TALLINNA ÜLIKOOL

Mart Mäe

ISO/IEC 27002 STANDARDI RAKENDAMINE TEENUSEPORTAALI HALDAVAS ORGANISATSIOONIS

Magistritöö

INTERAKTIIVNE MEEDIA JA TEADMUSKESKKONNAD

Juhendaja: K. Kikkas

Autor: ..... “.....“ ..... 2010.a.

Juhendaja: ..... “.....“ ..... 2010.a.

Instituudi direktor: ..... “.....“ ..... 2010.a.

Tallinn 2010

SISUKORD

SISSEJUHATUS

Personaalarvutite, tava- kui ka ärilise suunitlusega tarkvara järjest laialdasem levik on kaasa toonud ühiskonnas uue nähtuse - tehniliselt oskuslikud, ent kuritahtlikud arvutientusiastid ehk kräkkerid. Viimaste tegevuse tulemusena hakkasid levima arvutiviirused, pahavara, elektrooniline rämpspost jms. Nüüdseks on nende viimati nimetatute kasutamisest välja kujunenud varimajanduse tähelepanuväärne osa. „Kräkkerid“ olid need, kes leiutasid järjest rohkem võimalusi, kuidas küberkuritegevuse kasuks tööle rakendada kõiki eelpool loetletuid pahalasi.

Eelkõige arvutientusiastide ehk kräkkerite järjest aktiivsem tegutsemine on põhjuseks, miks IT turvalisuse valdkond viimastel aastatel üha rohkem tähelepanu pälvib ja seda nii koduarvutikasutajate kui ka äriettevõtete hulgas. Reeglina konkureerivad ettevõtted ning finantsasutused oma ärisaladusi konkurentidele ei avalda - erandiks on saanud infoturbe valdkond. Selles valdkonnas on ühendatud jõud ning loodud vastavad organisatsioonid, et jagada kogemusi ning parimaid turvalisuse valdkonnas rakendatud praktikaid ja kõike seda seetõttu, et on jõutud arusaamisele, et organiseeritud küberkuritegevuse rünnaku vastu on kõige parem võidelda organiseeritud kaitsega. Eesmärgistatud koostöö tulemusena on valminud mitmeid turvet reguleerivaid standardeid. Enamus neist põhineb vähemal või suuremal määral ettevõtete parimatel turvalisuse praktikatel ning IT audiitorite ja konsultantide kogemustel.

Infoturbe kvaliteetseks korraldamiseks on välja töötatud erinevaid parimate praktikate ning soovituste kogumeid. Muuhulgas on olemas rahvusvaheliselt tunnustatud standardid nagu organisatsiooni ISO/IEC poolt loodud standardid 17799 ja 13335 ning Saksamaa infoturbe korraldamise eest vastutava organisatsiooni poolt välja antud infoturbe korralduse juhendid, mille alusel on loodud ka Eesti infosüsteemide kolmeastmeline etalonturbe süsteem (ISKE). Eelpool esile toodud standardite näol ei ole tegemist lõpliku loeteluga infoturbe valdkonna korraldamiseks mõeldud juhendmaterjalidest. Hetkel ei ole välja töötatud standardit, mis oleks rakendatav igas ettevõttes ja organisatsioonis. Standardi või muu juhendmaterjali valikul tuleb lähtuda ettevõtte võimalustest ja vajadustest infoturbe korraldamiseks.

Käesolev magistritöö käsitleb ühte turvalisust reguleerivat standardit ISO/IEC 17799, millele tuginedes analüüsib autor teenuseportaali haldava ettevõtte arendus –ja muudatushalduse protsesside turvalisuse vastavust standardile. ISO/IEC 17799 standard on valitud analüüsitava organisatsiooni poolt, kuna see on nende hinnangul kõige sobivam infoturbe korralduse raamistik organisatsiooni eripära arvestades. Käesoleva töö koostamisel on kasutatud alusmaterjalina Eesti Vabariigi Standardiameti poolt välja antud standardit nimega „EVS-ISO/IEC 17799:2003", mis on inglisekeelse standardi üksikasjalik tõlge eesti keelde. Autori hinnangul on emakeelse standardi kasutamise eeliseks inglisekeelse originaalteksti ees töö ülesehituse parem arusaadavus ning probleemide sõnastuse üheselt mõistetavus. Analüüsi aluseks on autor kasutanud siiski inglisekeelset standardit ISO/IEC 17799:2005 ning samuti on autor ära võrrelnud töös käsitletavad eestikeelsed tekstid inglise keelsete tekstidega. Kuigi tegemist on kahe erineva versiooniga standardist ei tuvastanud autor erinevusi käesolevas töös käsitletavate teemade osas. Töö kirjutamise hetkel on standard vahetanud nime ISO/IEC 27002 vastu, millest tulenevalt on autor magistritöö pealkirja vastavalt ajakohastanud. Kuna auditeerimise hetkel järgis ettevõtte standardit ISO/IEC numbriga 17799:2005, siis viitab ka autor käesolevas töös standardile ISO/IEC 17799:2005.

Autorile teadolevalt ei ole käsitletavat standardit süvitsi varem analüüsitud. Kuna infoturbe valdkonda reguleerivad standardite valik on lai, soovib autor käesoleva tööga tutvustada ühe võimaliku turvastandardi rakendamist ning auditeerimist praktilise näite alusel. Käesoleva magistritöö esimeses osas annab autor ülevaate infoturbest, valdkonda reguleerivate standardite peamisest jaotusest ning käesolevas töös analüüsitava standardi tekkest ja sisust. Magistritöö teises osas analüüsib autor esmalt standardi nõudeid ja kõrvutab need analüüsitava organisatsiooni hetkeseisu vastavuse saavutamiseks rakendatud meetmetega, kasutades andmete kogumise vahendina intervjuusid ja rakendatud kontrollide testimisi. Analüüsi teises etapis analüüsivad standardile vastavust autor ning kaks eksperti, kusjuures iga analüüsija toob välja tema hinnangul olulisemad puudused ning kõik nimetatud annavad koondhinnangu igale analüüsitavale valdkonnale suutvusküpsusmudeli alusel. Lisaks koondab autor iga valdkonna lõikes enda ja ekspertide arvamused ning toob välja standardi rakendamise peamised puudused. Autori ja ekspertide poolt läbi viidava tulemuste analüüsi eesmärgiks on välja selgitada turvastandardi juurutuse võimalikkus või mitte võimalikkus teenuseportaali haldavates organisatsioonides ja seda mõlemal juhul - kui kogu arendustegevus tehakse sisemise arendusmeeskonna poolt ning ka juhul kui kogu arendustegevus on sisse ostetud väliselt

partnerilt. Autori ja ekspertide standardi nõuetele vastavuse analüüsi tulemusena kujuneb ülevaade ühe tavapärase organisatsiooni puudustest standardi juurutusel ning ühtlasi soovib autor näidata, et käsitletavale teemale on oluline tähelepanu pöörata olgu siis tegemist sotsiaalset keskkonda haldava ettevõtte/organisatsiooniga või siis teenuseportaali haldava ettevõtte/organsatsiooniga.

