYÍTÁSA
10.1. Működési eljárások és felelősségi körök
10.1.1. Dokumentált működési eljárások
10.1.2. Változáskezelés
10.1.3. Kötelességek szétválasztása
10.1.4. Fejlesztő-, teszt -és éles üzemi eszközök szétválasztása
10.2. Harmadik fél által nyújtott szolgáltatások menedzselése
10.2.1. Szolgáltatás nyújtása
10.2.2. Harmadik fél által nyújtott szolgáltatás megfigyelése és felülvizsgálata
10.2.3. Harmadik fél által nyújtott szolgáltatás módosításának kezelése
10.3. Rendszerek tervezése és átvétele
10.3.1. Kapacitástervezés
10.3.2. Rendszerátvétel
10.4. Védelem rosszindulatú és mobil szoftverek ellen
10.4.1. Óvintézkedések a rosszindulatú szoftverek ellen
10.4.2. Óvintézkedések a mobil kódok ellen
10.5. Mentés
10.5.1. Másolatok készítése
10.6. Hálózati biztonság menedzselése
10.6.1. Hálózati óvintézkedések
10.6.2. Hálózati szolgáltatások biztonsága
10.7. Adathordozók kezelése
10.7.1. Hordozható számítógépes adathordozók kezelése
10.7.2. Adathordozók megsemmisítése
10.7.3. Információkezelési eljárások
10.7.4. Rendszerdokumentáció védelme
10.8. Információcsere
10.8.1. Információcsere szabályozása és módja
10.8.2. Információcsere-megállapodások
10.8.3. Fizikai média szállítása
10.8.4. Elektronikus üzenetek
10.8.5. Üzleti információs rendszerek
10.9. Elektronikus kereskedelmi szolgáltatások
10.9.1. Elektronikus kereskedelem
10.9.2. On-line tranzakciók
10.9.3. Nyilvánosan hozzáférhető információ
10.10. Megfigyelés
10.10.1. Felügyeleti naplózás
10.10.2. A rendszerhasználat megfigyelése
10.10.3. Naplóinformáció védelme
10.10.4. Adminisztrátori és operátori napló
10.10.5. Hibanaplózás
10.10.6. Rendszerórák szinkronizálása

11. HOZZÁFÉRÉS SZABÁLYOZÁS
11.1. A hozzáférés szabályozásának szervezeti követelményei
11.1.1. Hozzáférés szabályozási politika
11.2. Felhasználók hozzáférésének menedzselése
11.2.1. Felhasználók nyilvántartása
11.2.2. Privilégiumok kezelése
11.2.3. Felhasználói jelszavak menedzselése
11.2.4. Felhasználói hozzáférési jogok átvizsgálása
11.3. Felhasználók felelőssége
11.3.1. Jelszóhasználat
11.3.2. Felügyeletlen felhasználói berendezések
11.3.3. Üres asztal és üres képernyő szabály
11.4. Hálózati hozzáférés szabályozása
11.4.1. Hálózati szolgáltatások használatának politikája (irányelvei)
11.4.2. Felhasználók hitelesítése külső kapcsolatoknál
11.4.3. Eszközök hálózati azonosítása
11.4.4. Távdiagnosztikai és konfigurációs portok védelme
11.4.5. Hálózat-szegmentálás
11.4.6. Hálózatokhoz való csatlakozás szabályozása
11.4.7. Hálózati útvonalválasztás szabályozása
11.5. Operációs rendszerekhez való hozzáférés szabályozása
11.5.1. Biztonságos bejelentkezési eljárások
11.5.2. Felhasználók azonosítása és hitelesítése
11.5.3. Jelszókezelő rendszer
11.5.4. Rendszer-segédprogramok használata
11.5.5. Folyamat időlejárat
11.5.6. Kapcsolati idő korlátozása
11.6. Alkalmazás és információ hozzáférés szabályozás
11.6.1. Információhoz való hozzáférés korlátozása
11.6.2. Kritikus rendszerek elkülönítése
11.7. Mobil eszközök és távmunka
11.7.1. Mobil eszközök és kommunikáció
11.7.2. Távmunka

