



ISKE on infosüsteemide kolmeastmeline etalonturbe süsteem. ISKE väljatöötamisel ja arendamisel on aluseks võetud Saksamaa BSI poolt avaldatav infoturbe standard - IT Baseline Protection Manual (saksa k. IT-Grundschutz),, mida on kohandatud vastavalt Eesti oludele. ISKE on üheks riigi infosüsteemi kindlustavaks süsteemiks.

ISKEs on kirjeldatud kolm turbe taset – madal (L), keskmine (M) ja kõrge (H). Vastav turbetase määratakse andmetele turvaklasside (turvaosaklasside) määramise kaudu. Turvaklasside määramisel lähtutakse teabe konfidentsiaalsusest, teabe terviklusest, teabe käideldavusest.

ISKE rakendamise eesmärgiks on tagada infosüsteemides töödeldavatele andmetele piisava tasemega turvalisus. ISKE on kohustuslik riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavatele infosüsteemidele ning nendega seotud infovaradele turvalisuse tagamiseks. ISKE rakendamist reguleerib Vabariigi Valitsuse 20. detsembri 2007. a määrus nr 252 „Infosüsteemide turvameetmete süsteem“. Tulenevalt eelpool mainitud määrusest peab ISKE olema rakendatud andmekogudele hiljemalt 1. jaanuariks 2008. Nendele andmekogudele, mis loeti andmekogudeks alates uue avaliku teabe seaduse jõustumisest, on kohustus rakendada ISKE't hiljemalt 1. juuliks 2008.

Selle aasta sees muudetakse „Infosüsteemide turvameetmete süsteemi“ määrust. Määruse muutmiselega kehtestatakse **ISKE rakendamise auditeerimise tingimused**. Määruse muudatus näeb ette „H“ (kõrge) turbeastmesse kuuluvate andmekogude auditeerimise läbi viimist hiljemalt 2010. aasta 1. märtsiks. „M“ ja „L“ turbeastmesse kuuluvate andmekogude puhul on auditeerimise tähtajad vastavalt 2010. aasta 1. detsember ja 2011. aasta 1. märts.

ISKE rakendamise aruandlus toimub riigi infosüsteemi haldussüsteemis (RIHA). RIHA'sse raporteeritakse:

1. andmekogule määratud turvaosaklassid ja nendest tulenev turbeaste;
2. andmekogu- ja sellega seotud infovarade turvameetmete loetelu rakendatuse protsent;
3. pärast auditi läbiviimist audiitori järeldusotsus.

ISKE'ga seotud materjalid: rakendusjuhend, pilootprojektid, koolituse materjalid, korduma kippuvad küsimused jpm on leitavad Riigi Infosüsteemide Arenduskeskuse kodulehelt (<http://www.ria.ee/iske/>)

ISKE rakendamist alustavatele asutustele on soovitatav esmalt oma asutuse siseselt leida inimene(ed), kes hakkab ISKE rakendamist korraldama. Kindlasti ei tohiks pidada ISKE rakendamist ainult IT-inimeste pärusmaaks – ISKE seab turvanõudeid ka organisatoorsele jt mitte IT-ga seotud valdkondadele. **Väga oluline on asutuse juhtkonna toetus ISKE rakendamisel**, ilma nende toetuseta võib ISKE rakendamine osutuda väga raskeks kui mitte võimatuks. Järgmise sammuna tuleks tutvuda ISKE't puudutava dokumentatsiooniga – heaks alguseks oleks ISKE rakendusjuhendi lk 1-22 mõttega läbitöötamine (ülejäanud ~430lk ei ole esmase ülevaate saamise jaoks olulised). Edasi tuleks tutvuda ISKE korduma kippuvate küsimuste ja teiste RIA kodulehel leitavate materjalidega. Kõikide küsimuste ja probleemide korral saab abi meiliaadressilt iske@ria.ee. Lisaks kodulehel leiduvatele materjalidele on RIA koostöös ATAK'iga töötanud välja ISKE praktilise rakendamise koolituse (lisainfo www.atak.ee).

Vaja on julget ja sihikindlat pealehakkamist!