ISO 27001: 2013

Snježana Grgić

ISO 27001 i ISO 22301 vodeći auditor
Član ISO Working Group 5
Konzultant za ISO 27001

Sigurnost I

Sigurnost i sustavi upravljanja informacijskom sigurnošću;
Norme niza ISO 27000;
ISO 27001 zahtjevi i kako ih tumačiti;
Problematika uvođenja i primjene sustava;
Rizici, alati i tehnike procjene;

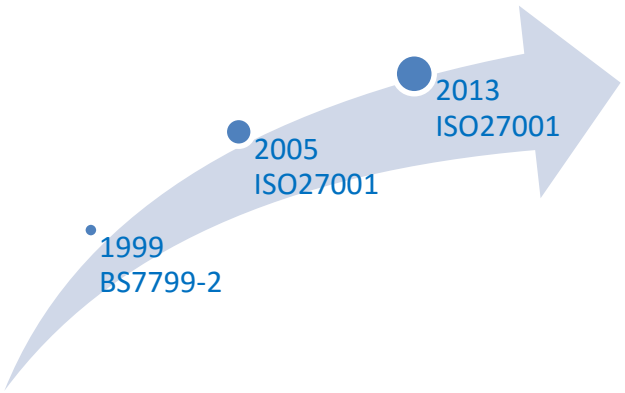
1990 UK vlada

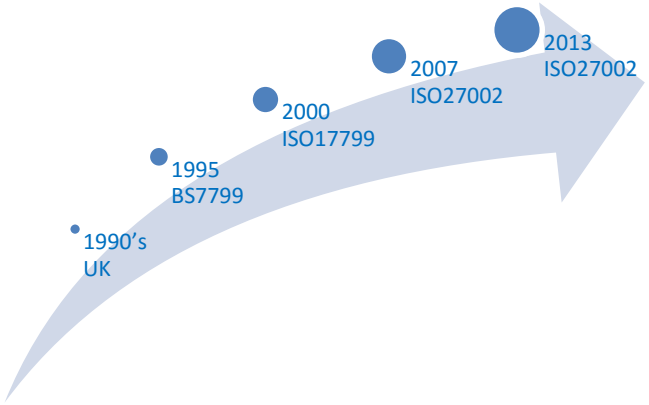
Kriteriji za sigurnosnu evaluaciju
1999 BSI BS7799-2

2005 ISO 27001: 2005
***2013* ISO 27001: 2013**

Dobre prakse sigurnosti
1995 BSI BS7799

2000 ISO 17799
2007 ISO 27002
***2013* ISO 27002**





Sigurnost II

Sigurnost i sustavi upravljanja informacijskom sigurnošću;
Norme niza ISO 27000;
ISO 27001 zahtjevi i kako ih tumačiti;
Problematika uvođenja i primjene sustava;
Rizici, alati i tehnike procjene;

Informacija:
Imovina

Sigurnost informacija :
Očuvanje povjerljivosti, integriteta i dostupnosti informacije

Povjerljivost:
Informacija je dostupna samo osobama kojima je i namijenjena

Cjelovitost:
Točnost i sadržajnost informacije mora biti zaštićena

Dostupnost:
Autorizirani korisnici moraju moći pristupiti informaciji kada im je potrebna

Sustav upravljanja informacijskom sigurnošću

Information Security Management System

- dio cjelokupnog sustava upravljanja u nekoj organizaciji,
- baziran je na upravljanju poslovnim ***rizicima***,
- zadaća mu je da skrbi o ***uspostavi, implementaciji, redovnom upravljanju, nadzoru, pregledavanju, održavanju i poboljšavanju*** informacijske sigurnosti.

