A tanúsítás és auditálási gyakorlat változása nemzetközi tükörben

Tarján Gábor

2014. április 10.

Tartalom és tematika

- Rövid bemutatkozás
- Pár fontos mondat
- Az átmenet szabályai nemzetközi (IAF, UKAS, DAKKS) tükörben
- Hangsúlyok eltolódása, követelmények finomhangolása és egyéb változások
- Kérdések-válaszok

MagiCom BUDAPEST LONDON

Tarján Gábor

- Szervező-vegyészmérnök - MSc (VE 1986)
- Mérnök-közgazdász (BKE 1992), MBA (BME 2000)
- *korábban* nemzetközi bejegyzésű „ISO 9001-es” vezető felülvizsgáló (Lead Assessor/Auditor - IQA IRCA)
- **2006 óta ISMS (ISO 27001) Lead Auditor (DEKRA Certifications)**
- CMC – „hites vezetési tanácsadó” (VTMSZ - ICMCI)
- CISA – bejegyzett információrendszer felülvizsgáló (ISACA)
- CISM - bejegyzett információbiztonsági menedzser (ISACA)
- CGEIT – bejegyzett vállalati informatikai menedzser (ISACA)
- 25 év vezetési tanácsadás, 20 év tréneri, oktatói tapasztalat
- 5 év cégvezetés, 13 év információbiztonság (www.hetpecset.hu)
- Hétpecsét Információbiztonsági Egyesület alelnöke
- Kompetenciák:
  - Minőségügyi és információbiztonsági felülvizsgálatok és auditok
  - Irányítási rendszerek bevezetése, IT szolgáltatás menedzsment
  - Tréningek és műhelyszemináriumok vezetése, lebonyolítása
  - Egyetemi és főiskolai oktatás (PE, BKF, ZSKF, Corvinus…)

MagiCom BUDAPEST LONDON

Pár fontos mondat

- Bár túl vagyok számos fejtágításon és blog olvasáson , de nem végeztem még auditot az új szabvány alapján (de már nagyon várom…)
- Nem a DEKRA (vagy más tanúsító testület) hivatalos álláspontját képviselem
- Nincsenek őrült nagy változások a régi szabványhoz képest (de a józan ész most is segíthet…)

MagiCom BUDAPEST LONDON

Az átmenet várható szabályai (UKAS)

- UKAS:
- "The General Assembly, acting on the recommendation of the Technical Committee, resolved to endorse ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements, as a normative document. The General Assembly further agreed that the deadline for conformance to ISO/IEC 27001:2013 will be **two years** from the date of publication. One year after publication of ISO/IEC 27001:2013, **all new accredited certifications issued shall be to ISO/IEC 27001:2013**.
- Note: As the date of publication was 1 October 2013, the deadline for Certification Bodies to conform will be 1 October 2015."

MagiCom BUDAPEST LONDON

Az átmenet várható szabályai (DAKKS)

- DAKKS (2013.12.09.):

Informationssicherheits-Management: Umstellung auf die neue ISO/IEC 27001:2013

Auf seiner 27. Generalversammlung hat das International Accreditation Forum (IAF) eine zweijährige Einführungsfrist für die revidierte Version des international anerkannten Standards für Informationssicherheits-Management ISO/IEC 27001:2013 („Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme – Anforderungen") beschlossen.

© Maksim Kabakou - Fotolia.com

Die Übergangsfrist für bestehende Zertifikate nach der Vorgängernorm ISO/IEC 27001:2005 endet danach am 1. Oktober 2015. Schon ein Jahr früher, also ab 1. Oktober 2014, dürfen bei Erst- und Re-Zertifizierung nur noch Zertifikate auf der Grundlage der neuen Norm ausgestellt werden. Die Umstellung erfolgt auf der Basis eines Audits im Unternehmen.

MagiCom BUDAPEST LONDON

Az átmenet várható szabályai (MSZT/IAF)

