XXX. NEMZETI
MINŐSÉGÜGYI
KONFERENCIA

MagiCom
BUDAPEST LONDON

Dr. Tarján Gábor
információbiztonsági
tanácsadó, MagiCom Kft.

Az információbiztonsági követelménydzsungel – azonosságok és különbségek

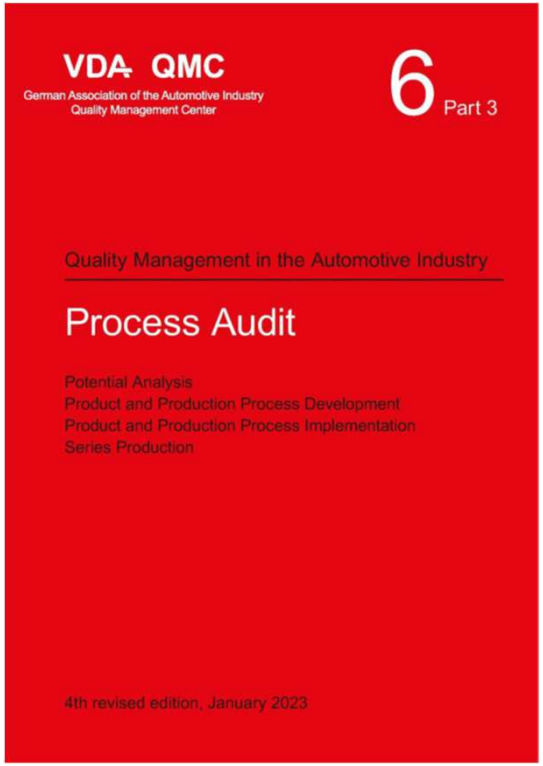
Áttekintő tartalom

- Rövid bemutatkozás
- Miért (is) fájhat egy minőségügyi vezető feje manapság?
- Néhány mítosz és tévképzet az információbiztonsággal kapcsolatban
- Az információbiztonsági követelménydzsungel
  - Bizonyos iparágakhoz kötődőek
  - Nemzetköziek és iparágtól függetlenek
- Azonosságok és különbségek
- Kérdések és válaszok

Miért (is) fájhat egy minőségügyi vezető feje manapság?

XXX. NEMZETI MINŐSÉGÜGYI KONFERENCIA

- „Post-Covid szindróma” (home office?)
- Háború (a szállítói láncok és szállítási feltételek átalakulása)
- Szakképzett munkaerő hiánya (távozása, fluktuációja…)
- Változó követelmények (pl. VDA 6.3:2023)
- …és támad az információbiztonság! Pl. ISO 27001:2022 (Ki legyen a cégnél az információbiztonsági vezető, mert most már ilyen is kell nekünk?!)



Néhány mítosz az adatvédelemmel és az információbiztonsággal kapcsolatban

- ”Ehhez nekem semmi közöm, ez egy informatikusoknak szóló dolog”
- “Ez csak szabályzatok és eljárások írogatását jelenti”
- “Csak elveszünk a sok papír és előírás között”
- “Ezek a követelmények (pl. GDPR, ISO, TISAX) csak a napi munkánkat nehezítik”
- “Egy ilyen irányítási rendszert két hónap alatt megcsinál és bevezet a cégünk”
- “Csak a tanúsítványok miatt csináljuk”

Hasznok a cégünk számára

- A bizalmas információk megtartását segíti
- A vevőket és más érdekelt feleket biztosítja arról, hogy megfelelően kezeljük a kockázatokat!
- Növeli a vevői elégedettséget
- Biztonságossá teszi az információcserét
- Versenyelőnyt biztosít a cégnek a versenytársakkal szemben
- A kockázati kitettséget csökkenti
- Védi a szervezet információs vagyonát, az érdekelt feleket és a vevőket