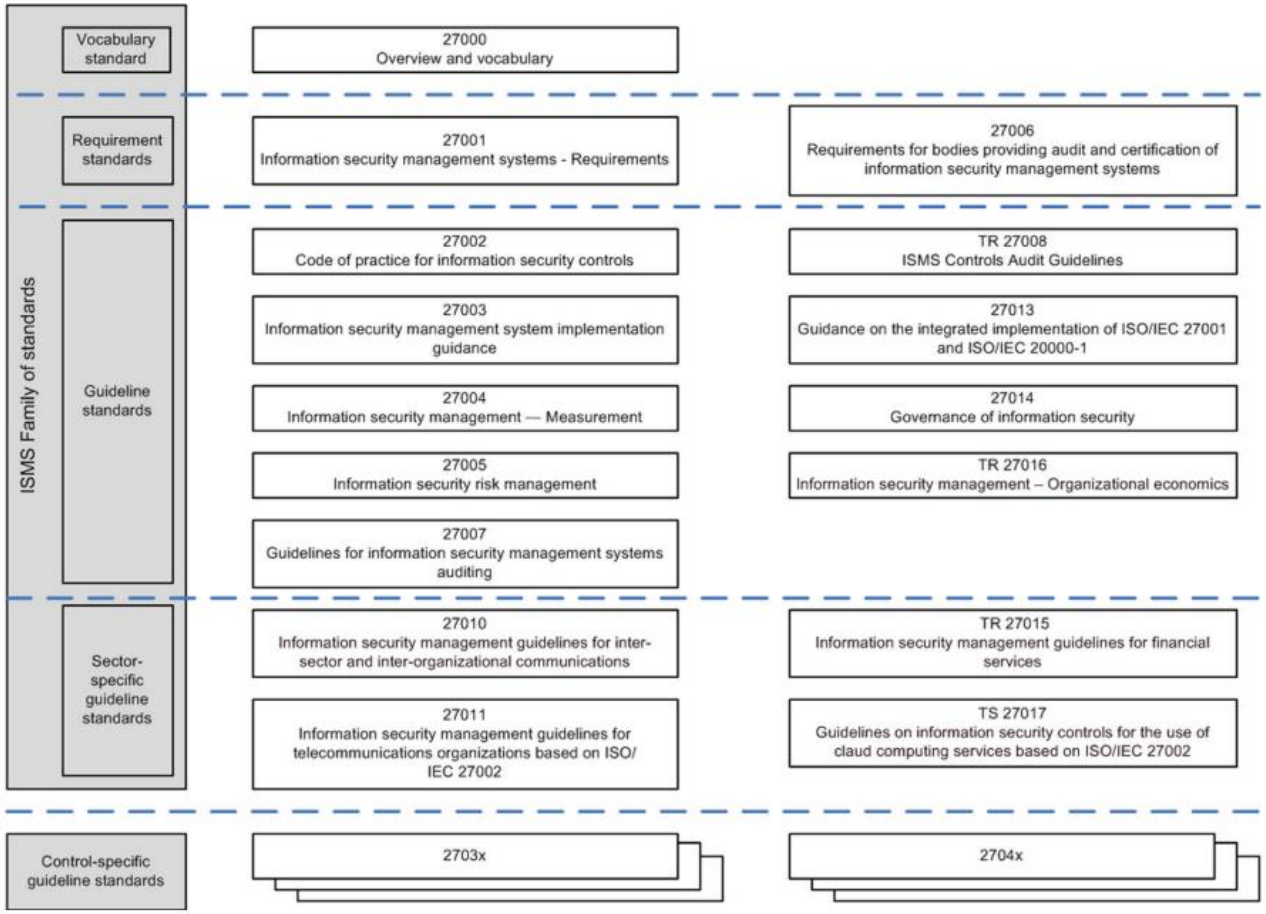
Norme I

— ISO/IEC 27000, Information security management systems — Overview and vocabulary
— ISO/IEC 27001, Information security management systems — Requirements
— ISO/IEC 27002, Code of practice for information security controls
— ISO/IEC 27003, Information security management system implementation guidance
— ISO/IEC 27004, Information security management — Measurement
— ISO/IEC 27005, Information security risk management
— ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems
— ISO/IEC 27007, Guidelines for information security management systems auditing
— ISO/IEC TR 27008, Guidelines for auditors on information security controls
— ISO/IEC 27010, Information security management for inter-sector and inter-organizational communications
— ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
— ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
— ISO/IEC 27014, Governance of information security
— ISO/IEC TR 27015, Information security management guidelines for financial services
— ISO/IEC TR 27016, Information security management — Organizational economics
— ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC 27002

Norme II

Sigurnost i sustavi upravljanja informacijskom sigurnošću;
Norme niza ISO 27000;
ISO 27001 zahtjevi i kako ih tumačiti;
Problematika uvođenja i primjene sustava;
Rizici, alati i tehnike procjene;

ISO/IEC 27000:2014(E)



Zahtjevi I

Organizacija mora ispuniti sljedeće zahtjeve:

4 Kontekst organizacije
4.1 Razumjeti organizaciju i kontekst
4.2 Razumjeti potrebe i očekivanja zainteresiranih strana
4.3 Odrediti opseg ISMS-a
4.4 ISMS