A Nemzetközi Akkreditálási Fórum határozata

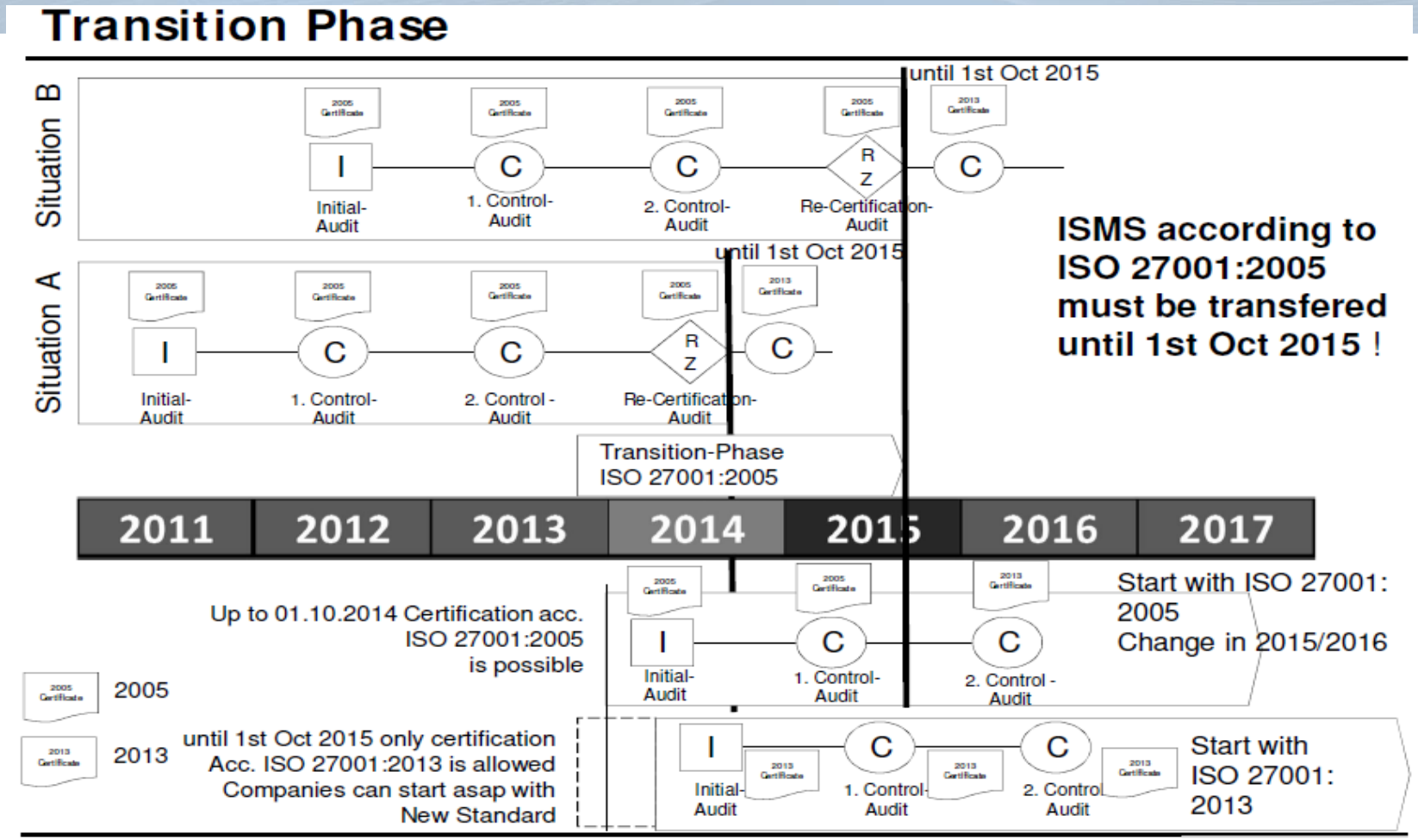
A Nemzetközi Akkreditálási Fórum (IAF;International Accreditation Forum) 2013. október 23-25. között tartott 27. közgyűlése a fórum műszaki bizottságának ajánlása alapján úgy határozott, hogy az irányítási rendszereket tanúsító szervezetek számára egységesen alkalmazandó, szabályozó dokumentumként jóváhagyja az **ISO/IEC 27001:2013 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények** című szabványt, amely az **ISO/IEC 27001:2005** korszerűsített kiadása.
A közgyűlés megegyezett továbbá abban, hogy az ISO/IEC 27001:2013 szabvány szerinti megfelelésre való áttérés határideje az új szabvány közzétételének időpontjától, **2013. október 1-jétől számított két év** legyen és **egy évvel** a szabvány közzétételét követően **minden újonnan kiadott akkreditált tanúsítványnak** az ISO/IEC 27001:2013 szabvány követelményeinek való megfelelést kell igazolnia.

Ezekből következően az új szabványra való áttérés határideje a következő:

- az ISO/IEC 27001:2005 szabvány szerint már tanúsított szervezetek számára **2015. október 1.,** megújító audit esetén azonban **2014. október 1.** után már az új ISO/IEC 27001:2013 szabvány követelményeinek kell megfelelni;
- kezdeti tanúsító audit (első audit) esetén **2014. október 1.**

MagiCom BUDAPEST LONDON

Az átmenet várható szabályai (DEKRA és más nemzetközi tanúsítók)



MagiCom BUDAPEST LONDON

Hangsúlyok és egyebek változásai

- A szervezet környezete
  - Érdekelt felek (Kik ők? Lista..)
  - … és milyen elvárásaik vannak
- A megfigyelés és mérés önálló fejezetben, tehát… célok és mérhetőségük?
- Kockázat tulajdonos (és nem vagyonelem tulajdonos)
- Kockázatértékelés (nem előfeltétel a vagyonelemek, a veszélyek és a sérülékenységek azonosítása!)