Hasonló követelményrendszerek

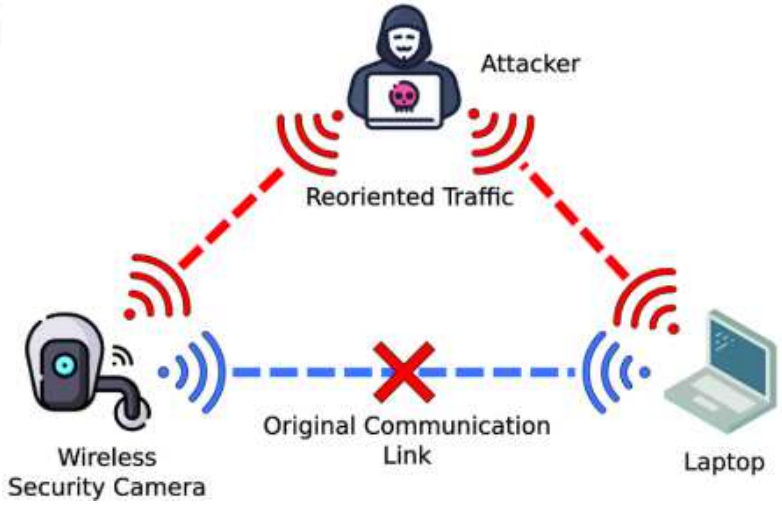
- Az érintett és röviden bemutatott információbiztonsági követelményrendszerek:
    - Bizonyos iparágakhoz kötődőek:
        - HIPAA (egészségügy)
        - PCI DSS 4.0 – 2022.03 (elektronikus kártya)
        - TISAX 5.1.0 – 2022.05.01 (autóipar)
    - „Nemzetköziek és iparágtól függetlenek”:
        - SOX / tőzsdei cégek (New York)
        - ITIL (ISO 20000) / IT szolgáltatás menedzsment
        - COBIT2019 / IT szabályozás
        - ISO 27001 : 2022 információbiztonság
- A bemutatás értelemszerűen messze **nem teljes**, de kellően reprezentatív, és az egyes követelményrendszerek közös gyökereire illetve rokon vonásaira mutat rá.

Hasonló követelményrendszerek

- Iparágfüggetlen, közös témák!

Kulcsszavak:

- Kockázat alapú megközelítés
- Dokumentált folyamatok
- Folyamati kontrollok
- Belső auditok
- Vezetőségi átvizsgálás
- Helyesbítő és megelőző intézkedések
- Folyamatos fejlődés
- Tudatosítás (képzés…)



Az ISO 27000-es szabványcsalád

XXX. NEMZETI MINŐSÉGÜGYI KONFERENCIA

27000 Áttekintés és szótár

27001 Követelmények

Útmutatók
27002 Code of practice for IS controls
27003 Implementation guide

Auditorok, auditálás
27006 Követelmények ISMS tanúsítóknak
27007 ISMS auditálás útmutató
27008 IS kontroll audit útmutató

Biztonsági területek, ágazatok
27004 Mérés
27005 Kockázat menedzsment
27035 Incidens menedzsment
27031 Folytonosság

