RIIGI INFOSÜSTEEMI AMET

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

Riskianalüüsi ja riskide hindamise juhendmaterjal ETOdele

11. detsember 2015

Mõisted

Elutähtis teenus	teenus, mis on hädavajalik eluliselt tähtsate ühiskondlike toimingute, tervishoiu, turvalisuse, julgeoleku ning inimeste majandusliku ja sotsiaalse heaolu korraldamiseks.
Elutähtsa teenuse osutamise kriitiline tegevus	tegevus, mille katkestus ohustab tõsiselt asutuse või ettevõtte võimekust osutada elutähtsat teenust ning takistab asutuse või ettevõtte sõnastatud eesmärkide saavutamist teenuse osutamisel
Infosüsteem	andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talitluseks vajalike vahendite, ressursside ja protsessidega
Infosüsteemi riskianalüüs	analüüs, mille käigus tuleb kriitilise infosüsteemi kohta selgitada välja võimalikud ohud ja nõrkused, hinnata ohtude realiseerumise tõenäosust ja nendega kaasnevaid kahjusid ning valida sobivad turvameetmed ohtude realiseerumise mõju vähendamiseks
Infovara	informatsioon, andmed ja nende töötlemiseks vajalikud infotehnoloogilised rakendused ning tehnilised vahendid
Konfidentsiaalsus	infovara kättesaadavus ainult selleks volitatud tarbijaile (isikutele või tehnilistele süsteemidele) ning kättesaamatus kõigile ülejäänutele
Katkestus	negatiivne kõrvalekalle teenuse eesmärgi- ning plaanipärasel osutamisel, mis on põhjustatud kas prognoositavast (nt streik) või ootamatust (elektrikatkestus, torm) sündmusest
Käideldavus	eelnevalt kokkulepitud vajalikul/nõutaval tööajal kasutamiskõlblike infovarade õigeaegne ja hõlbus kättesaadavus (st vajalikul/nõutaval ajahetkel ja vajaliku/nõutava aja jooksul) selleks volitatud tarbijaile (isikutele või tehnilistele vahenditele)
MTD	maksimaalne katkestuse lubatud kestvus; kriitilise tegevuse katkemise periood, mille möödumisel pole juriidiline isik või asutus võimeline osutama elutähtsat teenust seadustes või nende alusel kehtestatud õigusaktides või lepingutes sätestatud tingimustel
RTO	taaste sihtaeg; elutähtsa teenuse osutaja poolt määratud maksimaalne aeg kriitilise tegevuse jätkamiseks ja taastamiseks; ajaline eesmärk taasteplaanide koostamiseks
Nõrkus	infovara haavatav koht, mille kaudu saab realiseeruda üks või mitu ohtu (EVS ISO/IEC 27005:2014)
Oht	sündmus või asjaolu, mis võib põhjustada katkestust või kahjustada

	infovara muul viisil
Risk	määramatust arvestav hinnang asjaoludele, mis võivad takistada asutuse või ettevõtte võimekust osutada elutähtsat teenust tähtajaliselt, ettenähtud kvaliteediga või planeeritud mahus. Infoturvariski väljendatakse sageli infoturvasündmuse tagajärgede ja selle sündmuse võimalikkuse kombinatsioonina
Terviklus	infovara õigsuse/täielikkuse/ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine
ETO	elutähtsa teenuse osutaja
RIA	Riigi Infosüsteemi Amet
ISKE	infosüsteemide kolmeastmeline etalonturbe süsteem
BIA	toime kaalutlemine; riskianalüüsi protsess, millega vaadatakse läbi elutähtsaid äriprotsesse toetavaid IT-süsteeme mõjutavate infoturvaintsidentide võimalik toime äritegevusele, et selgitada välja nendega seotud käideldavusnõuded
RPO	taaste sihtseis; üks intsidendijärgsele taastele seatud eesmärke: andmete taaste kestusena või säilinud andmete vanusena väljendatav lubatav andmete kadu; määrab varukopeerimise minimaalse lubatava sageduse; aeg, millele eelnevad andmed peavad olema täielikult taastatud (näiteks eelmine tund, eelmine tööpäev, eelmine nädal)

Sisukord

1 Miks IT riskianalüüsi tuleb teha?

1.1 Seadusandlusest tulenevad nõuded

Hädaolukorra seadus (vastu võetud 15.06.2009) §37 lõige 3 sätestab elutähtsa teenuse osutaja (edaspidi ka ETO) kohustused elutähtsa teenuse toimepidevuse tagamisel.

Elutähtsa teenuse osutaja on kohustatud:

1) koostama tema poolt osutatava elutähtsa teenuse toimepidevuse riskianalüüsi (edaspidi toimepidevuse riskianalüüs);

2) koostama tema poolt osutatava elutähtsa teenuse toimepidevuse tagamise plaani (edaspidi toimepidevuse plaan);

3) teavitama viivitamata elutähtsat teenust korraldavat asutust või tema määratud asutust elutähtsa teenuse toimepidevust oluliselt häirivast sündmusest või sellise sündmuse toimumise vahetust ohust;

4) andma elutähtsat teenust korraldavale asutusele või asutusele, kelle ta on määranud elutähtsa teenuse toimepidevuse üle järelevalvet teostama, tema nõudmisel teavet elutähtsa teenuse osutamise kohta;

5) täitma muid õigusaktidega talle elutähtsa teenuse toimepidevuse tagamiseks pandud kohustusi.

Hädaolukorra seaduse §38 selgitab toimepidevuse riskianalüüsi teostamise toiminguid.

Toimepidevuse riskianalüüs on dokument, milles kirjeldatakse:

1) elutähtsa teenuse osutamise osalist või täielikku katkestust põhjustavaid ohtusid;

2) elutähtsa teenuse osutamise osalise või täieliku katkestuse tõenäosust;

3) elutähtsa teenuse osutamise osalise või täieliku katkestuse võimalikke tagajärgi;

4) muud olulist teavet.

(2) Toimepidevuse riskianalüüsi kinnitab elutähtsat teenust osutava asutuse juht või juriidilise isiku puhul juhatus või seda asendav organ.

(3) Riskianalüüsi koostanud asutus või isik esitab riskianalüüsi elutähtsat teenust korraldavale asutusele või elutähtsat teenust korraldava asutuse määratud allasutusele. Elutähtsat teenust korraldav asutus hoiab saladuses temale edastatud teavet, mida edastades on isik teatanud, et tegemist on ärisaladusega.

(4) Toimepidevuse riskianalüüsi koostanud asutus või isik hindab vähemalt üks kord kahe aasta jooksul riskianalüüsi ajakohasust ning teeb vajaduse korral muudatused. Muudatuste tegemisel järgitakse käesoleva paragrahvi lõigetes 2 ja 3 sätestatut.