1. INFOTURVE JA INFOTURBE STANDARDID

1.1 Infoturve

Ettevõtte esmaseks funktsiooniks on teenida kasumit ning olla edukas oma tegevusvaldkonnas. Ärimaailmas on valdkondi, mille edu põhineb peamiselt inimpotentsiaalil (näiteks auditeerimise ettevõtted) ning kus tehnoloogia omab pigem toetavat funktsiooni. Samas on vastukaaluks ka palju selliseid ettevõtlusvaldkondi, kus suurem osa inimtööst on võimalik asendada tehnoloogiaga (näiteks autotööstus), kuna viimane on lihtsalt nii aja- kui ka kuluefektiivsem. Siiski seob erinevaid ärivaldkondi vähemalt üks ühine huvi ja selleks on infoturve. Infoturve all peetakse silmas teabe ja infosüsteemide kaitsmist loata juurdepääsu, kasutamise, avaldamise, muutmise või hävitamise eest [44 U.S.C § 3542 (b)(1), 2006]. Peaaegu kõikide ettevõtete jaoks on oluline maandada infovaradest tulenevad ohud ja riskid minimaalse aktsepteeritava tasemeni (RIA, 2004). Ameerika Ühendriikides 2005. aastal läbiviidud uuringu käigus selgus muuhulgas, et 67 % küsitletud ettevõtetest tunnistas vähemalt ühte esinenud intsidenti seoses küberkuritegevusega. Nendest omakorda 68% olid kannatanud kahju vähemalt 10,000 USD ulatuses, mis on märkimisväärne summa, andes hea pildi küberkuritegevuse tegelikust levikust ja mahust [BJS, 2005].

Turvalisuse korraldamise eesmärgiks on kaitsta organisatsiooni olulisemaid varasid nagu informatsioon, riist –ja tarkvara. Läbi hoolikalt valitud meetmete rakendamise kaitseb organisatsioon oma füüsilisi ning rahalisi ressursse, mainet, juriidilist staatust, töötajaid ning teisi materiaalseid ja immateriaalseid varasid, mis on olulised organisatsioonile äriliste eesmärkide täide viimisel. Üldjuhul turvalisuse ja selle korralduse all kujutatakse ette liigseid äri takistavaid (aeglustavaid) protseduure ja bürokraatiat nii juhtidele kui ka spetsialistidele. Üldjuhul on selline arvamus kujunenud valede meetmete ja protseduuride rakendamise tulemusel. Mittesobivate meetmete rakendamise tulemusena on hakanud levima arusaam, et meetmete rakendamine ei paranda turvakorraldust, vaid suurendab üksnes bürokraatiat. Tegelikkuses tuleb meetmed rakendada vaid organisatsiooni jaoks tõelistele riskikohtadele, sest ainult selliselt valitud ja juurutatud meetmed tagavad oluliste äriliste eesmärkide saavutamise ja sama ajal ka organisatsiooni varade kaitse. Meetmeid rakendatakse vähendamaks tõenäosust vigade esinemiseks, kuna ükski meede ei taga 100% turvalisust. Meetmeid valides tasub alati mõelda, et mis on võimalik meetme rakendamise ning käitamise kulu ning kas see kaalub üles mitte rakendamisest saadava võimaliku kahju. Iga rakendatud

meede vajab hilisemat ümberhindamist, sest organisatsiooni ja tarkvarade muudatustega võib muutuda ka vajadus meetme järgi (NIST, 1995).

1.2 Infoturbe standardite jaotumine

Turvastandardid võib suures plaanis jagada andmeturbe ning auditi/kontrolli keskseteks.

Andmeturbekeskseid metoodikaid iseloomustab lähtumine vajalikest andmeturbe meetmetest / tegevustest ehk mida on vaja teha selleks, et oleks tagatud infosüsteemi(de) turvalisus. Kuigi metoodikad põhinevad hetke parimale teadmisele ja praktikale, vajavad need pidevat ajakohastamist. Välja töötatud metoodikate ülesandeks on anda andmeturbespetsialistile selgeid ning üheselt mõistetavaid juhiseid meetmete rakendamiseks. Eelpool kirjeldatud kategooriasse kuulub näiteks Infosüsteemide Kolmeastmeline Etalonturbe süsteem (ISKE) (Kivimaa, 2004). Rahvusvahelistest standarditest võib siinkohal välja tuua Bundesamt für Sicherheit in der Informationstechnik (BSI) poolt välja antud IT etalonturbe käsiraamatu, mille alusel on välja töötatud eelpool nimetatud ISKE standard (RIA, 2006).

Kontrolli / auditikesksed metoodikad põhinevad äriprotsesside ja nende turvariskide käsitlusel - määratletakse ohtude / riskide loetelu ja kontrollitakse, kas kõigi nende jaoks on turvameetmed rakendatud ja piisavad (turvameetmete piisavuse hinnang põhineb samuti hetke parimale teadmisele / praktikale). Rahvusvahelistest turvakorralduse andmeturbekesksetest standarditest võiks tuntumaks lugeda Rahvusvaheline Standardiorganisatsioon (ingl. International Standard Organisation, edaspidi ISO) ja Rahvusvaheline Elektrotehnikakomisjon (ingl. International Electrotechnical Commission, edaspidi IEC) standardit numbriga 13335, mille eesmärgiks on anda infoturbe haldusaspektide kohta suuniseid, mitte lahendusi. Teine tuntum standard infoturbe vallast, mis on samuti ISO ja IEC poolt publitseeritud, kannab numbrit 17799. Standardis lahatakse turvalisust eelkõige regulatoorsel / kontrolli tasandil. Standard kirjeldab detailsed nõudmised, kuid ei täpsustata meetmeid, millega infoturvalisuse nõuetele vastavus saavutada (EVS TK 4, 1999).

