

Infosüsteemi audit

Jaak Tepandi, CISA
TTÜ, Tepinfo, EVS TK4, EISAÜ, ISACA

Üks võimalik lahendus vastutusrikaste rakenduste hindamiseks on, et süsteemi omadustest huvituv osapool kutsub olukorrast ülevaate saamiseks tööle kolmanda isiku - audiitori. Infosüsteemid pole selles suhtes erand, analoogiline on olukord näiteks raamatupidamises, keskkonnakaitses ja mujal.

Audit, selle objekt ja läbiviijad

Infosüsteemi audit on mitmekülgne ülevaade ja hinnang auditeeritava ettevõtte, asutuse või organisatsiooni automatiseeritud infosüsteemile või selle osadele, kaasa arvatud seostele automatiseerimata protsessidega ja organisatsioonilise struktuuriga.

Toome näiteid küsimustest, millele auditi käigus püütakse vastust leida. Asutusel on probleem infolekkega. Kas saab selgitada põhjuseid ja hoida ära sellised juhtumid tulevikus? Juhtkonnale tundub, et infotehnoloogia ressursse ei kasutata hästi. Mida teha? Oluline projekt venib. Mida ette võtta?

Näiteid auditi eesmärkide kohta:

- hinnata süsteemide ja infotöö vastavust ettevõtte (äri)huvidele
- hinnata ettevõttega seotud kolmandate osapoolte (näiteks avalikkuse) nõuete rahuldatust
- hinnata firma tegevusele eluliselt vajaliku info usaldatavust, kättesaadavust ja kaitstust
- hinnata süsteemide või infotöö korralduse kvaliteeti, turvet ja töökindlust
- kaitsta tellija huve, kui tellitavas projektis on põhiline teadmine täitja poolel
- kontrollida venivaid või muus mõttes ebaedukaid projekte
- pakkuda tuge uute projektide käivitamisel

Auditeeritakse kõiki infosüsteemidega seotud objekte, tegevusi, protsesse ja valdkondi, sealhulgas planeerimist, organisatsiooni, dokumentatsiooni, hanget, projekti, projekti juhtimist, arendust, meetodikaid, kasutamist, hooldust, mõõtmist, aruandlust, jälgimist (sisemist kvaliteedijuhtimist).

Infosüsteemi audiitor on isik, kes soovitatavalt, omades kehtivat infosüsteemi audiitori sertifikaati, auditeerib auditi eesmärgist lähtudes auditeeritava organisatsiooni infosüsteemi vastavalt infosüsteemide audiitorkontrolli eeskirjadele ja järgib infosüsteemi audiitori eetikanormistikku.

Audiitorile esitatakse mitmesuguseid nõudmisi. Ta peaks olema sõltumatu auditeeritavast rakendusest, olema ekspert infosüsteemide auditeerimises ja infotehnoloogia vastavas valdkonnas, jälgima auditeerimise head tava ja reegleid, olema tuttav Eesti seadusandlusega ja standarditega ning tundma mõnda tunnustatud auditeerimise meetodikat.

Eetikareeglid ütlevad muuhulgas, et audiitor peab

- toetama infosüsteemide eeskirjade, protseduuride ja kontrollide väljatöötamist ning nende järgimist
- tegutsema hoolikalt, lojaalselt ja ausal viisil oma tööandja, ettevõtte omanike, klientide ja avalikkuse huvides ning teadlikult mitte osa võtma mis tahes seadusevastasest või ebasüüdsast tegevusest
- säilitama oma kohustuste täitmise käigus saadud informatsiooni konfidentsiaalsust. Informatsiooni ei tohi kasutada isikliku kasusaamise huvides ega avaldada asjasse mittepuutuvatele osapooltele
- täitma oma kohustusi sõltumatult ja objektiivsel viisil ning hoiduma tegevustest, mis ohustaksid või võiksid ohustada tema sõltumatust
- säilitama asjatundlikkust auditi ja infosüsteemide alal, arendades oma ametialaseid oskusi ning võttes osa koolitusest
- hoolikalt koguma ja dokumenteerima piisavat faktilist materjali, millel põhjal teha järeldusi ja soovitusi
- informeerima asjassepuutuvaid osapooli sooritatud auditist
- toetama juhtkonna, klientide ja avalikkuse koolitamist, et laiendada nende arusaamist auditist ja infosüsteemidest

Auditi korraldus

Auditi läbiviimine sisaldab selliseid samme nagu eelläbirääkimised, auditeerimislepingu sõlmimine, auditi planeerimine, olukorra identifitseerimine ja dokumenteerimine, näiteks kehtestatud infosüsteemi kasutamise ja arendamise poliitika; protseduurireeglid; vastavus seadusandlusele, organisatsiooni äriplaanile, rahvusvahelistele *de jure* ja *de facto* standarditele, tehnoloogilistele nõuetele ja standarditele; hindamine, nt riskide hinnang, vastavustestimine, reeglite tegeliku täitmise ulatuse hindamine, vajadusel sisuline testimine, hinnang ja raportid.