(5) Toimepidevuse riskianalüüsi koostamise juhendi kehtestab valdkonna eest vastutav minister määrusega.

Hädaolukorra seaduse § 40 sätestab kohustuse tagada elutähtsa teenuse osutamise elektrooniline turvalisus.

(1) Elutähtsa teenuse osutaja on kohustatud tagama elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise.

(1'1) Kui elutähtsa teenuse toimimist tagavad infosüsteemid asuvad välisriigis, peab elutähtsa teenuse osutaja tagama elutähtsa teenuse toimepidevuse ka viisil ja vahenditega, mis ei ole sõltuvuses välisriikides paiknevatest infosüsteemidest.[RT I, 30.10.2012, 1 - jõust. 01.01.2014]

(2) Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed kehtestab Vabariigi Valitsus määrusega.

Hädaolukorra seaduse §40 lõike 2 alusel kehtestatud määrus „Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed" (vastu võetud 14.03.2013) reguleerib elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ja nendega seotud infovarade turvameetmete rakendamise korraldust.

Määruse § 3. Kriitilise tegevuse sõltuvus infosüsteemist.

(1) Elutähtsa teenuse osutaja koostab hädaolukorra seaduse § 37 lõike 3 punkti 1 alusel toimepidevuse riskianalüüsi. Toimepidevuse riskianalüüsist selgub, kas ja millisel määral mõjutavad infosüsteemid kriitilise tegevuse toimepidevust.

(2) Kui kriitilise tegevuse sõltuvus infosüsteemist on oluline, on elutähtsa teenuse osutaja kohustatud rakendama turvameetmed vastavalt §-le 4.

(3) Kui kriitiline tegevus sõltub infosüsteemist, kuid on olemas alternatiivne lahendus kriitilise tegevuse toimepidevuse tagamiseks, peab elutähtsa teenuse osutaja kirjeldama asendusmeetmed hädaolukorra seaduse § 39 lõikes 1 nimetatud toimepidevuse plaanis.

(4) Kui kriitilise tegevuse sõltuvus infosüsteemist ei ole oluline, peab elutähtsa teenuse osutaja rakendama sellele infosüsteemile turvameetmed tasemel, mis tagab teenuse toimepidevuse.

Määruse § 4. Turvameetmete rakendamine infoturbe halduse süsteemi alusel.

(1) Elutähtsa teenuse osutaja loob oma põhitegevusi ja riske arvestades infoturbe halduse süsteemi, mida ta rakendab, seirab ja vajaduse korral täiustab.

(2) Elutähtsa teenuse osutaja järgib infoturbe halduse süsteemi rakendamisel soovitatavalt:

1) EVS-ISO/IEC 27001:2006 standardit;

2) Vabariigi Valitsuse 20. detsembri 2007. a määrusega nr 252 „Infosüsteemide turvameetmete süsteem" kehtestatud infosüsteemide kolmeastmelise etalonturbe süsteemi ISKE või

3) oma tegevusvaldkonnas kehtestatud infoturbe halduse erinõudeid ja head tava, mis tulenevad õigusaktist, välislepingust või muust lepingust ja on samaväärsed punktides 1 ja 2 nimetatud standarditega.

(3) Elutähtsa teenuse osutaja teeb infosüsteemi riskianalüüsi ja valib selle alusel infosüsteemi kaitseks vajalikud turvameetmed eesmärgiga tagada elutähtsat teenust korraldava asutuse kehtestatud teenuse toimepidevuse nõuete täitmine.

(4) Elutähtsa teenuse osutaja dokumenteerib turvameetmete rakendamise.

(5) Elutähtsa teenuse osutaja peab turvameetmete rakendamisel tagama:

1) ligipääsu kriitilisele infosüsteemile vaid selleks õigustatud isikutele;

2) õigustatud isikute turvalise tuvastamise;

3) kontrolljälje olemasolu, mis võimaldab tagantjärele kindlaks teha katkestuse toimumise aja ja muud kontrolli või uurimise teostamiseks tähtsust omavad asjaolud;

4) olulise mõjuga turvaintsidendi raporti olemasolu, mis sisaldab muu hulgas teenuse taastamise käiku pärast katkestust ja meetmeid katkestuste edasiseks vältimiseks;

5) elutähtsa teenuse osutamiseks vajalike andmete koopia säilitamise elektromagnetilise kiirguse eest kaitstud ruumides;

6) elutähtsa teenuse osutamiseks vajalike andmete varundusmeedia säilitamise asukohtades, mis on üksteisest piisaval kaugusel, arvestades võimalikke ohtusid ja nendest tulenevaid riske.

(6) Elutähtsa teenuse osutaja määrab isiku, kes vastutab turvameetmete rakendamise eest ning teavitab regulaarselt juhtkonda toimunud turvaintsidentidest ja toimepidevuse häiretest.

Hädaolukorra seaduse alusel kehtestatud määrus "Toimepidevuse riskianalüüsi koostamise juhend" (vastu võetud 08.06.2010) reguleerib elutähtsa teenuse toimepidevuse riskianalüüsi korraldust.

§7. lõigete 3 ja 4 kohaselt kuuluvad kriitiliste tegevuste toimimiseks vajalike ressurside hulka ka infotehnilised süsteemid ning elutähtsa teenuse osutamiseks vajalik informatsioon.

Infotehnoloogiliste süsteemide määratlemisel tuleb lähtuda määruse lisast 5.

Siseministri 8. juuni 2010. a määruse nr 16
«Toimepidevuse riskianalüüsi koostamise juhend»
lisa 5

Kriitilise tegevuse toimepidevust mõjutavad infotehnoloogilised süsteemid

Infosüsteem või IT teenuse nimetus	Infosüsteemiga seotud kriitilise tegevuse number või numbrid (numbrid tulenevad eelmisest tabelist lisas 4)	Infosüsteemi või IT teenuse kirjeldus	Teenuse pakkuja ja asukoht (asutuse/ettevõtte sisene ja väline)	Katkestuse maksimaalne lubatud kestus	Nõutav taasteaeg	Kriitilise tegevuse sõltuvus infosüsteemist või IT teenusest skaalal: 1 – sõltuvus ei ole eriti oluline; 2 – sõltuvus on oluline, aga on olemas alternatiivne lahendus 3 – kriitiline sõltuvus

Joonis 1. Toimepidevuse riskianalüüsi koostamise juhendi lisa 5.

Kuidas täpsemalt peavad ETOd infotehnoloogisi süsteeme määratlema ja infosüsteemide riskianalüüsi koostama, toodud määrused ei kirjelda.