5 Rukovodstvo
5.1 Rukovodstvo i predanost
5.2 Politika
5.3 Uloge, odgovornosti i ovlasti

6 Planiranje
6.1 Akcije za rješavanje rizika i prilika
6.2 Ciljevi IS-a i plan kako ih ostvariti

7 Podrška
7.1 Sredstva
7.2 Kompetencije
7.3 Svijest
7.4 Komunikacija
7.5 Dokumentirana informacija

8. Operacije
8.1 Operativno planiranje i kontrola
8.2 Procjena rizika IS-a
8.3 Tretman rizika IS-a

9. Procjena rada
9.1 Nadzor mjerenje analiza i procjena
9.2 Interni audit
9.3 Pregled od strane rukovodstva

10 Poboljšanja
10.1 Neusklađenosti i korektivne radnje
10.2 Kontinuirana poboljšanja

Zahtjevi II

Za to ima na raspolaganju sljedeće kontrole:

A.5 Sigurnosna politika
A.6 Organizacija i informacijska sigurnost
A.7 Sigurnost ljudskih resursa
A.8 Upravljanje imovinom
A.9 Kontrola pristupa
A.10 Kriptografija
A.11 Fizička sigurnost i sigurnost okruženja
A.12 Operaciona sigurnost
A.13 Sigurnost komunikacija
A.14 nabava, razvoj i održavanje
A.15 Odnosi dobavljača
A.16 Upravljanje incidentima informacijske sigurnosti
A.17 Aspekti informacijske sigurnosti za upravljanje kontinuitetom poslovanja
A.18 Sukladnost

Uvođenje I

Dobrobiti:

- sigurnost i pouzdanost uvedenih rješenja
- povjerenje poslovnih partnera u sigurnost informacijske imovine
- usklađenje sa zakonskom regulativom EU
- konkurentska prednost na tržištu
- osiguranje kontinuirane raspoloživosti usluge
- povećanje svijesti zaposlenika o informacijskoj sigurnosti
- posjedovanje međunarodno priznatog certifikata prema normi ISO 27001

Uvođenje II

- **Uspostava** sustava

analiza stanja, klasifikacija informacija, izrada kataloga imovine i upravljanje rizicima.

- **Implementacija**

izrada plana tretiranja rizika, odabir kontrola, izvedba potrebnih postupaka za uspostavu i mjerenje učinkovitosti sustava, program izobrazbe svih zaposlenika.

- **Postavljanje nadzora**

Omogućuje žurno otkrivanje pogrešaka, sigurnosnih incidenata te redovite provjere i mjerenja učinkovitosti, što uključuje i unutarnje prosudbe kvalitete sustava.

- **Postupak certifikacije**

neovisna prosudba sustava od strane vanjske certifikacijske kuće.

Rizici I

Zahtjevi za procjenom rizika

1. Identificirati metodologiju procjene rizika primjerenu potrebama ISMS-a, informacijske sigurnosti kao i zakonskim zahtjevima i propisima.

2. Razviti kriterij za prihvaćanje rizika i identificirati prihvatljive rizike.

Rizici II

Izbjegavanje – podrazumijeva obustavljanje ili preinaku tekućih aktivnosti ili unaprijed određenih ciljeva koji povećavaju mogućnost nastanka rizika. Rizici se mogu izbjeći izmjenom opsega, dizajna i/ili tehnologije.

Prijenos – Poduzimaju se aktivnosti smanjivanja učinka rizika ili vjerojatnosti njegovog nastanka prenošenjem rizika na treću stranu ili podjela rizika s trećom stranom.

Smanjenje – Najčešći odgovor na rizik. Poduzimaju aktivnosti smanjivanja učinka rizika ili njegovog nastanka, ili oboje.

Prihvaćanje – Ne poduzimaju se nikakve aktivnosti za smanjenje rizika. Uprava daje mišljenje da se razina uočenog rizika može prihvatiti ili donosi zaključak da je cijena ublažavanja rizika veća od potencijalne štete.

ISO seminari:

15. 11. 2016. Informacijska sigurnost u laboratorijima i inspekcijskim tijelima
29. – 30. 11. 2016. Interni auditor po ISO 27001
12. – 16. 12. 2016. Lead implementer po ISO 27001

Hvala na pažnji!

Kontakt podaci:

Snježana Grgić
snjgrgic@gmail.com
info@privatnost.hr
091 2030 008