12. RENDSZEREK BESZERZÉSE, FEJLESZTÉSE ÉS KARBANTARTÁSA
12.1. Információs rendszerek biztonsági követelményei
12.1.1. Biztonsági követelmények elemzése és előírása
12.2. Alkalmazások helyes működése
12.2.1. Bemenő adatok érvényesítése
12.2.2. Belső folyamatok ellenőrzése
12.2.3. Üzenetek sértetlensége
12.2.4. Kimenő adatok érvényesítése
12.3. Kriptográfiai óvintézkedések
12.3.1. Kriptográfiai óvintézkedések használatának irányelvei
12.3.2. Kulcsgondozás
12.4. Rendszerállományok biztonsága
12.4.1. Éles üzemben működő szoftverek felügyelete
12.4.2. Rendszerteszt adatok védelme
12.4.3. Forráskódokhoz való hozzáférés szabályozása
12.5. A fejlesztési és támogatási folyamatok biztonsága
12.5.1. Változtatások felügyeleti eljárása
12.5.2. Alkalmazások műszaki felülvizsgálata az operációs rendszer változásakor
12.5.3. Szoftvercsomagok módosításának korlátozása
12.5.4. Információ szivárgás
12.5.5. Kiszervezett szoftverfejlesztés
12.6. Műszaki sebezhetőségek kezelése
12.6.1. Műszaki sebezhetőségek felügyelete

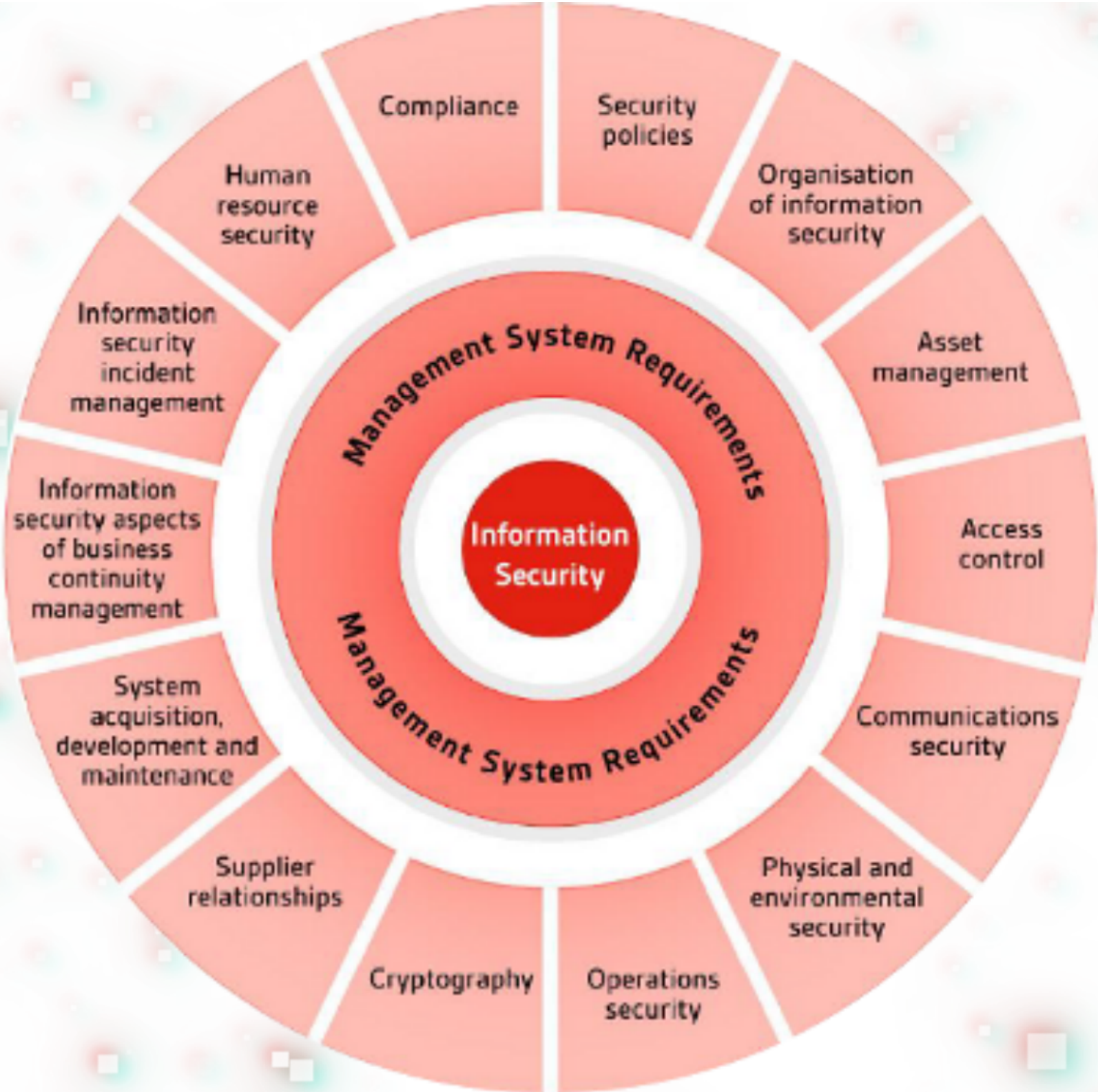
13. INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE
13.1. Információbiztonsági események és gyengeségek jelentése
13.1.1. Információbiztonsági események jelentése
13.1.2. Információbiztonsági gyengeségek jelentése
13.2. Információbiztonsági incidensek és fejlesztések kezelése
13.2.1. Felelősségek és eljárások
13.2.2. Tanulás az információbiztonsági incidensekből
13.2.3. Bizonyítékok gyűjtése