1.2 Äritegevusest tulenevad nõuded

IT riskianalüüs on üks osa elutähtsa teenuse osutaja infoturvariski halduse protsessist ja veel laiemalt võttes organisatsiooni riskijuhtimise süsteemist. Riskijuhtimise eesmärk on tagada organisatsiooni äriliste eesmärkide saavutamine ja jätkusuutlikus lühemas ja pikemas perspektiivis.

IT riskianalüüs on oluline osa elutähtsa teenuse osutaja infoturbe halduse süsteemist. Infoturbe halduse süsteemi, infoturbepoliitikate ja protseduuride kehtestamise eest vastutab organisatsiooni juhtkond. Juhtkond peab ilmutama eestvedu ja kohustumust sellega, et tagab infoturbe halduse süsteemile vajalike ressursside olemasolu ja edendab selle pidevat täiustamist. ETO peab määrama isiku, kes vastutab turvameetmete rakendamise eest ning tagama talle ülesande täitmise jaoks vajalikud ressursid.

Infoturvariski haldus on süstemaatiline lähenemine infoturvariskide tuvastamiseks, analüüsimiseks, kaalutlemiseks, aruandluseks, käsitlemiseks ja seireks organisatsioonis kehtestatud poliitikate, protseduuride ja tegevuste abil.

Infoturvariski haldus peab olema kooskõlas ETO eesmärkidega ja arvestama ETO tegevustest tulenevate turvanõuetega.

Infoturvariskide haldus saab toimida, kui sellele lähenetakse organisatsiooni vajadustest lähtuvalt. Ei ole võimalik efektiivselt riske maandada, kui me ei tea juhtkonna ootusi, seadusandlusest tulenevaid nõudeid ning ei oma ülevaadet organisatsiooni infovaradest.

Riskide halduse juurutamisel puudub mõte, kui meil ei ole seatud selget eesmärki, milleks seda tehakse. Samuti ei ole piisav, kui me kaardistame riskid ja teeme vastavad aruanded, kuid ei võta ette praktilisi samme nende riskide maandamiseks. ETO peab tagama, et juhtkond oleks pidevalt informeeritud toimunud turvaintsidentidest ja teenusekatkestustest kui ka kaalukamatest riskidest, mis võivad nimetatud olukorrad tekitada.

RIA poolt väljaantud **ISKE kataloogid ver7** käsitleb antud teemat meetmete plokis M6:Hädaolukorraks valmisolek. Eelduseks sellele on hädaolukorraks valmisoleku kontseptsiooni koostamine (ISKE meede 6.114). Hädaolukorraks valmisoleku kontseptsiooni koostamise algatamise eest vastutab asutuse/ettevõtte juhatus ja elluviimise eest hädaolukorraks valmisoleku eest vastutav töötaja.

Hädaolukorraks valmisoleku kontseptsiooni eesmärk on äriprotsesside stabiilsuse tugevdamine, et vähendada kahjustava sündmuse tõenäosust ning asutuse või ettevõtte ettevalmistamine hädaolukorra või kriisiga toimetulekuks, et viia kahjustuste mõju miinimumini.

Hädaolukorraks valmisoleku kontseptsiooni koostamise **eelduseks on põhjalikud teadmised asutuse või hädaolukorra haldamiseks määratud kehtivusala kohta ning äritegevuse põhjalik tundmine**. Hädaolukorra halduseks peavad olema kättesaadavad asutuse või ettevõtte põhiandmeid ning ülevaade äriprotsessidest. Ülevaade äriprotsessidest peaks sisaldama ka teavet protsessidevaheliste seoste kohta, samuti infot selle kohta, millised äriprotsessid on vajalikud põhitoodete tootmiseks või põhiteenuste osutamiseks. Äriprotsessi ülevaatesse tuleb kaasata ka väljasaalitud protsessid, sõltuvussuhete korral ka tarnijad, koostööpartnerid ja välised teenusetarnijad.

Üheks esimeseks sammuks kontseptsiooni koostamisel on ärimõjude analüüsi läbiviimine. BIA läbiviimist koordineerib hädaolukorra lahendamise eest vastutav töötaja. BIA tulemused peavad olema kirjalikult dokumenteeritud ning ettevõtte või asutuse juhtkonna poolt kinnitatud.

Ärimõjude analüüsi läbiviimine on IT riskide analüüsi eelduseks. Ärimõjude analüüsi läbiviimisel osalevad äriprotsesside toimumise ja ressursside eest vastutavad töötajad ja infovarade omanikud.

Ärimõjude analüüs (BIA) uurib äriprotsesside katkemise mõju, äriprotsessidele esitatavaid käideldavuse nõudeid ja selleks vajalikke ressursse ning taaskäivitamiseks vajaminevat aega. Asutusele

tuleb välja valida sobiv meetod BIA läbiviimiseks, määrata kindlaks valitud meetodi parameetrid ja otsused dokumenteerida. BIA käigus viiakse läbi analüüs ja antakse hinnang, millist mõju avaldab asutusele või ettevõttele äriprotsesside või väärtusahela katkemine ning millised kahjulikud tagajärjed sellega kaasnevad.

Äriprotsesside taaskäivitamiseks tuleb identifitseerida ja kindlaks määrata vähemalt järgmised normväärtused:

- **Maksimaalne katkestuse lubatud kestvus** (MTD- maximum tolerable downtime) – kui katkestus venib pikemaks kui MTD, suureneb organisatsioonile tekkiv kahju oluliselt. Elutähtsa teenuse osutaja puhul tähendab MTD ajalist piiri, mille ületamine tähendab oluliste teenusetarne lepete rikkumist. See võib põhjustada sanktsioone ja/või riikliku või kohaliku tähtsusega eriolukorra kehtestamist.

- **Nõutav taasteaeg** (RTO – recovery time objective) – nõutav maksimaalne taasteaeg konkreetsele süsteemile, ajaline eesmärk taasteplaanide koostamiseks

- **Maksimaalselt lubatav andmekadu** (RPO- recovery point objective) – ajavahemik, mille ulatuses võivad andmed taaskäivitamise puhul kaotsi minna. RPO on vajalik äripoolele sobiva IT taastestrateegia ja varundusmeetodite rakendamiseks.

Tuleb kindlaks määrata, **millised äriprotsessid on ETO jaoks kriitilised ning millised on kriitilised tegevused, mis neid äriprotsesse toetavad.** Organisatsiooni kriitiliste tegevustega seotud ja neid toetavad infosüsteemid ja infovarad võetakse ETO toimepidevust toetava IT riskianalüüsi sisendiks. Riskianalüüsi tulemusena koostatakse nimekiri olulistest riskidest, mis ohustavad elutähtsa teenuse katkematust.