Eelpool esile toodud standardite näol ei ole tegemist lõpliku loeteluga infoturbe valdkonna korraldamiseks mõeldud juhendmaterjalidest. Hetkel ei ole välja töötatud standardit, mis oleks rakendatav igas ettevõttes ja organisatsioonis (Kivimaa, 2008).

Standardi või muu juhendmaterjali valikul tuleb lähtuda ettevõtte võimalustest ja vajadustest infoturbe korraldamiseks (NIST, 2003).

1.3 ISO/IEC 17799 standard

ISO või IEC rahvuslikud liimeskogud osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendes organisatsioonides rajatud käsitlema tehnilise tegevuse eri valdkondi. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale huvi pakkuvatel aladel /…/" (EVS TK 4, 2003). Selles töös osalevad käsikäes ISO ja IEC-iga ka muud rahvusvahelised riiklikud ja mitteriiklikud organisatsioonid (EVS TK 4, 2003).

„Infotehnoloogia alal on ISO ja IEC loonud ühise tehnilise komitee ISO / IEC JTC 1. Ühises tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse rahvuslikele kogudele hääletamiseks. Avaldamine rahvusvahelise standardina nõuab vähemalt 75% hääletanud rahvuslike kogude heakskiitu" (EVS TK 4, 2003). Tähelepanu tuleb pöörata ka seigale, et mõned käsitletava rahvusvahelise standardi elemendid võivad olla patendiõiguse objektiks. ISO ega IEC ei ole kohustatud nimetatud patendiõigusi välja selgitama (EVS TK 4, 2003).

Käesolevas töös käsitleb autor ISO ja IEC poolt publitseeritud standardit numbriga 17799. Standardis lahatakse turvalisust eelkõige regulatoorsel / kontrolli tasandil. Standard kirjeldab detailsed nõudmised, kuid ei täpsustata meetmeid, millega infoturvalisuse nõuetele vastavus saavutada. Nagu ISKE standardiski, peetakse infoturvalisuse all silmas mitmeid erinevaid alamkategooriad (EVS TK 4, 2003) :

a. konfidentsiaalsus: on tagatud, et informatsioon on kättesaadav ainult neile, kes on volitatud saama juurdepääsu;
b. terviklus: informatsiooni ja ta töötlusmeetodite täpsuse ja täielikkuse kaitstus;
c. käideldavus: on tagatud, et volitatud kasutajail on vajaduse korral juurdepääs informatsioonile ja sellega seotud varadele;

Informatsiooni turvalisus saavutatakse sobivate meetmete rakendamisega, milledeks võivad olla poliitikad, menetlusviisid, protseduurid, organisatsioonilised struktuurid ja tarkvarafunktsioonid. Need meetmed tuleb kehtestada organisatsiooni konkreetsete turvaeesmärkide saavutamise tagamiseks (EVS TK 4, 2003).

Kõnealune standard on väga mahukas, sisaldades muuhulgas meetmeid ja regulatsioone personali korraldusest, kasutajaõiguste jagamisest ning taasteplaanide

koostamisest ja viimaste testimiste nõuetest. Tulenevalt autori erialast käsitletakse käesolevas töös peamiselt tarkvara arenduse ja muudatuste halduse protsessiga seotud turvalisuse meetmeid ning regulatsioone. Täpsemalt käsitleb autor kolme valdkonda standardist: süsteemide turvanõuded, turve rakendussüsteemides ning arendus- ja tugiprotsesside turve. Tabelis 1 on välja toodud analüüsi aluseks olevas standardis käsitletavad põhivaldkonnad.

Tabel 1

Reguleeritavad valdkonnad ISO/IEC17799 standardis

Nr	Standardi pealkiri
1	Käsitlusala
2	Terminid ja määratlused
3	Turvapoliitika
4	Organisatsiooniline turve
5	Varade liigitamine ja ohje
6	Personaliturve
7	Füüsiline ja keskkonnaturve
8	Side ja ekspluatatsiooni haldus
9	Pääsu reguleerimine
10	Süsteemide arendus ja hooldus
11	Äritegevuse jätkuvuse haldus
12	Vastavus

Allikas: /autor/

1.4 Suutvusküpsusmudel

Suutvusküpsusmudeli ehk Capability Maturity Model (edaspidi CMM) esimene versioon ilmus 1987. aasta septembris muuhulgas Watts S. Humphrey poolt ning kandis nime „A Method for Assessing the Software Engineering Capability of Contractors", CMU/SEI-87-TR-23. Tegemist oli 40-leheküljelise küsimustikuga, mis andis juhised selleks, et hinnata sisseostetava tarkvaraarenduse teenusepakkuja võimekust (SEI, 1987). Juba nimetatud dokumendis eksisteeris CMM alustala - viie palli süsteemis hindamisskaala, mis on säilinud erinevates redaktsioonides tänaseni. Käesolevas töös kasutatava mudeli tööpõhimõte on sama: hinnata erinevaid ISO/IEC 17799 standardi valdkondade vastavust viie palli skaalal. Hinnang on antud kõigi nelja kriteeriumi lõikes (vt. ka lisa nr. 1) ning lõpliku hinnangu valdkonnale annab madalaim väärtus. See on kõrgeim tase, kus kõik kriteeriumid on täidetud. Sellisel viisil hindamine annab auditile tellija seisukohast lisandväärtuse, kuna on võimalik tuvastada hinnanguline hetkeseis. Alternatiivina saaks hinnangut anda ka lihtsustatud meetodil, otsustades kas standardi

nõuded on rakendatud või ei ole. Paraku selline analüüs ei anna lisandväärtust töö tellijale ning ei võimalda anda suuniseid ettevõtte turvalisuse arengu juhtimiseks järgnevatel aastatel.

2. ISO/IEC 17799 STANDARDI RAKENDAMINE TEENUSEPORTAALI HALDAVAS ORGANISATSIOONIS

2.1 Andmed

Käesoleva magistritöö analüüsi objektiks on autor valinud avalikku sektorisse kuuluva organisatsiooni. Analüüsitava ettevõtte põhitegevuseks on erinevat liiki toetuste jagamine taotlejatele. Oma tegevuse spetsiifilisuse tõttu kuulub ettevõte delegeeritud funktsioone täitvate institutsioonide koosseisu. Viimastele laienevad suhteliselt spetsiifilised nõuded infoturbe korralduse osas ning sellest tulenevalt on nimetatud gruppi kuuluvatel ettevõtetel ja organisatsioonidel regulatsioonist tulenev kohustus järgida andmeturbe korralduse standardites sätestatut. Analüüsitav ettevõte lähtub oma infoturbe korraldusel ISO/IEC 17799 standardis sätestatust.