Kuna audit ei kontrolli kõike, siis jääb nagu teistegi auditi tüüpide puhul risk, et auditi käigus ei avastata ka suhteliselt olulisi vigu. Seda riski tuleb teadvustada lepingu läbirääkimistel ja sellele tuleb viidata ka auditi lepingus. Auditiga on seotud ka korralduse ja ootuste riskid. Näiteks kui vead olid enne teada ja nende parandamiseks pole soovi või ressursse, võib auditi kasu olla piiratud. Audit pole ka arendus ega jooksev vigade parandus.

Auditi planeerimise käigus määratletakse kriitilised valdkonnad, pühendatakse neile piisavalt tähelepanu ja varutakse ressursse. Lepitakse kokku töö õige järjekord ja koordineerimine, tõendusmaterjalid, kontrolli meetoodika, raportid, tähtajad ja töö maht.

IS auditi organisatsioonid maailmas ja Eestis

Maailmas ühendab infosüsteemide audiitoreid eelkõige Infosüsteemide Auditi ja Kontrolli Assotsiatsioon (*Information Systems Audit and Control Association*, ISACA, vt <http://www.isaca.org>). Assotsiatsioonil on 18 000 liiget sajades riigis. Ta sertifitseerib infosüsteemide audiitoreid, avaldab auditaalast kirjandust, töötab välja auditi meetodikaid, korraldab koolitust, algatab uurimis- ja arendustöid, avaldab ajakirja *IS Audit & Control Journal* ning korraldab viiel mandril rahvusvahelisi konverentse.

ISACA poolt välja antud info- ja sellega seotud tehnoloogia kontrolli sihid (COBIT) annavad auditi korralduse üldise meetoodika. COBIT eristab nelja põhilist ala: planeerimine ja organisatsioon, hange ja rakendus, ülekanne ja tugi, jälgimine. Nendel

aladel on määratletud infotehnoloogia protsessi ja kontrolli üldised sihid. Iga sihi jaoks on määratud detailsed auditi alad, meetodid, kontrollide hindamine, vastavuse hindamine, riskide hindamine.

Üks ISACA olulisemaid tööloike on audiitorite sertifitseerimine. Sertifitseeritud infosüsteemide audiitor (CISA) peab sooritama vastava eksami, tõendama pidevat koolitust, jälgima audiitori eetikanorme ja standardeid, omama töökogemust.

CISA koolitust ja eksamit arendavad ISACA ja selle tütarorganisatsioonid. Eksam korraldatakse igal aastal ühel kindlal päeval. Eksamil testitakse kandidaadi kogemusi infotehnoloogia auditi, kontrolli ja turbe alal, samuti tema oskusi rakendada erialaseid standardeid ja teadmisi. Selleks tuleb nelja tunni jooksul vastata kaheksajale küsimusele. Eksami valdkondadel on järgmine osakaal:

- audit ja infosüsteemide (IS) turve 8%
- IS organisatsioon (sh strateegia, korraldus) ja juhtimine 15%
- IS protsess (sealhulgas infotehnoloogia) 22%
- IS terviklus, konfidentsiaalsus, käideldavus 29%
- IS arendus, hange, hooldus 26%

ISACA on praeguseks välja andnud umbes 100 IS auditi alast raamatut. Raamatute hulgas on kogu auditi ala katvad monograafiad, eriküsimusi käsitlevad raamatud, näiteks UNIX-, EDI-, COBIT-teemalised väljaanded, sissejuhatavad tekstid, CISA eksami materjalid, videod.

Eestis on olemas Eesti infosüsteemide audiitориühing (EISAÜ), kuhu kuuluvad alast huvitatud isikud. Ühingu tegevusvaldkonnad on koolitus, avalikkuse informeerimine, koostöö teiste organisatsioonidega (ISACA), auditi standardite ülevõtmine või koostamine, infosüsteemide audiitorkontrolli eeskirjade koostamine ja arendamine.