

Informacijos apsaugos standartai – 27000 serija

Parengė: Marius Celskis

UAB „Informacijos saugos sprendimai“

www.isec.lt

2007 m. balandis 12 d.



ISO 27000 serija

- Tarptautinė standartizacijos organizacija ISO informacijos apsaugos standartizavimui rezervavo seriją 27000.
- Šią standartų grupę sudaro šie, jau išleisti ar rengiami standartai:
 - ISO 27000: Terminai ir apibrėžimai. Numatytas išleisti 2007 metais.
 - ISO 27001: Informacijos apsaugos vadybos sistema – IAVS (buvęs BS 7799-2).
 - ISO 27002: Informacijos apsaugos priemonės (dabartinis ISO 17799). Numatytas išleisti 2007 metais.
 - ISO 27003: Rekomendacijos IAVS įgyvendinimui. Numatytas išleisti 2008 metais.
 - ISO 27004: IAVS efektyvumo vertinimas, numatytas išleisti 2008 metais.
 - ISO 27005: Informacijos apsaugos rizikų valdymo standartas (pakeisiantis BS7799-3), numatytas išleisti 2007 metais.

ISO 27000 – terminai ir apibrėžimai

- Šio standarto tikslas – nustatyti, apibrėžti ir suvienodinti ISO 27000 standartų serijoje naudojamas sąvokas ir terminus. Standartas kol kas nėra paskelbtas. Planuojama, kad standarto sąvokos ir apibrėžimai bus analogiškai naudojamiems šiuose dokumentuose:
 - ISO/IEC Guide 2:1996 “Standardization and related activities – General vocabulary” ir
 - ISO/IEC Guide 73:2002 “Risk management – Vocabulary – Guidelines for use in standards”

ISO 27001:2005 - informacijos apsaugos vadybos sistema IAVS

4 iš 9

- Standarte aprašyta Demingo PDCA (Planavimas-Įgyvendinimas-Matavimas-Gerinimas) ciklu pagrįsta informacijos apsaugos vadybos sistema.
- Standarto tikslas – padėti organizacijoms sukurti ir įgyvendinti IAVS.
- Organizacijoms atitinkančioms ISO 27001 reikalavimus ir praėjusioms sertifikavimo procedūrą, suteikiamas atitiktis šiam standartui sertifikatas (analogiškai ISO 9000 kokybės vadybos sertifikatui)

ISO 27002 - informacijos apsaugos priemonės ^{5 iš 9}

- Šis standartas tai informacijos apsaugos priemonių rinkinys, apimantis organizacines ir technines saugumo priemones. Standarte aprašytos 133 saugumo priemonės suskirstytos į 11 sričių.
- Dabartinis standarto pavadinimas ISO 17799:2005 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas“. Standartą planuojama pervadinti 2007 metais.

ISO 27003 – rekomendacijos IAVS įgyvendinimui

- 2008 metais planuojamas išleisti standartas, kurio tikslas padėti organizacijoms įgyvendinti IAVS (apibrėžtą pirmajame serijos standarte). Standarte numatytos įgyvendinimo rekomendacijos skirtinguose PDCA (Planavimas–Įgyvendinimas–Matavimas–Gerinimas) ciklo etapuose.

ISO 27004 – IAVS efektyvumo vertinimas

- 2008 metais planuojamas išleisti standartas, kurio tikslas padėti organizacijoms išmatuoti ir įvertinti:
 - Informacijos apsaugos valdymo proceso (27001) efektyvumą;
 - Informacijos apsaugos priemonių (27002) efektyvumą.

ISO 27005 - informacijos apsaugos rizikų valdymas ^{8 iš 9}

- Šio standarto tikslas – padėti organizacijoms įgyvendinti rizikų valdymo procesą. Planuojama publikavimo data: 2007-2009 metai. Kaip pagrindas šiam standartui gali būti panaudotas jau paskelbtas standartas BS 7799-3:2006 “Information security management systems - guidelines for information security risk management”.

Trumpai drūtai

- Informacijos apsaugos standartai atsako į šiuos klausimus:
 - ISO 27000: ką reiškia sąvokos šiuose standartuose?
 - ISO 27001: kas yra informacijos apsaugos valdymo sistema?
 - ISO 27002: kokios būna saugumo priemonės?
 - ISO 27003: kaip valdymo sistemą įgyvendinti?
 - ISO 27004: ar pavyko ją įgyvendinti?
 - ISO 27005: kaip valdyti saugumo rizikas?

Klausimai ?

UAB „Informacijos saugos sprendimai“

www.isec.lt

Marius Celskis

Mob. tel.: +370 685 52330

El. paštas: marius@isec.lt