Käesolev magistritöö on edasiarendus autori bakalaureusetööst pealkirjaga „ISO/IEC 17799 standardi vastavuse analüüs“, mille raames autor analüüsis organisatsiooni turvakorralduse vastavust nimetatud standardiga. Magistritöös keskendub autor ISO/IEC 17799 standardi punktidele 10.1, 10.2 ning 10.5, mis käsitlevad teenuseportaali arendamise ja muudatuste halduse turvalisust.

Sarnaselt bakalaureusetööle analüüsib autor standardi nõudeid ja ettevõtte hetkesituatsiooni ning toob välja olulisemad puudused. Lisaks annab autor hinnangu igale analüüsitavale standardi valdkonnale suutvusküpsusmudeli alusel.

Analüüsi käigus kaasab autor kaks infotehnoloogia korralduse ja auditeerimise eksperti ühest suurimast IT konsultatsiooni ja auditeerimise ettevõttest. Eksperdid on valitud samast ettevõttest, kuna käsitletavat infot ei ole andmete delikaatsuse tõttu võimalik laialdaselt avaldada.

Ekspert 1 on osalenud mitmetes rahvusvahelistes majanduse ja infotehnoloogia valdkonda kuuluvates konsultatsiooni projektides nii meeskonna liikme ja kui ka juhina. Ekspert on konsulteerinud IT projekte aga ka juhtinud IT konsultantide osakonda. Igapäevaselt tegeleb eelkõige IT ja -juhtimise ning nendega seotud standardite ja metoodikate juurutamise konsulteerimisega.

Ekspert 2 on spetsialiseerunud peamiselt tarkvaraarenduse valdkonnale. Enamasti on konsultant olnud analüütiku ja projektijuhi rollis. Hetkel konsulteerib ettevõtteid IT valdkonnas, peamiselt IT protsesside parendamise ja efektiivsemaks muutmise osas.

2.2 Hüpoteesid

Analüüsi aluseks olev organisatsioon järgib oma turvakorralduses standardit ISO/IEC 17799. Kuna organisatsioon on ka teenuseportaali haldaja, siis on oluline aru saada arenduste ja muudatuste halduse korralduse vastavusest standardi nõuetele. Lisaks soovib autor koos ekspertidega välja selgitada käsitletava standardi rakendatavuse võimalused analüüsitavas organisatsioonis ja muudes portaale haldavates sarnastes organisatsioonides.

*H_1: **ISO/IEC 17799 standard on rakendatav teenuseportaali haldavas organisatsioonis***

2.3 Metoodika

Standardile vastavuse analüüsi alginfo omandamiseks viib autor läbi intervjuud kliendiga , mille alusel tuvastab kontrollikohad. Intervjuude käigus läbib autor standardi nõuded valdkonna eest vastutava organisatsiooni töötajaga esitades intervjueeritavale küsimusi standardi nõuetest lähtuvalt, tuvastamaks juba organisatsiooni poolt rakendatud meetmeid. Peale organisatsiooni poolt rakendatud meetmete tuvastamist tuvastas autor meetmete reaalset toimivust testimisi läbi viies. Testimised viis autor läbi vastavalt IT auditi metodoloogiale, mille põhimõtted on kirjeldatud infosüsteemide audiitorite ühingu ISACA poolt (ISACA, 2010). Intervjuude ja testimiste alusel omandatud info põhjal kirjeldas autor organisatsiooni situatsiooni ekspertidele esitatud materjalides. Käesoleva töö analüüsi teises osas analüüsivad kaks kaasatud eksperti autori poolt esitatud materjali, kus on muuhulgas kirjeldatud detailselt organisatsiooni poolt rakendatud meetmed. Kõrvutades autori kirjeldust ja standardi nõudeid, annavad eksperdid hinnanguid suutvusküpsusmudeli alusel. Suutvusküpsusmudeli alusel annab hinnanguid ka autor. Samuti toovad autor kui ka eksperdid eraldi välja suuremad puudujäägid aga ka ettepanekud analüüsitud protsesside paremaks ning turvalisemaks korraldamiseks.

Autor koondab enda ja kahe eksperdi arvamused ning soovitused, analüüsib viimaste ühisosa ning erinevusi. Lõpptulemusena esitab autor nii enda kui ka ekspertide poolt tuvastatud olulisemad puudused ja soovitused ning esitab suutvusküpsusmudeli alusel keskmise hinde iga analüüsitava standardi punkti kohta. Keskmine hinne arvutatakse autori ja ekspertide poolt antud konkreetse valdkonna suutvusküpsusmudeli hinnete aritmeetilise keskmisena. Kui esimene number peale koma on 5, 6, 7, 8, 9, suurendatakse viimast allesjäävat järku ühe võrra. Ülejäänud juhtumitel jäetakse järk muutmata.

Soovituste korrektsel rakendamisel oleks organisatsioonil teoreetiline võimalus saavutada vastavus analüüsitavate standardi punktide osas.

2.4. Analüüs

2.4.1 Süsteemide turvanõuded

Standardi nõue ja sisu

ISO standardi punkti 10.1 kohaselt on süsteemide turvanõuete määratlemise eesmärgiks tagada turbe sisseehitamine infosüsteemidesse (EVS TK 4, 2003).

Hea tava ja käsitletava ISO standardi kohaselt peaks ettevõtte enne infrastruktuuri ning ärirakenduste väljatöötamise algust selgelt piiritlema ning kokku leppima turvanõuetes. Piiritlemine peaks aset leidma juba projekti alg- ehk nõuete faasis, kus tuleb läbi viia analüüs, mille tulemused dokumenteeritakse ühe osana infosüsteemi väljatöötamise üldistest tööülesannetest. Samuti sätestab käsitletav standard, et dokumendis peab olema kirjeldatud nii automatiseeritud turvamehhanismid kui ka käsi-turvamehhanismide toe vajadus. Analüüsi käigus tuleb arvestada, et turvanõuded ja meetmed peavad olema vastavuses infovarade ärialase väärtusega. Lisaks soovitab standard arvesse võtta, et meetme rakendamise kulu ei tohi olla kõrgem, kui võimaliku kahju suurus meetme mitte rakendamise korral (Ibid., lk 84).