Võrreldes BIA käigus kindlaksmääratud normväärtusi ja organisatsioonis eelnevalt kindlaks määratud riskitaluvust (riskide aktsepteerimise taset) tegelikult realiseeritud turvameetmetega, tehakse kindlaks olemasolevad vajakajäämised riskide haldamisel.

Kõik eelpool kirjeldatud protsessid, kokkulepitud normväärtused ja aktsepteeritav turvatase tuleb asjakohaselt dokumenteerida. Seejuures tuleks ka fikseerida, kuidas peab toimuma koostöö tarnijate, koostööpartnerite või väliste teenusetarnijatega hädaolukorras. IT-alased meetmed tuleb samuti kooskõlastada infoturbeosakonnaga.

1.3 IT riskianalüüsi tulemusel saadav lisandväärtus

IT riskianalüüsi läbiviimine organisatsioonis, riskide hindamine, tegevusplaani koostamine ja selle hilisem üle vaatamine aitab organisatsioonil vältida potentsiaalseid kahjujuhtumeid ja vähendada nendega seotud otseseid ja kaudseid kulutusi. Lisaks potentsiaalsete kahjude vähendamisele soodustab riskianalüüsi läbiviimine muude otseselt ja kaudselt rahas mõõdetavaid tulude saamist. IT riskihaldus aitab parendada organisatsiooni juhtimisprotsesse, suurendada tegevuste ja kulutuste läbipaistvust ning selgitada investeeringute majanduslikku põhjendatust.

Peamised efektiivsest riskihaldusest tulenevad üldised kasud organisatsiooni jaoks on järgmised:

- **juhtkond on kursis, mis organisatsioonis toimub**. Teades potentsiaalseid riske, on võimalik teha paremaid juhtimisotsuseid.

- **kolmandate osapoolte usalduse kasv**. Usaldusväärsuse kasv võib tähendada organisatsioonile uusi ja paremaid koostöölepinguid;

- **paremad võimalused kaasata lisainvesteeringuid**, sest finantsinstitutsioonid ja potentsiaalsed investorid jälgivad pidevalt ettevõtete jätkusuutlikkusega seotud aspekte;

- **läbipaistvamad protsessid, aruandlus ja suhtlus regulaatoritega** tänu rahvusvaheliste standardite ja tunnustatud parimate praktikate järgimisele;

- **täpsemalt prognoositavad tegevusplaanid ja parem ressursikasutus**, sest suudetakse paremini ära hoida võimalikke finantsalaseid ja põhitegevust mõjutavaid üllatusi ning teenusekatkestusi;

- **paraneb organisatsiooni maine** ja väheneb tõenäosus mainekahju tekkimiseks tulevikus;

- **selged organisatsioonisisesed rollid ja vastustuspiirid** tänu heale ülevaatele organisatsiooni varadest ning vastu võetud ning dokumenteeritud riskijuhtimisotsustele;

- **üldise riskiteadlikkuse kasv ja jätkusuutlik sisekultuur** motiveerib ja arendab organisatsiooni töötajaid. Riskianalüüsi läbiviimine aitab töötajatel ja juhtidel aru saada „suurest pildist" ja võimalikest tagajärgedest, mis võib tühisena näivast eksimusest tekkida.

IT riskide halduse protsesside juurutamine toetab ka organisatsiooni IT eesmärkide saavutamist ning muudab infotehnoloogiste vahendite kasutamise tõhusamaks läbi järgmiste tegurite:

- **riskikäsitluse väljundina saadav riskipõhine tegevusplaan** aitab planeerida IT tegevusi ja vajaminevaid ressursse ning seada tegevustele prioriteete. Tegevustele seatud konkreetsed vastutajad ja tähtajad võimaldavad eesmärkide täitmist paremini mõõta.

- **läbipaistvam ja põhjendatum IT eelarve**. Infoturbele tehtavad kulutused on võimalik siduda võimalike kulutustega, mis tekivad infoturbe intsidendiga ning on otseselt ja kaudselt rahas mõõdetavad. Riskianalüüsi käigus saadud ülevaade rakendavatest infoturbemeetmetest aitab tuvastada tehtud üle- ja alakulutusi, vajalikud kulutused on paremini põhjendatavad;

- **kasvab IT töötajate riskiteadlikkus.** IT organisatsiooni siseprotsessid sisaldavad infoturbe nõudeid ja neid järgitakse ka praktikas.

- **IT protseduurid on kooskõlas valdkonna parimate praktikatega**. Infoturbe riskidega arvestamine IT projekti varases faasis aitab vähendada võimalikke intsidente tulevikus ja optimeerida projektikulusid.

Uuendusmeelsed ettevõtte juhid on aru saanud, et infoturbemeetmete integreerimine kasutajatele mõeldud toodetesse ja teenustesse suurendab pikemas perspektiivis kasutajate rahulolu ja tekitab organisatsioonile uusi arenguvõimalusi. Kui organisatsioon suudab oma riske efektiivsemalt hallata kui konkurendid, omab ta teiste ees selget konkurentsieelist.

2 IT riskianalüüsi metoodika valik

Hetkel võib iga ETO kehtestada enda jaoks sobiva IT riskianalüüsi metoodika. Infoturvariski halduse üldraamistik on kirjeldatud rahvusvaheliselt tunnustatud standardis EVS-ISO/IEC 27005:2014. Samas jätab standard detailsete suuniste osas organisatsioonile vabad käed, oluline on riskipõhise lähenemise rakendamine ja sisendi andmine infoturbe halduse protsessile.

Eesmärgiga ühtlustada ETOde riskianalüüsi metoodikat ning muuta seeläbi riskianalüüsi tulemused omavahel võrreldavaks, koostas RIA soovitusliku metoodika elutähtsa teenuse osutaja IT riskianalüüsi läbiviimiseks, esitatud juhendis **„IT riskianalüüsi koostamise juhend ETOdele“**. Juhendi loomisel peeti silmas eesmärki, et IT riskide hindamise tulemused oleks võimalik viia ETO äri – ja operatsiooniliste riskidega sarnasesse taustsüsteemi. Levinud probleem on see, et IT riskianalüüsi tulemused on äritegevuse riskidega võrreldes kas liiga üle- või alahinnatud ning nende detailsusaste on oluliselt erinev teiste ettevõtte üksuste poolt kaardistatud tegevusriskidest.

Juhend jagab riskianalüüsi läbiviimise allpooltoodud etappideks ja etappidega seotud alamtegevusteks.