14. ÜZLETMENET FOLYTONOSSÁGÁNAK MENEDZSELÉSE
14.1. Folyamatos működés biztosításának információbiztonsági szempontjai
14.1.1. Információbiztonság figyelembe vétele az üzletmenet folytonossági folyamatokban
14.1.2. Üzletmenet folytonosság és kockázatelemzés
14.1.3. Az információbiztonságot figyelembe vevő üzletmenet folytonossági tervek készítése és bevezetése
14.1.4. Üzletmenet folytonosság tervezési keretrendszere
14.1.5. Üzletmenet folytonossági tervek tesztelése, karbantartása és újraértékelése

15. MEGFELELŐSÉG BIZTOSÍTÁSA
15.1. Megfelelés a jogi követelményeknek
15.1.1. Vonatkozó jogszabályok azonosítása
15.1.2. Szellemi tulajdonjogok
15.1.3. Szervezeti feljegyzések védelme
15.1.4. Adatvédelem és személyes adatok bizalmassága
15.1.5. Információfeldolgozó eszközökkel való visszaélés megelőzése
15.1.6. Kriptográfiai óvintézkedések szabályozása
15.2. Megfelelés a biztonsági politikának és szabályozásnak, műszaki megfelelőség
15.2.1. Megfelelés a biztonsági politikának és szabályozásnak
15.2.2. Műszaki megfelelés ellenőrzése
15.3. Rendszer felülvizsgálat szempontjai
15.3.1. Információs rendszer felülvizsgálati óvintézkedések
15.3.2. Rendszer felülvizsgálati eszközök védelme

Legfontosabb változások (ISO 27001:2005 -> 2013)