Analüüs ja protseduurid

Standardi punkt 10.1.1 sätestab, et uusi süsteeme või seniste süsteemide täiustusi nõudvate ärivajaduste sõnastused peavad sisaldama ka nõudeid turvameetmetele. Ärivajaduste spetsifikatsioonis peaks olema kirjeldatud nii automatiseeritud turvamehhanismid kui ka käsi-turvamehhanismide toe vajadus (Ibid., lk 84).

Tuvastamaks nõuete täitmist küsisin kliendilt arenduskorra, mis kirjeldab ka vajaduse süsteemi arendamise algfaasis turvameetmete ja kontrollide kirjeldamiseks. Kontrollimaks arendustegevuste vastavust korrale ning algfaasis kontrollide kirjeldamist sain kliendilt aasta jooksul läbi viidud kolme suurema arenduse dokumentatsiooni. Iga analüüsitud arenduse kohta oli detailselt kirjeldatud arenduse sisu, arendusega saavutatavad funktsionaalsused ning rakendatavad sisestuskontrollid. Rakendatavate sisestuskontrollide kirjeldamisel oli lähtutud kasutuslugude kirjeldustest ning protsesside järgnevusest ja viimaste seostest. Näiteks ei ole postiindeksit võimalik sisestada enne aadressi ning sisestatud andmeid ei ole võimalik kinnitada enne aadressi sisestamist.

Tulemused ja järeldused

Kõrvutades standardist tulenevaid nõudeid ettevõttes evitatuga võib ühe olulise puudusena välja tuua detailse riskianalüüsi puudumise tarkvara kontrollidele. Pehmendava asjaoluna saab siiski välja tuua selle, et kuigi formaliseeritud kujul ei ole riskianalüüsi tehtud, on detailselt analüüsitud riskikohti infosüsteemi dokumentatsioonis ja tarkvara disainidokumentides. Autori hinnangul on tegemist formaalse puudusega.

2.4.2 Turve rakendussüsteemides

Standardi nõue ja sisu

ISO standardi punkti 10.2 kohaselt on oluline vältida kasutaja andmete kaotust, muutumist või väärkasutust rakendussüsteemides (EVS TK 4, 2003).

Hea tava ja käsitletava ISO standardi kohaselt tuleks rakendussüsteemidesse ning sealhulgas kasutajate kirjutatud rakendustesse kavandada sobivad turvameetmed ja kontrolljäljed või tegevuselogid. Need peaksid hõlmama sisendandmete, sisemise töötluse ja väljundandmete valideerimist. Süsteemides, mis töötlevad tundlikke, väärtuslikke või elutähtsaid organisatsiooni varasid või mõjutavad neid, võidakse vajada ka lisameetmeid. Sellised meetmed tuleks määrata turvanõuete ja riskide hindamise põhjal (Ibid., lk 85).

Analüüs ja protseduurid

Tulenevalt ISO standardi punktist 10.2.1 tuleb andmesisestust rakendussüsteemidesse valideerida veendumaks, et see on õige ja asjakohane. Kontrollimist tuleks rakendada äritehingute püsiandmete (nimed ja aadressid, krediidilimiidid, klientide viitenumbrid) ja parameetritabelite (müügihinnad, valuutakursid, maksumäärad) sisestusele (Ibid., lk 85).

Standardi punkt 10.2.1 soovitab kaaluda järgnevaid kontrolle.

„a) topeltsisestust või muid sisestuse kontrolle vigade avastamiseks:

1) piirkonnavälised väärtused;
2) väärad märgid andmeväljadel;
3) puuduvad või puudulikud andmed;
4) andmemahu üla- ja alapiire ületavad andmed;
5) volitamata või vastuolulised juhtandmed;“

Lisaks soovitab standard kaaluda järgmisi meetmeid:

> „b) võtmeväljade või andmefailide sisu perioodilisi läbivaatusi nende lubatavuse ja tervikluse kinnituseks;
> c) sisendandmete paberdokumentide kontrolli sisendandmete volitamata muutuste avastamiseks (kõik muudatused sisenddokumentides tuleks volitada);
> d) protseduure valideerimisvigadele reageerimiseks;
> e) protseduure sisendandmete usutavuse testimiseks;
> f) kõigi andmesisestuse protsessiga seotud töötajate kohustuste määratlemist.“ (EVS TK 4, 2003)

Intervjuu käigus arendusjuhiga selgus, et tema hinnangul on analüüsitud tarkvara arendusfaasis kontrollide rakendamise vajadust. Muuhulgas tõi arendusjuht esile kliendi identifikaatori terviklikkuse kontrolli rakendamise. Tema sõnul on identifikaator oluline, kuna selle alusel seotakse süsteemis erinevad dokumendid ja teenused konkreetse kasutajaga. Sellest tulenevalt kontrollitakse isikukoodi, sisestatud nime ja kliendi identifikaatori omavahelist sobivust, kuna kliendi identifikaator on tuletatud tema nimest ja isikukoodist. Lisaks on arendusjuhi sõnul rakendatud ka elementaarseid meetmeid takistamaks tekstiväljadele numbrite sisestamist ja ka vastupidi. Sisestatavad andmed, mis ei muutu tihti, on proovitud defineerida eelseadistatud valikutena ehk juhtandmetena. Arendusjuhi hinnangul on juhtandmed vähendanud inimlikust eksimisest tulenevate vigade esinemist nii klientidel kui ka klienditeenindajatel.

Standardi punktis 10.2.1 loetletud kontrollide rakendatust reaalses töökeskkonnas testis autor andmesisestusprotsessi simuleerides. Esmalt proovis autor sisestada suvaliselt valitud väljale „Aadress“ ainult numbreid, selle tulemusena kuvati veateate ekraanil, et sisestatud väärtuses on viga ning et aadress peab koosnema tänava nimest ehk tähtedest ja numbritest ehk süsteem kontrollib, et väljal oleks nii tähti kui ka numbreid. Sellest saame järeldada, et väärasid märke ning piirkonna väliseid väärtusi ei ole võimalik sisestada. Andmemahu ülem -ja alampiiri testimiseks proovis autor üles laadida faili suurusega ~10 megabaiti (MB). Infoväljas oli aga märgitud maksimaalseks lubatud failisuuruseks 5 MB ning faili serverisse laadimise lõpus andis infosüsteem veateate, et üles laetud fail ületab lubatud suurust 5 MB ning faili ei salvestata. Siit järeldab autor, et piirang serverisse failide salvestamisel on infosüsteemis rakendatud. Järgnevalt jättis autor infosisestamise vaates sisestamata isikukoodi, mille tulemusena kuvas infosüsteem andmete salvestamisel veateate, et on täitmata kohustuslik väli „Isikukood“. Seejärel autor sisestas tahtlikult