Riskianalüüsi etapid	Võtmetegevused
Kriitiliste IT varade ja teenuste identifitseerimine	• Oluliste infosüsteemide kaardistamine, kirjeldamine ja kriitilisuse hindamine. • Infosüsteemidega seotud muude infovarade kaardistamine.
Ohtude tuvastamine	• Kriitiliste tegevuste katkestusi põhjustavate ohtude väljaselgitamine ja seostamine infosüsteemidega. • Tuleb arvestada, et ohud ei ole staatilised ega esitatavad ammendava loeteluna.
Nõrkuste tuvastamine	• Nõrkuste tuvastamine, mille kaudu saavad realiseeruda varadele või organisatsioonile kahju põhjustavad ohud. • Nõrkuste seostamine eelnevalt kaardistatud infosüsteemide ja tuvastatud ohtudega.
Tõenäosuse hindamine	• Olemasolevate katkestusi ennetavate, avastavate ja tagajärgi leevendavate turvameetmete väljaselgitamine. • Tuvastatud ohtude realiseerumise tõenäosuse leidmine (arvestades turvameetmeid).
Tagajärgede hindamine	• Ohu realiseerumisel käideldavuse, tervikluse ning konfidentsiaalsuse kao võimalike tagajärgede tuvastamine. • Tagajärgede kaalukuse hindamine.
Riskihinnang	• Riskiklassi määramine. • Riskimaatriksi koostamine.
Riskikäsitlus	• Riskide loetlemine prioriteetsuse järjekorras koos riske ennetavate ja tagajärgi leevendavate turvameetmetega ning nende rakendamise eest vastutajate ja tähtajaga.

Tabel 1. Riskianalüüsi etapid. Allikas: IT riskianalüüsi koostamise juhend ETOdele.

Võrdleme standardis toodud tegevusi IT riskianalüüsi koostamise juhendis toodud riskianalüüsi etappidega.

Standard EVS-ISO/IEC 27005:2014 defineerib järgmised riskihalduse protsessid:

Riski kaalutlemine – kogu riskituvastuse, riskianalüüsi ja riski hindamise protsess tervikuna;

Riskituvastus – riskide otsingu, kindlakstegemise ja kirjeldamise protsess;

Riskianalüüs – protsess riski iseloomu väljaselgitamiseks ja riskitaseme määramiseks;

Riski hindamine – riskianalüüsi tulemite ja riski kriteeriumite võrdlemise protsess eesmärgiga teha kindlaks, kas risk ja/või selle suurus on aktsepteeritav või talutav;

Riskikäsitlus – riski muutmise protsess.

Mõistete kasutamisel tuleb tähel panna, et ISO standard käsitleb riskianalüüsi ühe alamprotsessina riskide kaalutlemisest, aga „IT riskianalüüsi koostamise juhend ETOdele“ näeb IT riskianalüüsi kui IT riskide haldamise koondprotsessi (vt. tabel 3 „Riskihalduse protsesside vastavustabel“).

Standard seostab riskide halduse protsessid organisatsiooni infoturbe halduse süsteemi (ISMS) põhitegevustega. Infoturbe riskide haldamine on pidev protsess, milleks on võimalik järgida Demingi PDCA (Plan, Do, Check, Act) pideva parendamise tsükli protsessimudelit.

ISMS- i protsess	Infoturvariski halduse protsess
Plaanimine	Konteksti loomine Riski kaalutlemine (riskituvastus, riskianalüüs, riski hindamine) Riskikäsitlusplaani koostamine Riski aktsepteerimine
Rakendamine	Riskikäsitlusplaani elluviimine
Kontrollimine	Riskide pidev seire ja läbivaatus
Järeltoimingud	Infoturvariski halduse protsessi käigushoid ja täiustamine

Tabel 2. ISMS-i protsessi ja infoturvariski halduse protsessi vastavus. Allikas: EVS-ISO/IEC 27005:2014.

IT riskianalüüsi koostamise juhend ETOdele“ on sisulises vastavuses **standardiga EVS-ISO/IEC 27005:2014**, kohandades selles toodud põhimõtteid elutähtsa teenuse osutajate spetsiifilkale ning tagades ühilduvuse elutähtsa teenuse toimepidevuse riskianalüüsi korraldusliku määrusega **“Toimepidevuse riskianalüüsi koostamise juhend” .**

Juhendis „IT riskianalüüsi koostamise juhend ETOdele“ määratletud etapid on vastavuses ISO standardis toodud etappidega järgnevalt:

ISO 27005 protsess	IT riskianalüüsi koostamise juhend ETOdele
Riskituvastus	Kriitiliste IT varade ja teenuste identifitseerimine Ohtude tuvastamine Nõrkuste tuvastamine
Riskianalüüs	Tõenäosuse hindamine Tagajärgede hindamine
Riski hindamine	Riskihinnang
Riskikäsitlus	Riskikäsitlus

Tabel 3. Riskihalduse protsesside vastavustabel

3 Riskianalüüsi etapid

3.1 Riskituvastus

3.1.1 Kriitiliste infosüsteemide ja varade kaardistamine

Vara on iga asi, mille jaoks on organisatsiooni jaoks väärtus. Oluline on selgelt määratleda ETO elutähtsa teenuse talitluspidevuse jaoks kriitilised tegevused, mille riske me kaalutleme ja mille varasid me sellest tulenevalt kaardistama hakkame. Infovarade kaardistamist tuleb alustada kriitiliste infosüsteemide ja teenuste tuvastamisest. Infosüsteem võib omakorda koosneda infovaradest, mis on infosüsteemi toimimise jaoks eluliselt ja otseselt vajalikud (kriitilised infovarad) ja nendest infovaradest, mis on ainult infosüsteemi toimimist toetava iseloomuga. Kaardistuse käigus tuleb üles loetleda ka toetavad infovarad (nt. UPS-seade, varundusserver, uksekaardisüsteem).

Infovarad klassifitseeritakse selle järgi, millist mõju sellega seotud intsident organisatsiooni normaalsele toimimisele avaldab. Teine alus klassifitseerimise läbiviimiseks on see, millise salastatuse astmega (nt. Avalik, Asutusesisene, Salajane, Konfidentsiaalne) andmeid infovara sisaldab. Kriitilisuse astme määramisel peab kindlasti osalema infovara omanik. Ilma varasid identifitseerimata ja nende kriitilisust määramata pole võimalik riskihaldust läbi viia.

Üks risk võib ohustada korraga paljude infovarade toimimist. Riskide mõju potentsiaalse kahju hindamiseks võib kasutada erinevaid meetodeid, kombineerides võimalikke rahalisi (nt. seadme asenduskulu) ja mitterahalisi (nt. mainekahju) kahjusid. Infovarade kaardistuse käigus selgub organisatsiooni äritegevusest lähtuv infovara tegelik väärtus, mis võib oluliselt erineda selle infovara soetusmaksumusest või raamatupidamislikust jääkväärtusest (Äriprotsessi ja varade kaardistamise seosed on toodud punktis 1.2).