MagiCom BUDAPEST LONDON

Hangsúlyok és egyebek változásai

- Kockázatértékelés (nagyobb hangsúly van rajta, erre az auditor válasza: több idő)
  - Módszertan? (a választás szabadsága!)
    - ISO 27005 (nem változott)
    - ISO 31000 (ERM – enterprise risk managment)
    - OCTAVE, NIST stb.
  - Világos kockázatkezelési opciók (csökkent, elfogad, elkerül, megoszt)
- Mi a kockázat-tulajdonos szerepe?
  - Elfogadja a kockázatkezelési tervet és a maradvány kockázatot!

MagiCom BUDAPEST LONDON

Hangsúlyok és egyebek változásai

- Az Alkalmazhatósági Nyilatkozat és a szabvány „A” mellékletének viszonya, szerepe és a tanúsítói, tanácsadói megközelítés:
  - „2005”: Az alkalmazandó kontrollok (intézkedések) kiválasztása a „leltárból”…
  - „2013”: Az alkalmazandó kontrollok a kockázatkezelési folyamatból potyognak ki…

MagiCom BUDAPEST LONDON

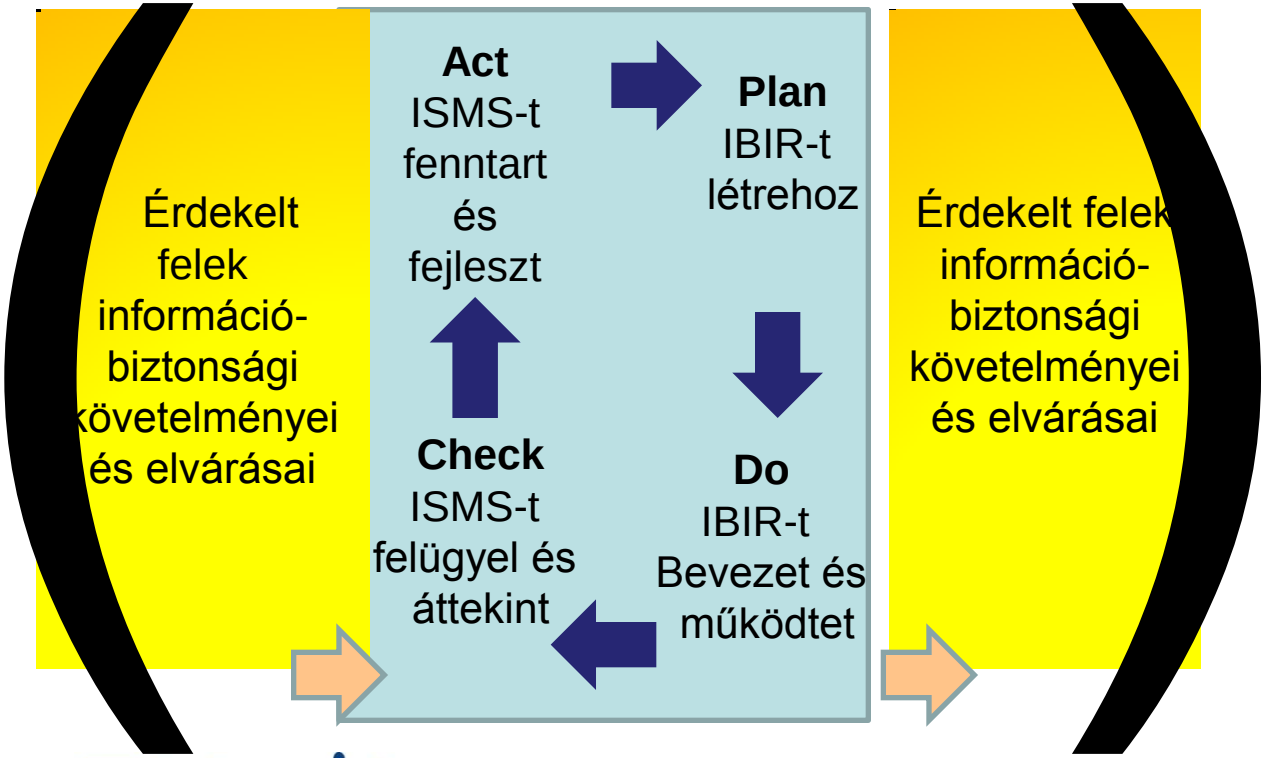
Hangsúlyok és egyebek változásai

- A PDCA explicit módon nem említett a szabványban, de ugye nem gondoljuk, hogy ez azt jelenti…
- Continuous / continual improvement
  - Változó környezet (veszélyek, fenyegetések)
  - Változó igények az érdekelt felek részéről
  - Technológiai fejlődés (lásd pl. felhő)
  - Változó szervezet (működési mód)