27033 Network security
27034 Application security

27011 Telecom
27017 Cloud services
27019 Energy utilities
27799 Health informatics

Az ISO 27001:2022 szabvány

INTERNATIONAL STANDARD

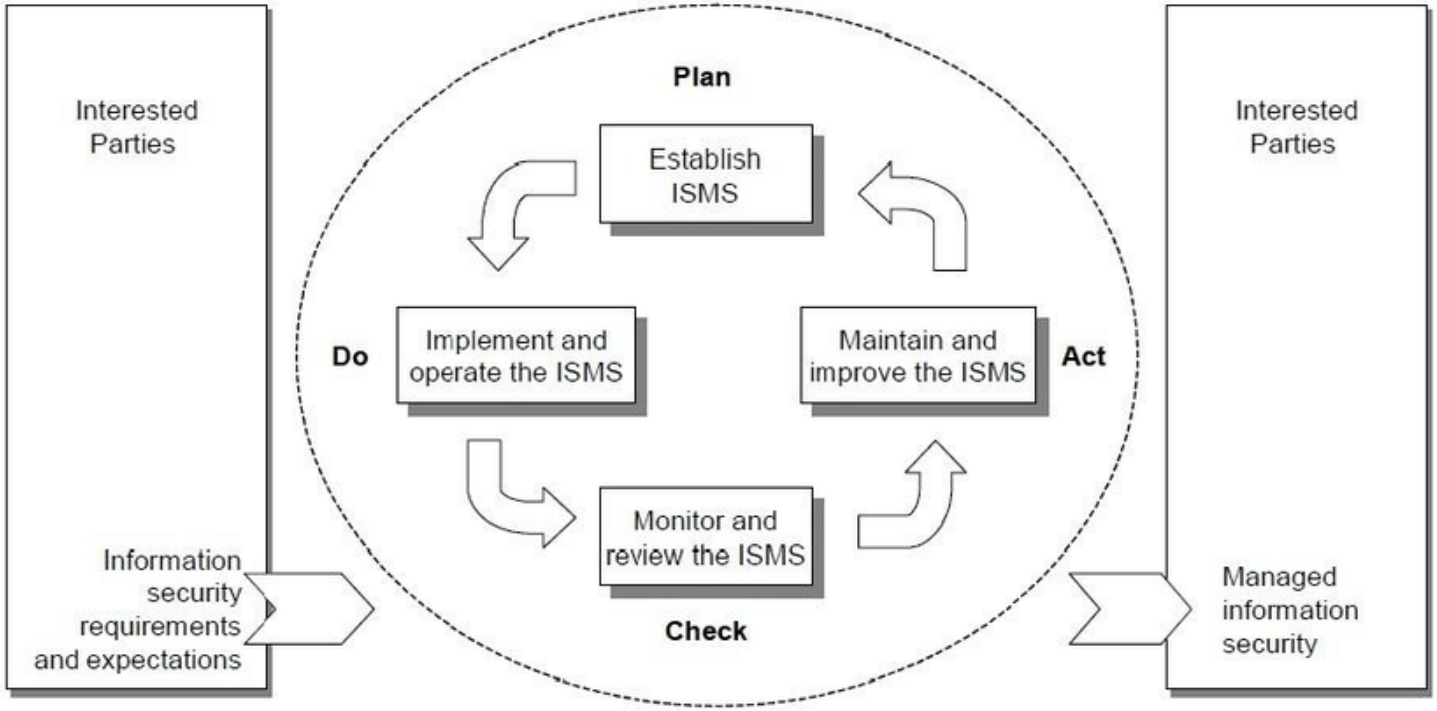
ISO/IEC 27001

Third edition
2022-10

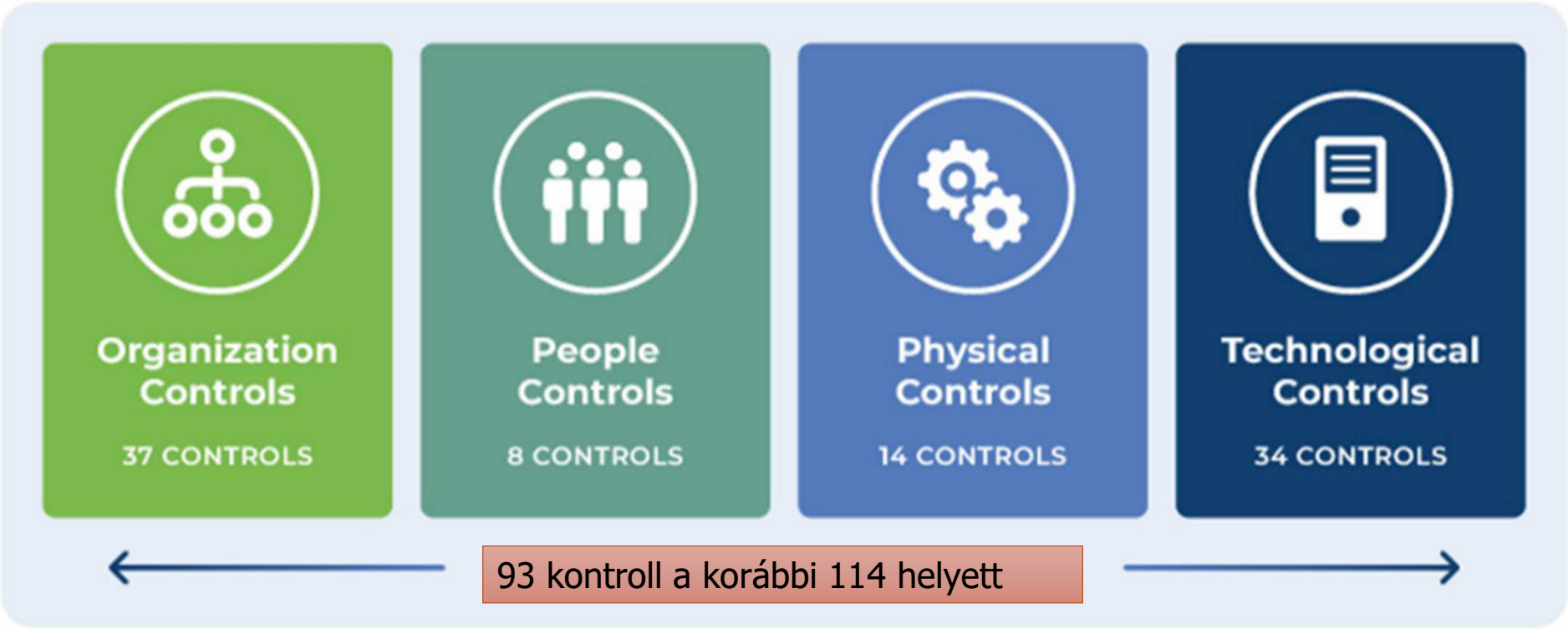
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Az ISO 27001:2022 szabvány belső logikája (szabványtest)



Az ISO 27001:2022 szabvány belső logikája („A” melléklet)



XXX. NEMZETI
MINŐSÉGÜGYI
KONFERENCIA

Köszönöm a figyelmet!

Dr. Tarján Gábor

20-502-7775

gabor.tarjan@magicom.com