3.1.2 Ohtude ja nõrkuste tuvastamine

Riski saab vaadelda varaga seotud ohu ja varaga seotud nõrkuse kombinatsioonina. Risk eksisteerib, kui mõlemad komponendid on esindatud. Seega võimalike riskide tuvastamiseks tuleb teada oma varasid, selle nõrkusi ja sellega seotud ohtusid.

Oht (eng threat) on soovimatu protsess või sündmus, mis võib organisatsiooni kahjustada.

Nõrkus (eng vulnerability) on organisatsiooni varade nõrk koht, mida üks või mitu ohtu on võimelised ära kasutama.

Peab tõdema, et me oskame arvestada vaid teadaolevate nõrkuste ja ohtudega. Suurt riski kujutavad tegelikult nõrkused ja ohud, mille kohta meil antud hetkel teadmine puudub, seega me ei oska neid ka takistada ega vältida. Nõrkuse olemasolu iseenesest ei tekita veel kahju, kui puudub oht, mis seda ära kasutab. Näiteks tarkvara puhul on need sellised vead, mis ei ole veel avalikuks tulnud. Häkkerid kasutavad tihti ära ajamomenti, mis jääb nõrkuse avastamise ja selle kõikides süsteemides parandamise vahele nn. „zero-day“ rünnete korraldamiseks.

Küberrünnete ja teiste tahtliku tegevusega seotud ohtude kaardistamisel tuleb tähelepanu pöörata võimaliku ründaja profiili kindlaks määramisele. Tuleb enda jaoks läbi mõelda, kes ja millistel põhjustel võib organisatsiooni tahta rünnata, mis oleks ründajale kõige tõenäolisem sihtmärk ja kui palju ründaja oleks valmis ründe õnnestumiseks kulutama ja riske võtma. Tõenäolisemaid ründestsenaariume teades

saame paremini planeerida kaitsemeetmeid ja kasutada ressursse nende varade kaitseks, mida kõige tõenäolisemalt rünnatakse.

Asjakohaste nõrkuste kindlakstegemiseks on vajalik teada, millised varad ja süsteemid on organisatsioonis kasutusel. Sellest lähtuvalt on võimalik kaardistada, millised turvameetmed on juba eelnevalt rakendatud ehk millised nõrkused on juba elimineeritud. Eelnevalt rakendatud turvameetmete efektiivsust tuleb ka järjepidevalt kontrollida.

Riskianalüüsi läbiviimise hõlbustamiseks on loodud erinevaid ohtude ja võimalike nõrkuste katalooge, mis varieeruvad väga üldistest loeteludest kuni spetsiifiliste ja detailsete tootepõhiste registriteni. Üks võimalik ohtude liigitus on järgmine:

- looduslikud sündmused (üleujutus, tuulepurustused, maavärin);
- ette kavatsemata sündmused (tulekahju, riistvara rike, elektrikatkestus);
- tahtlikud ja materiaalsed (süütamine, vargus, seadmete hävitamine);
- tahtlikud ja mittemateriaalsed (pettus, identiteedivargus, häkkerlus).

Üks võimalik ohtude kataloog on toodud ka riskianalüüsi koostamise juhendi lisas 3. Tüüpiliste ohtude näited. Selliseid katalooge saab kohandada konkreetse organisatsiooni iseärasustele, välistades ebatõenäolised ohud ja lisades juurde uusi, organisatsiooni tegevuse ja varadega seotud ohte ja riske. Eesti tingimustes võib näiteks välistada vulkaanipurske kui äärmiselt ebatõenäoliselt esineva klimaatilise sündmuse pool tekitatud ohu. Võimalike riskide ja eriti uute, päevakajaliste infoturvariskide kohta saab infot erinevate rahvusvaheliste organisatsioonide (nt. CERT ja SANS), infoturbeteemaliste veebiportaalide ja viirustõrje vahendite tootjate kodulehtede kaudu. Need organisatsioonid ja ettevõtjad tegelevad pideva infoturberiskide jälgimise ja avalikkuse riskidest teavitamisega.

Organisatsioonis kaardistatud riskid kajastavad tegelikult ainult sellel hetkel teadaolevat riskimaastikku. Praktikas on tegemist pidevalt muutuva keskkonnaga. Muudatused on tingitud tehnoloogia ja kasutatava tarkvara arengust, äsja avastatud turvanõrkustest, muutuvatest ärinõuetest, pilvetehnoloogia ja internetipõhiste teenuste laialdasest kasutuselevõtust ja kasutajate muutunud harjumustest. Kõige sellega peab riskide määratlemisel suutma kohaneda, lisades uusi ja ümber hinnates eelnevalt kaardistatud ohte ja nõrkuseid. Nõrkuste tuvastamisel on abi perioodilisest läbiviidavast infoturbe auditist. Olulisteks sisenditeks on ka organisatsioonis peetav intsidentide register. On üsna tõenäoline, et korra juhtunud intsidendid võivad korduda ka tulevikus. Eriti kehtib see juhul, kui juurpõhjuste välja selgitamiseks ja olukorra parandamiseks ei ole midagi ette võetud.

3.2 Riskianalüüs

3.2.1 Tõenäosuse hindamine

Riski realiseerumise tõenäosuse ja võimalike tagajärgede hindamine on infoturvariskide halduse keskseim osa, selle tulemus on peamine infoturbetegevuste planeerimise tööriist ja infoturvaprogrammi koostamise mõjutaja organisatsioonis.

Peamisteks meetoditeks on organisatsiooni võtmeisikutega läbiviidavad intervjuud, ettevalmistatud küsimustikud ning riskihindamise mudelite ja simulatsioonide kasutamine. Riskianalüüsi tulemuste esitamiseks ja üksikute riskide omavahelise võrreldavuse tagamiseks on kolm erinevat võimalust-kvalitatiivne ja kvantitatiivne riskianalüüs ning nende omavaheline kombineerimine.

Kuna kõik riskianalüüsid sisaldavad teataval määral subjektiivsust ja määramatust, siis võib täpsete rahaliste hinnangutega tulemi taotlemine osutuda ebaotstarbekaks. Kui kvalitatiivse riskianalüüsi

tulemusena on tekkinud riskidest üldine ettekujutus, võib suuremate riskide täpsemaks määratlemiseks kasutada mõjude rahalist määrangut.

IT riskianalüüsi koostamise juhend ETOdele kasutab tõenäosuste ja tagajärgede hindamiseks **kvalitatiivse riskianalüüsi** metoodikat.