Az ISO 27001:2013 struktúrája

A szabványtest (0-10 fejezetek) és az „A” melléklet, melyben:

- 14 Információbiztonsági szabályozási terület (A5-A18)
- 35 Információbiztonsági szabályozási cél
- 114 Információbiztonsági intézkedés (kontroll)



14 Szabályozási terület:

1. Információbiztonsági politika
2. Az információbiztonság szervezete
3. A humánerőforrás biztonsága
4. Vagyonmenedzsment
5. Hozzáférés-szabályozás
6. Titkosítás
7. Fizikai és környezeti biztonság
8. A működés biztonsága
9. A kommunikáció biztonsága
10. Rendszerek beszerezése, fejlesztése, karbantartása
11. Szállítói kapcsolatok
12. Információbiztonság és incidens menedzsment
13. Üzletmenet-folytonosság
14. Megfelelőség

MagiCom BUDAPEST LONDON

ISO 27001:2013 – „kontroll-leltár”

ISO27001 Fejezet hivatkozás		Leírás	Kontroll összesen
Irányítási rendszer	4	A szervezet környezete	9
	5	Vezetés	17
	6	Tervezés	31
	7	Támogatás	25
	8	Működtetés	8
	9	Teljesítmény értékelés	27
	10	Fejlesztés	13
		Az IBIR kontroll pontok összesen:	130
Megítélés szerinti elemek	A5	Az információbiztonság vezetői irányítása	2
	A6	Az információbiztonság szervezete	7
	A7	Humán-erőforrás biztonsága	6
	A8	Vagyon-menedzsment	10
	A9	Hozzáférés szabályozás	13
	A10	Titkosítás	2
	A11	Fizikai és környezeti biztonság	15
	A12	A működtetés biztonsága	15
	A13	A kommunikáció biztonsága	7
	A14	Rendszer beszerzés, fejlesztés és karbantartás	13
	A15	Szállítói kapcsolatok	5
	A16	Információbiztonsági incidensek kezelése	7
	A17	A működésfolytonosság információbiztonsági aspektusai	4
	A18	Megfelelőség	8
		Az "A" Melléklet kontrolljai összesen:	114
		ISO/IEC 27001:2013 összesen:	244
		2. táblázat 'ISO/IEC 27001:2013' Kontroll összesítés	

MagiCom BUDAPEST LONDON

Tényleg vannak „új” kontrollok az „A”-jelű mellékletben?

1.	A.6.1.5	Információbiztonság a projekt menedzsmentben
2.	A.8.2.3	Vagyonelemek kezelése
3.	A.9.2.2	Felhasználói hozzáférés kiosztása
4.	A.9.2.4	A felhasználók bizalmas hitelesítési információinak kezelése
5.	A.9.3.1	A bizalmas azonosság-kezelési információk használata
6.	A.12.6.2	Szoftver-telepítési korlátozások
7.	A.13.2.1	Információ továbbítási szabályzatok és eljárások
8.	A.13.2.2	Megállapodások az információk továbbítására
9.	A.14.1.2	Nyilvános hálózatokon nyújtott alkalmazás szolgáltatások biztonságának megteremtése
10.	A.14.2.1	A biztonságos fejlesztés szabályzata
11.	A.14.2.5	A biztonságos rendszer-tervezés alapelvei
12.	A.14.2.6	Biztonságos fejlesztési környezet
13.	A.14.2.8	A rendszer biztonsági tesztje
14.	A.15.1.1	A szállítói kapcsolatokra vonatkozó információ-biztonsági szabályzat
15.	A.15.1.3	Információs és kommunikációs technológiai szállítói lánc
16.	A.16.1.4	Értékelés és döntés az információ-biztonsági események felől
17.	A.16.1.5	Válaszadás az információ-biztonsági incidensekre
18.	A.17.1.2	Az információ-biztonság folytonosságának bevezetése
19.	A.17.2.1	Információ-feldolgozó létesítmények rendelkezésre állása

MagiCom
BUDAPEST LONDON

ISO 27001 „A” melléklet változásai számokban kifejezve

	ISO 27001:2005	ISO 27001:2013	Változás
Biztonsági területek	11	14	+3
Kontrollok száma	133	114	-19

Ez egy félrevezető információ, amelyet már számos blogban leközöltek.
-19 az abszolút eltérés számokban – de nem ennyi a változás!

MagiCom BUDAPEST LONDON

Hasznos olvasmányok

- BSI – Mapping guide - Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013
- BSI – Transition guide - Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013

MagiCom BUDAPEST LONDON

Kérdések? – Válaszok!

MagiCom
BUDAPEST LONDON