vaid isikukoodi esimesed 5 numbrit, mille tulemusel kuvas infosüsteem veateate, et sisestatud isikukoodi formaat on vigane. Peale isikukoodi korrektset sisestamist kustutas autor oma perekonnanimest ühe tähe ära ning proovis tulemust salvestada. Selle tegevuse tulemusena kuvas süsteem veateate, et isikukood ja nimi ei ole kooskõlalised. Testimiste tulemusena saame järeldada, et on rakendatud ka puuduolevate ja puudulike oluliste andmete kontroll, sest isikukood ja nimi olid aluseks kliendi identifikaatori koostamisel. Andmete sisestamise vaates olid mitmetes kohtades defineeritud ka juhtandmed. Näiteks valides teenuse liiki, kuvatakse vaid etteantud valikuid ning infosüsteemi kasutajal ei ole võimalik välja tühjaks jätta ega ka väljale vabateksti sisestada. Küsides arendusjuhilt viimase põhjalikuma infosüsteemide kontrollide testimise akti või memo selgus, et hetkel ei viida ettevõttes läbi perioodilisi ülevaatusi rakendatud kontrollide toimivuses veendumiseks ning seda ka peale suuremaid arendusi.

Käsitletava standardi punkte c, d, e ja f autor käesoleva töö raames ei vaatle, kuna käesoleva töö teemaks on infosüsteemide arendamise ja haldamise turvalisus. Standardi punktid c - f ei ole enam infosüsteemi halduse ja arendusega nii lähedalt seotud ja on pigem organisatsioonisisesed andmete kvaliteedikontrollid.

Standardi punkt 10.2.2.1 soovitab andmeid rikkuda võivate töötlusvigade või sihilike andmete rikkumise toimingute avastamiseks rakendada süsteemis erinevaid valideerimiskontrolle. Selle juures tuleks silmas pidada, et rakendatakse kontrolle just terviklikkuse kaoni viivate töötluse tõrgete riski esinemise minimeerimiseks. Standardi kohaselt tuleks kaaluda järgmiste meetmealade kasutuselevõtu vajadust:

> „a) andmete muutmist teostavate liitmis- ja lahutusfunktsioonide kasutamist ja asukohta programmides;
>
> b) protseduure, millega vältida programmide käitust vääras järjestuses või käitust pärast algse töötluse nurjumist;
>
> c) andmete õige töötluse tagamiseks õigete programmide kasutamist tõrgetest taastamiseks“ (Ibid., lk 86).

Intervjuu käigus selgus, et eelkirjeldatud meetmealade rakendamise vajadusega on arendusjuhi sõnul arendamise käigus arvestatud. Arendusjuhi sõnul oli juurutusfaasis kirjeldatud protseduurid ja piirangud reguleerimaks ning kontrollimaks andmetega tehtavaid toiminguid ja andmete kvaliteeti.

Standardi punktis 10.2.2.1 loetletud nõuete täitmiseks palusin arendusjuhilt juurutusfaasis kirjeldatud protseduure ja piiranguid ning infosüsteemi kontrollpäringute programmitekste. Dokumentide vaatluse käigus selgus, et on loodud taastamise

protseduur, mis sisaldas ka detailset kirjeldust andmete taastamisest toimingute logidest. Arendusjuhi sõnul on selle protseduuri eesmärk taastada andmebaasi vigade eelne seis kuni vigase kirjeni ning seeläbi minimeerida võimalikku andmekadu. Palusin ka infosüsteemi juurutusdokumentatsiooni osa, kus on kirjeldatud andmete kustutamise ja muutmisfunktsioonide infosüsteemivaadetele jaotamine. Säärane jaotis oli loodud kasutajalugude ning kasutajaõiguste gruppide kirjeldamise sektsioonis. Andmete muutmise õigused olid vaid andmetöötlejate poolt kasutatavatel infosüsteemi vaadetel. Intervjuu käigus vaatles autor infosüsteemi vastavat infosüsteemi vaadet ning veendus andmete kustutamise võimaluse puudumises. Vaatluse käigus salvestas autor andmed infosüsteemi ning veendus, et peale salvestamist oli võimalus vaid sisestatud andmeid mitte-aktiivseks muuta, kuid kustutamise funktsiooni ei olnud programmivaates. Võimalus andmetel vaid kehtivus lõpetada tagab autori hinnangul lisaks kustutamise piiramisele ka kõikide andmete muudatuste logimise.

Standardi punkt 10.2.2.2 soovitab andmete kontrollimiseks vajalikke vahendeid rakendades pidada silmas, et viimaseid tuleb valida sõltuvalt rakenduse iseloomust ja andmete riknemise võimalikust mõjust äritegevusele. Kontrollivahendid, mille rakendamise vajadust on käsitletavas standardis võimalike riskide maandamiseks kirjeldatud, on järgmised:

„a) seansi- või pakimehhanismid andmefailide seisude sobituseks pärast tehinguvärskendusi;

b) tasakaalustuskontrollid avamisseisude võrdlemiseks eelmiste sulgemisseisudega, nimelt

1) käitustiirude vahelised kontrollid;

2) failivärskenduste kontrollsummad;

3) programmidevahelised kontrollid;

c) süsteemi genereeritud andmete valideerimine (vt 10.2.1);

d) kesk- ja kaugarvuti vahel alla- või üleslaaditud andmete või tarkvara tervikluse kontrollid (vt 10.3.3);

e) kirjete ja failide kontrollsummad;

f) kontrollid veendumiseks rakendusprogrammide õigeaegses käituses;

g) kontrollid veendumiseks, et programme käitatakse õiges järjestuses ja nende töö lõpetatakse tõrke korral ning et edasine töötlus peatatakse kuni probleemi lahendamiseni“ (EVS TK 4, 2003).