- 133/11 vs 114/14
- Definíciók a 27000-ben
- PDCA nem kötelező (PDCA vagy process megközelítés)
- "Management Commitments" -> "Leadership Clause"
- Megelőző tevékenységek helyett:
  megoldandó feladatok, kockázatok és lehetőségek
- Általános kockázatelemzési követelmények (ISO 31000)
- Nagyobb hangsúlyt kapnak:
  célok, ellenőrzések, mérések

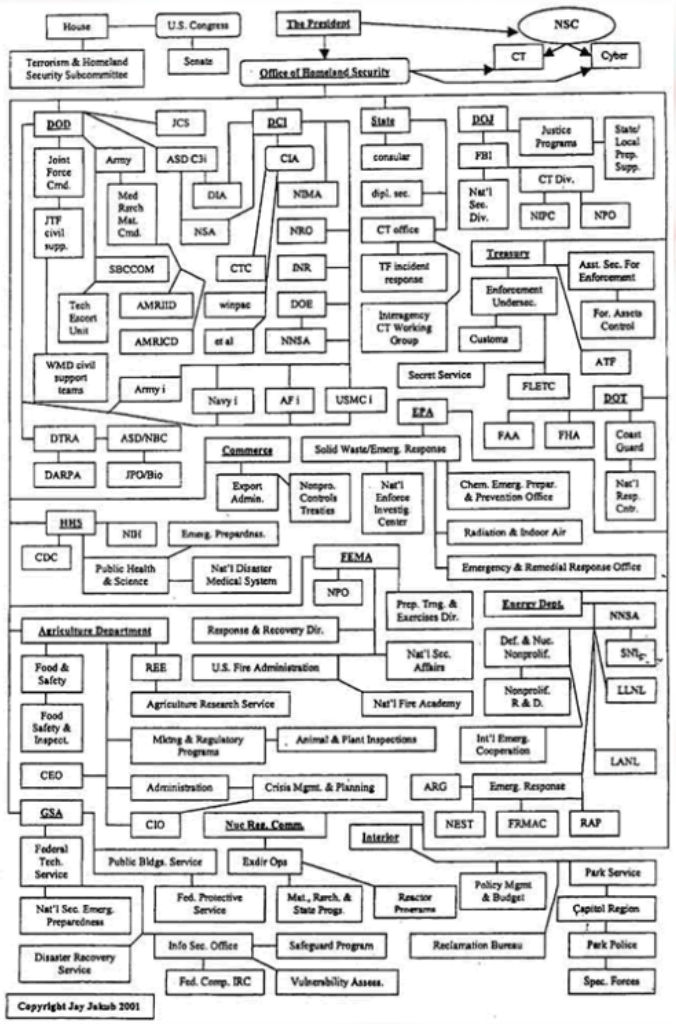

Compliance
Security policies
Organisation of information security
Asset management
Access control
Communications security
Physical and environmental security
Operations security
Cryptography
Supplier relationships
System acquisition, development and maintenance
Information security aspects of business continuity management
Information security incident management
Human resource security
Management System Requirements
Information Security
Management System Requirements

Bevezetési tapasztalatok

- Nincs ingyen...
- Nem "csak" technológia, két részből áll...
- "Mindenki" kell hozzá...
- Kiszervezett IT - black box?
- Igen, meg lehet bukni...
- Egyre nagyobb az igény a tanúsításra...
- A tanúsítvány következmény legyen, ne cél!

CISO, BISO, CSO, LSO... Hol a helye?

- Független
- Összeférhetetlenség
- Több sapkás...
- 1 ember vs csapat
- Kiszervezve?



Egyéb gondolatok, kérdések

- Irányítási rendszer
- ISMS <> BCMS
- Belső erőforrás vs. tanácsadó
- Mérőszámok hiánya
- Amíg nincs baj, addig nincs baj...
- 2013. évi L. törvény

Köszönöm a figyelmet!
Kérdések ?

Rónaszéki Péter, CISA, CISM, ISO27001 LA
peter.ronaszeki@isaca.hu
peter.ronaszeki@secure-it.hu
(30) 222 5585