Kvalitatiivse riskianalüüsi läbiviimisel tuginetakse erinevate riskistsenaariumide analüüsile, arvestades ohtude olulisust ja kaitstavate varade väärtust ning nende võimalikke nõrkusi. Hinnangute andmisel tuginetakse organisatsiooni kogemustele ja otsused tehakse suuresti hindajate varasema kogemuse ja teadmiste baasil. Kvalitatiivse riskianalüüsi korral kasutatakse riskide võimalike tagajärgede ja intsidentide esinemise sageduse hindamiseks eelnevalt kokku lepitud skaalal paiknevaid astmestikke.

Kvalitatiivne riskianalüüs on omal kohal, kui kogukahjudest moodustavad suure osa rahaliselt raskesti mõõdetavad kahjud, nagu näiteks mainekahju. Kvalitatiivse riskianalüüsi miinus on suur sõltuvus hindajate personaalsetest hinnangutest. Väga palju sõltub sellest, kuidas üks või teine osapool enda jaoks astmestikku tõlgendab. Seetõttu on vajalik astmestik üheselt mõistetavalt defineerida.

Tõenäosus	Ohu realiseerumise tõenäosuse kriteeriumid
5 - väga suur	• oht on juba avaldunud või ohu avaldumine on vältimatu; • >90% tõenäosusega leiab aset ühe aasta jooksul; • juhtub sageli; • võib juhtuda päevade ja nädalate jooksul.
4 - suur	1. ohu avaldumise tõenäosus on suur ning on olemas tõenäosust toetavad selged tõendusmaterjalid; 2. >50% tõenäosusega leiab aset ühe aasta jooksul; 3. võib kergesti juhtuda; 4. võib juhtuda nädalate ja kuude jooksul.
3 - keskmine	• ohu avaldumine on võimalik, eksisteerivad tõendusmaterjalid; • >10% tõenäosusega leiab aset ühe aasta jooksul; • võib juhtuda aasta jooksul.
2 - väike	• võimalik, aga praktilisi juhtumeid on üksikuid; • >1% tõenäosusega leiab aset ühe aasta jooksul; • võib juhtuda aastate pärast.
1 - väga väike	• riski avaldumine on pigem teoreetiline, praktikas üliharvad juhtumid; • < 1% tõenäosusega leiab aset ühe aasta jooksul; • mõeldav, kuid ainult ekstreemsetes tingimustes; • vähem kui 1 kord 100 aasta jooksul

Tabel 4. Tõenäosuse hindamine IT-riskianalüüsi koostamise juhendi kohaselt

3.2.2 Tagajärgede kaalukuse hindamine

Tagajärgede kaalukuse hindamisel on oluline meeles pidada, et negatiivsed tagajärjed ei tulene ainult sellest kui teenust ei saa mingil põhjusel osutada. Lisaks käideldavuse kaole tuleb arvestada ka kahjudega, mis tekivad teenusega seotud andmete konfidentsiaalsuse ja tervikluse rikkumisest.

Tagajärgede kaalukus (Tj)	Ohu realiseerumise tagajärgede kriteeriumid
Katastroofiline (E)	• kaasnevad katastroofilised (missioonikriitilised) kahjud; • ohu realiseerumine (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab elutähtsa teenuse pikaaegse katkemise või seab ohtu riigi julgeoleku või suure hulga inimeste elud või tekitab katastroofilisi tagajärgi keskkonnale või kriitilisi rahalisi kaotusi; • äärmiselt vaenulik avalikkuse ja meedia tähelepanu, mis kestab püsivalt kuid ning põhjustab klientide loobumise teenuse kasutamisest; • võivad tekkida pikaaegsed katkestused teiste elutähtsate teenuste toimimises või vahetu oht säärase olukorra tekkeks; • elutähtis teenus on häiritud 80 -100% ulatuses.
Väga raske (D)	• kaasnevad olulised kahjud; • ohu realiseerumine (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab elutähtsa teenuse olulise katkemise või seab ohtu riigi julgeoleku või põhjustab ohtu inimelule või keskkonnasaastet või väga olulisi rahalisi kaotusi; • märkimisväärne negatiivne avalikkuse tähelepanu, mis kestab nädalaid ning võib esile kutsuda klientide loobumise teenuse kasutamisest; • teiste elutähtsate teenuste pakkumine on oluliselt häiritud või on vahetu oht säärase olukorra tekkeks; • elutähtis teenus on häiritud 50 -80% ulatuses.
Raske (C)	• kaasnevad keskmised kahjud; • ohu realiseerumine (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) võib põhjustada katkestuse elutähtsa teenuse toimepidevuse töös või põhjustab ohtu inimeste tervisele või keskkonnale või olulisi rahalisi kaotusi; • negatiivne tähelepanu, mis kestab päevi ning mis võib hiljem korduda; • häiritud võib olla teiste elutähtsate teenuste pakkumine või on vahetu oht säärase olukorra tekkeks; • elutähtis teenus on häiritud 30 -50% ulatuses.
Kerge (B)	• kaasnevad vähe-olulised kahjud; • ohu realiseerumine (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt märkimisväärseid takistusi organisatsiooni funktsiooni täitmisele või märkimisväärseid rahalisi kaotusi; • negatiivne tähelepanu, mis on ajaliselt piiratud ühe päevaga; • elutähtsa teenuse osutamine võib olla häiritud 10-30% ulatuses.
Vähetähtis (A)	• ei kaasne märkimisväärseid kahjusid või kahjud puuduvad; • ohu realiseerumine (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) ei põhjusta olulisi takistusi organisatsiooni funktsiooni täitmisele; • põgus negatiivne tähelepanu, mis väljendub mõnes meediasõnumis; • elutähtsa teenuse osutamine ei ole häiritud.

Tabel 5. Intsidendi tagajärgede hindamine IT-riskianalüüsi koostamise juhendi kohaselt

3.3 Riskihinnang

Riskianalüüsi tulemusena leitakse elutähtsa teenuse osutamist enim kahjustada võivad riskisteenaariumid valemiga:

Riskiklass = Tagajärg * Tõenäosus

Riskianalüüsi käigus leitud võimalike riskistsenaariumid võrreldakse omavahel ja järjestatakse riskiklassi kaalukuse alusel. On võimalik, et pärast esmase riskianalüüsi läbiviimist tuleb seda osaliselt korrata, sest nüüd on võimalik omavahel võrrelda esmase analüüsi käigus sarnase riskireitingu saanud riske.

Võib arvata, et esmajärjekorras tuleb tegeleda riskidega, mis on nimekirja eesotsas ehk saanud endale kõige kõrgema prioriteedi. Praktikas tuleb arvestada ka sellega, et ühe riski avaldumine ja seotud intsidendid võivad endaga lumepalliefektina kaasa tuua ka teiste riskide avaldumise. Üheaegselt avaldunud riskid võivad kokkuvõttes tuua märksa olulisema kahju kui nende kogukahjude summad kokku liites. Kuna riskianalüüsi läbiviimine on aega ja inimressurssi nõudev tegevus, tuleks läbiviimise metoodika hoida võimalikult lihtne ja standardne. Vastasel puhul võib see jääda ühekordseks projektiks ega anna oodatud tulemusi.

