RIIGI INFOSÜSTEEMI AMET

Euroopa Liit
Euroopa struktuuri- ja investeerimisfondid

Eesti
tuleviku heaks

ISKE

Marek Vasar
RIA / riigi infosüsteemi turbe talitus

03.06.2016

Agenda

- Mis on ISKE?
- ISKE protsess
- ISKE vs ISO
- ISKE arendused
- Metoodika ja sisu uuendamine
- Rakendamine ja järelevalve
- Teadlikkuse tõstmine

ISKE?

- ISKE - infosüsteemide kolmeastmeline etalonturbe süsteem ehk **riigi infosüsteemi infoturbe standard**
- Aluseks on Saksamaa BSI infoturbe ameti etalonturbe käsiraamat, mis omakorda baseerub ISO 27000 perekonnal
- Eesmärk tagada avalike ülesannete täitmisel töödeldavatele andmetele ja nendega seotud infovaradele elementaarse tasemega turvalisus
- annab asutusele ülevaate infovarade turvanõrkustest ja võimaluse riske minimeerida

Alused:

- Avaliku teabe seadus
- 20.12.2007 VV määrus nr 252 “Infosüsteemide turvameetmete süsteem” ISKE määrus
- 15.03.2012 VV määrus nr 26 “Infoturbe juhtimise süsteem” infoturbejuht

ISKE 11 sammu

1	Infovarade inventuur
2	Andmekogude kaardistamine, andmekogudele turvaklassi ja turbeastme määramine, turvaklassid RIHAsse märkimine
3	Muude infovarade turvaklassi määramine
4	Kõikide turvaklassiga infovarade vajaliku turbeastme määramine
5	Infovarade tsoneerimine (vajadusel)
6	Tüüpmoodulite spetsifitseerimine
7	Turvameetmete loetelu koostamine
8	Turvameetmete rakendamise plaani koostamine
9	Turvameetmete rakendamine
10	Tegeliku turvaolukorra kontroll
11	Konfiguratsiooni- ja muudatustehalduse sisseviimine

ISKE vs ISO

- Metoodika: detailne riskianalüüs versus etalon

Detailne riskianalüüs: (ISO)

- Kaardista varad ja leia omanik;
- Määra iga vara väärtus (AV);
- Leia igale varale mõjuvad ohud;
- Leia iga ohu kohta kahjustatuse määr (EF) ja arvuta üksiku kahju hinnang (SLE=AV*EF);
- Analüüsi ja leia iga ohu avaldumise tõenäosus aastas (ARO);
- Arvuta aastase kahju hinnang (ALE=SLE*ARO);
- Leia iga vara igale ohule vastumeede ja arvuta ümber ARO ja ALE.
- Leia iga vastumeetme aastane kulu (ACS);
- Teosta kuluefektiivsuse analüüs iga vara iga ohu igale vastumeetmele (ALE1-ALE2-ACS).
- Vali välja kõige efektiivsemad meetmed ja juuruta need.

Etalonmetoodika: (ISKE)

- Kaardista varad ja leia omanik;
- Määra omanikuga koos andmete olulisus ehk turvaklass;
- Selekteeri ISKE kataloogist välja meetmed ja juuruta need.

ISKE Portaal

2015 loodi ISKE Portaal

- Veebipõhine keskkond (wiki)
- Sisu masintöödeldav
- ISKE rakendajatele ISKE kataloogidega töötamiseks
- RIA-le ISKE haldamiseks

Portaal võimaldab

- ISKE ajakohastamisel operatiivset koostööd ISKE rakendajate ja RIA vahel
- Kataloogide sisu vastavalt vajadusele jooksvalt uuendada/ täiendada
- ISKE-t ajakohasemaks muuta

https://iske.ria.ee

ISKE tööriist

Hange – 2016 III kv

Arendustööde kestus 14 kuud + juurutamine

Tööriist võimaldab:

- tõsta ISKE rakendamise efektiivsust infovarade, turvameetmete ja vastutajate haldamisel ning raportite ja väljavõtete genereerimisel.
- Vähendada ISKE haldamisel tehtava käsitöö mahtu ja sellest tingitud vigade tekkimise ohtu.
- Kuvada ISKE rakendatuse kohta terviklikumat ja ajakohast infot.
- Tõsta asutuste infoturbe taset hindavate audiitorite töö efektiivsust ja kvaliteeti.

Turvaline e-kirjavahetus

- Turvalise e-kirjavahetuse eelanalüüs
- Tulem 2016 II kv
  - Eesmärk teha kindlaks optimaalseim lahendus turvalise (krüpteeritud) e-kirjavahetuse tagamiseks Eesti riigiasutustes
  - Tulemi põhjal saab RIA esitada omapoolse ettepaneku konkreetse lahenduse arendamiseks ning riigiasutustes kasutusele võtmiseks

Kataloogide uuendamine

ISKE vs 8.00 plaanitud tähtaeg 2016 II kv

- BSI IT-Grundschutz uuenduste tõlkimine ca 900 lk
- Tõlke tulemi valideerimine
- Kokku 318 uut/muutunud artiklit
  - 20 moodulit
  - 174 meedet
  - 124 ohtu
- Pilve moodulid, meetmed ja ohud

ISKE uuendamine

- Loodud turvajuhtide komisjon
- ISKE töörühm:
  - ISKE metoodika ajakohastamine ja täpsustamine
  - ISKE kataloogide ajakohasuse ja efektiivsuse hindamine ja tõstmine
- BSI IT Grundschutzi plaanitavad uuendused
  - Sisu kiirem tarnimine
  - Parem struktuur
  - Skaleeritavus vastavalt asutuse vajadustele
  - Rohkem rõhutakse riskijuhtimise ja riskianalüüsi protsessidele
  - Arvestatakse rohkem kasutajaspetsiifilisi (valdkonnaspetsiifilisi) vajadusi ja luuakse vastavad profiilid
  - Standardi alaline ühilduvus ISO nõuetega
  - Küsimustikud mis aitavad rakendajal otsustada meetmete sobivust
  - Samuti on lubatud sisu mahtu oluliselt vähendada

ISKE riigiasutustes

Riigiasutused peavad rakendama ISKEt ja tellima korralisi auditeid

ISKE rakendamise kohta viimane ülevaade aastast 2015

- Vaadati läbi auditite raportid
- Hinnati raportites toodud järeldusi
- Puuduste esinemisel viidi läbi järeltoiminguid

ISKE KOV-des

KOV-del ISKE rakendamise kohustus, auditeerimise kohustust ei ole

- 2012 kuni 2014 viidi KOV-des läbi infoturbe taseme hindamised
- 2016 plaanis pisteliselt KOV-des tegeleda infoturbe teadlikkuse hindamise ja tõstmisega

RIA järelevalve

JV tegevused

- regulaarne auditi raportite läbivaatus ja puudustele tähelepanu juhtimine
- infoturbe taseme hindamised
- asutuste nõustamine infoturbe tõhustamise osas
- vajadusel JV menetluste läbiviimine

Koolitused

- Koolitused 2016
  - ISKE rakendamise koolitus (ISKE rakendajatele)

    2016.10.13

    2016.12.01

  - Turvateadlikkuse tõstmise koolitus (mitte IT inimestele)

    Ajakava täpsustub sügisel

Tänan!

iske@ria.ee