3.4 Riskikäsitlus

Riskikäsitlus on protsess tuvastatud riskidega tegelemise viisi valimiseks ja valitud meetodi elluviimiseks vastavalt organisatsiooni riskitaluvusele ja valitud strateegiale.

Riski käsitlemiseks on neli erinevat võimalust: riski vältimine, riski vähendamine, riski jagamine ja riski aktsepteerimine.

Kõige lihtsamini kohaldatav meetod on **riski vältimine**. Organisatsioon kohandab oma siseseid protsesse lihtsalt niimoodi ümber, et risk ei ole enam päevakorras. Näiteks lõpetatakse organisatsioonis Windows XP tööjaamade kasutamine, sest toetuseta operatsioonisüsteemi kasutamine on seotud erinevate turvariskidega. Kui ettevõtte hooned asuvad üleujutusohtlikus piirkonnas, võib riski vältimiseks olla mõistlik ettevõtte kriitilised tegevused sealt ära kolida. Organisatsioon võib otsustada ka lõpetada tegevuse antud tegevusalas, millega antud risk seotud on.

Riski vähendamine toimub eelkõige läbi infoturbe meetmete ja kontrollide rakendamise organisatsioonis. Meede võib olla võetud kasutusele ühe või mõne konkreetse riskiga seotud ohu või nõrkuse vähendamiseks. Sellised meetmed on eelkõige tehnilist laadi. Samas eksisteerivad ka üldised ja organisatsioonilised infoturvameetmed, mis parendades üldist infoturvataset vähendavad mõjusalt korraga paljusid tuvastatud infoturvariskide mõjusid. Infoturbe meetmete rakendamine organisatsioonis vajab ressursse, seega tuleb hoolega kaaluda, millised kulutused infoturbele on mõttekad ja millised mitte. Teoreetiliselt on võimalik leida selline taluvuspunkt, millest suuremaid eeldatavaid kahjusid organisatsioon ei aktsepteeri. Iga taluvuspiiri ületava riski vähendamiseks tuleb rakendada meetmeid, mis toovad eeldatava kahju allapoole määratud taluvuspiiri.

Riskide maandamise meetmeid võib jagada ka ennetavateks, tagajärgi leevendavateks ja avastavateks turvameetmeteks.

Riski jagamist on käsitletud kui riskistsenaariumi toimimise kohta kindlustusasutusest kindlustuse võtmist. Selline kindlustuseliik ei ole väga levinud, kuna ühelt poolt napib vastavaid kindlustusandjaid ja teiselt poolt tuleb arvestada kindlustusettevõtetele makstavate tasude suurusega. Teatud olukorras on see siiski mõistlik ja mõne elutähtsa teenuse pakkuja puhul ka kohustuslik meede, tagamaks ettevõtte ärijätkuvuse ka kõige katastroofilisemate tagajärgedega riskide ilmnemise korral. Teine oluline riski jagamise viis on väliste teenusepakkujate kasutamine. Kui välise teenusepakkuja juures midagi juhtub,

siis on see teenuse pakkuja, mitte teenuse saaja risk. Riski jagamine ei võta organisatsioonilt andmete ja teiste varade kaitsemise kohustust ja vastutust oma klientide, omanike ja teiste seotud osapoolte ees.

Risk on äritegevusega paratamatult kaasnev nähtus. Kuna kõikide riskide elimineerimine on võimatu ettevõtmine, peab iga organisatsioon enese jaoks kehtestama taseme, millest alates ollakse teadlikult nõus jääkriski aktsepteerima. **Riskide aktsepteerimine** on päevakorral, kui täiendavate riskimaandamise meetmete rakendamine osutub majanduslikult või muudel põhjustel ebaotstarbekaks. Teistel puhkudel ei ole riski vähendamisega mõistlik tegeleda, kuna eeldatavad kahjud riski avaldumisel on nii väikesed, et ei põhjusta sellega organisatsioonile märgatavaid probleeme. Riski aktsepteerimine peab olema kalkuleeritud otsus ja seda ei tohi segamini ajada riski ignoreerimisega. Mida suurema riskiastmega riskidega on tegemist, seda kõrgemal tasemel peavad olema vastu võetud riskide käsitlemise otsused. Aktsepteeritud riske tuleb perioodiliselt üle vaadata, sest muutuvas ärikeskkonnas võib riskitolerants ajas muutuda.

Riske, mis jäävad alles pärast riskikäsitluse etappi, nimetatakse **jääkriskideks**.

4 Riskide pidev seire ja läbivaatus

Tõhusa riskihalduse süsteemi elushoidmise jaoks peab ETO juurutama asjakohased riskide monitooringu protseduurid. Pidev riskide seire ja läbivaatus annavad aluse selleks, et riskianalüüs ja riskikäsitlusplaanid oleks ajakohased. Infoturbe halduse protseduurid näevad ette perioodiliste staatusaruannete koostamise ning vajalike töötajate ning juhtkonna teavitamise infoturbe olukorrast. Infoturbe aruanded ei pruugi olla otseselt seostatud eelnevalt kaardistatud infoturvariskidega, kuid infoturbearuannete sisu ja aruandes kajastatud mõõdikute trendianalüüs annavad olulise sisendi järgmise plaanilise riskianalüüsi läbiviimiseks.

Elutähtsa teenuse pakkuja peab kindlustama, et riskianalüüsi tulemused ja riskikäsitlusplaanid oleks asjakohased ja ajakohased. Olulise infoturbeintsidendi toimumine võib koheselt muuta seotud riskide reitingut ning tähendada täiendava riskianalüüsi ning riskikäsitluse protsessi läbiviimist. Organisatsioon peab olema suuteline jälgima infoturbemeetmete tõhusust ja avastatud häiretele kiiresti ja asjakohaselt reageerima. Väga oluline on koostöö ja kommunikatsioon kõigi seotud töötajate vahel. Avastatud anomaaliatest tuleb kiiresti teada anda, selleks peab olema töötajate hulgas läbi viidud piisav infoturbeteavitus ja sisse seatud instantsid, kes seda infot koguvad ja analüüsivad.

Kui organisatsioonis toimuvad olulised muudatused, tuleks riskide hindamist korrata, sest muudatused põhitegevuses või IT süsteemides võivad kätkeda endas uusi infoturvariske või siis muutuvad osad seni kaardistatud riskid ebaolulisteks.