Intervjuu käigus arendusjuhiga selgus, et arendamisel on kaalutud ka andmevahetuse kontrollide rakendamist, tagamaks sisestatud andmete korrektne salvestamine. Arendusjuhi sõnul kontrollitakse andmeid iga päev, võrreldes andmebaasi hommikust kontrollsummat eelmise päeva õhtuse kontrollsummaga. Kontroll on rakendatud põhimõttel, et töövälisel ajal andmete sisestust on kas vähe või tegevus üldse puudub. Infosüsteemis on ka kirjeldatud päringud, mis kontrollivad peamiselt infosüsteemi salvestatud klientide andmete kvaliteeti. Andmete kvaliteeti valideeritakse jooksvalt rakendatud sisestuskontrollide abil, mida on autor käsitlenud käesolevas töös, analüüsides standardi punkti 10.2.2.1. Arendusjuhi sõnul veendutakse infosüsteemi õigeaegses käituses kaudselt andmetöötlejate poolt, kuna viimaste töö oleks häiritud süsteemi madala töökiiruse või mitte töötamise korral. Lisaks jälgib serverite parameetreid ka infosüsteemi administraator. Arendusjuhi sõnul infosüsteem andmeid ei salvesta, kui esineb viga salvestamisel. Meetmena on kasutusele võetud kontroll andmebaasi ja infosüsteemi rakenduse serveri vahele, mis kontrollib aktiivse ühenduse olemasolu andmebaasi serveriga. Kohe kui ühendus puudub, ei luba rakendus andmeid sisestada ega päringuid käivitada. Andmebaasivärskenduste kontrollsummasid kontrollitakse süsteemiadministraatori poolt võrreldes tootja kodulehelt alla laetud andmebaasi platvormi uuenduste faili kontrollsummat tootja kodulehel kuvatavaga.

Erinevate intervjuu käigus selgunud ja standardi punktis 10.2.2.2 kirjeldatud kontrollide reaalses toimivuses ja nende rakendamises veendumiseks viisin läbi järgnevalt kirjeldatud testid. Esmalt testisin andmebaasi terviklikkuse kontrolli ehk hommikuse ja õhtuse kontrollsumma võrdlust. Tööandmete mitterikkumise huvides viisime kontrolli läbi testkeskkonnas, mis oli töökeskkonna identne koopia. Autor vaatles, kuidas arendusjuht käivitas kontrollsummade võrdluse ning peale toimingu lõppu kuvas süsteem teate, et vigu ei tuvastatud. Tuvastamaks süsteemse võrdluse suutlikkust tekkinud vigu tuvastada muutis autor käsitsi kontrollsumma faili ning uuesti võrdlust käivitades andis süsteem veateate sisuga „Kontrollsummad on erinevad“. Sellest tulenevalt järeldab autor, et kontrollsummade võrdlus on edukalt rakendatud ja toimiv meede. Testimaks süsteemiadministraatori jälgimise efektiivsust ning infosüsteemi kontrolli mitte edastada päringuid andmebaasi serverile ilma aktiivse ühenduseta, katkestasime me andmebaasi testserveri töö operatsioonisüsteemi vahendeid kasutades. Seejärel avas autor infosüsteemi avalehe, kus oli kuvatud veateade, mille sisuks oli „Vabandame, hetkel on infosüsteemis käimas hooldustööd“. Kümme minutit peale serveri töö katkestamist helistas süsteemiadministraator arendusjuhile pärimaks aru katkestuse pärast, seega

toimis ka süsteemiadministraatori poolne jälgimine. Sisestuskontrollid testis autor käesolevas töös käsitledes standardi punkti 10.2.2.1.

Tulemused ja järeldused

Kõrvutades standardi nõudeid ettevõttes evitatuga tuvastas autor suurima puudusena standardi punktis 10.2.2.1 kirjeldatud kontrollide toimivuse järjepideva kontrolli puudumise. Vajakajäämine on oluline, kuna ettevõtte pidevalt arendab ja uuendab infosüsteemi. Lisaks on oluline kontrollida ka punktis 10.2.2.2 kirjeldatud kontrollide toimivust peale suuremaid muudatusi või arendusi infosüsteemis. Arendusjuhi sõnul ei ole kontrollide toimivuse teste hetkel läbi viidud, kuna vastavate testimiste läbiviimiseks ei ole organisatsioonil piisavalt ressurssi. Lisaks leiab autor hetkel rakendatud süsteemiadministraatori jälgimise olevat mitte piisava meetmena, kuna süsteemiadministraator ei jõua jälgida infosüsteemi töökiiruse parameetreid pidevalt. Testimiste käigus helistas süsteemiadministraator 10 minutit peale testserveri töö katkestamist arendusjuhile, mis on autori hinnangul liiga pikk reageerimise aeg arvestades töökeskkonna katkestust. Autori hinnangul tuleks organisatsioonil kaaluda infosüsteemi töökiiruse jälgimise automatiseerimist, kasutades kontrollpäringu(id)t, mille tulemused kuvatakse süsteemiadministraatorile reaalajas ekraanil.

2.4.3 Arendus- ja tugiprotsesside turve

Standardi nõue ja sisu

ISO standardi punkti 10.5 kohaselt on oluline säilitada rakendussüsteemi tarkvara ja informatsiooni turvalisus (EVS TK 4, 2003).

Hea tava ja käsitletava ISO standardi kohaselt peaksid rakendussüsteemide eest vastutavad juhid vastutama ka projekti- või tugikeskkonna turvalisuse eest. Vastutavad juhid peavad tagama, et kõik muudatused, mida plaanitakse süsteemi rakendada, kontrollitakse läbi veendumaks, et need ei riku süsteemi või töökeskkonna turvalisust. (Ibid., lk 95).

Analüüs ja protseduurid

Standardi punkti 10.5.1 kohaselt tuleb välja töötada ja kehtestada formaalsed muutuseohje sundprotseduurid. Protseduur peab tagama, et muudatuste rakendamise käigus ei rikutaks turbe –ja ohjeprotseduure, et tugiprogrammeerijatel on ligipääs vaid

nende tööks vajalikele süsteemide osadele ning et iga rakendatava muudatuse kohta saadakse ja säilitatakse formaalne nõusolek ja kinnitus. Lisaks soovitab standard võimalusel rakenduste ja ekspluatatsiooniliste muudatuste ohje protseduurid integreerida. Muutuseohje protseduur peaks reguleerima järgnevat:

„a) kokkulepitud volitustasemete registri pidamist;

b) tagamist, et muudatusi esitavad volitatud kasutajad;

c) turvameetmete ja tervikluseprotseduuride läbivaatust veendumiseks, et muudatused ei riku neid;

d) kogu parandusi vajava tarkvara, informatsiooni, andmebaasielemendistiku ja riistvara väljaselgitamist;

e) detailsetele ettepanekutele formaalse kinnituse saamist enne töö alustamist;

f) tagamist, et volitatud kasutaja nõustub muudatustega enne nende teostamist;

g) evitamise tagamist äritegevuse võimalikult minimaalse häirimisega;

h) tagamist, et iga muudatuse lõpuleviimisel süsteemi dokumentatsiooni komplekt värskendatakse ja et vana dokumentatsioon arhiveeritakse või kõrvaldatakse;

i) kõigi tarkvara värskenduste versiooniohje käigushoidu;

j) kõigi muudatustaotluste kontrolljälgede säilitamist;

k) tagamist, et vastavusse viimiseks ekspluatatsioonidokumentatsiooni ja kasutajaprotseduure muudetakse vajalikul viisil;

1) tagamist, et muudatuste teostamine leiab aset õigel ajal ega häiri äriprotsesse, mida ta puudutab.“ (EVS TK 4, 2003).

Lisaks informeerib standard, et paljud organisatsioonid hoiavad käigus eraldi keskkonda testimiste läbi viimiseks. Eraldi testimise keskkonna omamine võimaldab ka lisaturvet testimisel kasutatavale infole eraldatuse tõttu tootmis –ja arenduskeskkondadest (lbid, lk 96).

Nende nõuete täitmise kontrollimiseks viis autor läbi intervjuu ning testimised arendusjuhiga. Arendusjuhi sõnul oli välja töötatud ja juurutatud muudatuste haldamise protseduur. Intervjuu käigus analüüsis autor koos arendusjuhiga protseduuri üleseehitust ja sisu. Protseduuris oli infosüsteemi IT poolseks peakasutajaks ning ühtlasi vastutajaks määratud arendusjuht. Lisaks oli määratletud vastutajad ka organisatsiooni äripoolel, kelle ülesandeks oli veenduda arenduste toimivuses läbi funktsionaalsuste testimiste ning viimaste tulemuste dokumenteerimine. Lisaks sätestas protsess, et kõik infosüsteemi muudatused tuleb kiita heaks nii peakasutaja kui ka äripoole funktsionaalsuse testija poolt. Lisatingimusena oli määratud, et muudatuste paigaldamiseks tuleb kasutada

töövälist aega piiranguga, mis tähendas et muudatuse süsteemi rakendamise hetkest pidi jääma tööpäeva alguseni vähemalt 5 tundi. Protsessis kirjeldati ka kohustust ning vajadust uuendada infosüsteemi ja protsesside dokumentatsiooni enne muudatuse töökeskkonda rakendamist ja ka eelmise infosüsteemi versiooni salvestamist vahetult enne uue paigaldust. Vastavalt protsessile oli muudatuste töökeskkonda paigaldamise ainuõigus süsteemide hoolduse ja halduse osakonnal. Arendusjuhi peamiseks protsessi järgseks kohustuseks oli hallata kogu muudatuste protsessi ehk peamiselt koos arendajaga läbi viia eelanalüüs selgitamaks välja arenduse kulu ja võimalik saavutatav kasutegur. Protsess kirjeldas, et on loodud muudatuste ettepanekute esitamise vorm ning et muudatuse ettepanekuid võivad esitada kõik töötajad, kuid muudatuste kvaliteedi ja ka ressursside mõistlikuks kasutamiseks peab arendusjuht analüüsima kõiki esitatud muudatuste taotlusi. Muudatuste protseduuris eristati ka muudatuste suurust rahalises mõõtmes ehk kui üksik muudatus või omavahel seotud muudatuste kogumi arendustöö(de) maksumuseks oli rohkem kui viiskümmend tuhat krooni, siis pidi muudatus olema kiidetud heaks ka muudatuste halduse -ja arenduskomitee poolt, kuhu kuulusid IT juht, arendusjuht ja tegevjuht.

Testimaks eelmises lõigus kirjeldatud nõuete täitmist sain kliendilt nimekirja aasta jooksul infosüsteemi tehtud muudatustest. Nimekiri ei sisaldanud muudatusi, mida infosüsteemi erinevatel põhjustel ei oldud infosüsteemi auditi hetkeks rakendatud. Omandatud nimekirjas oli loetletud üle 200 muudatuse ning autor valis nimekirjast juhuvalikut kasutades 25 muudatust. Autor kontrollis, kas iga valitud muudatuse kohta on olemas autoriseeritud tellimus ja analüüs, kas muudatuse toimivuses veendumiseks on läbi viidud testimised ja tulemused tegevustest on säilitatud ning kas on olemas taasesitatavas vormis kinnitused arendusjuhilt ja äripoole kasutajalt muudatuse toimivuse ja muudatuste töökeskkonda rakendamise kohta ning samuti süsteemide haldus- ja hooldusosakonnalt muudatuse edukast või mitteedukast paigaldusest töökeskkonda.

Selgus, et valitud kahekümne viiel muudatusel esines erinevaid puudusi. Viiel juhul oli puudu kinnitus arendusjuhilt enne muudatuse töökeskkonda rakendamist, samas oli olemas äripoole esindaja testimiste tulemus ja kinnitus, et muudatuse funktsionaalsus on ootuspärane. Ühel juhul oli muudatus, mille arendamine maksis rohkem kui viiskümmend tuhat krooni, kiitmata heaks enne arendusse minekut muudatuste halduse - ja arenduskomitee poolt. Heakskiitmine oli tehtud muudatuse testimise ajal. Viieteistkümnel juhul oli testimiste kirjeldus lakooniline ning sellest tulenevalt puudus auditeerimise hetkel selge ülevaade, kas testiti muudetud funktsionaalsuse toimivust

korrektselt ja täielikult. Neljal juhul oli tellimus täidetud peale muudatuste töökeskkonda rakendamist. Kõikide vaadeldud muudatuste tellimuste puhul ei olnud organisatsioon analüüsinud muudatuste võimalikku mõju süsteemis rakendatud kontrollidele. Arendusjuht tõi intervjuu käigus välja asjaolu, et tellimused tehti hiljem, kuna tegemist oli kiireloomuliste muudatustega. Autor analüüsis ka muudatuste sisu ning leidis, et tegemist oli vigade parandustega. Muudele tuvastatud puudustele arendusjuht täpseid põhjusi ei osanud välja tuua, kuid tema arvamus oli, et organisatsiooni töötajatel ei olnud aega protsessi järgida. Arendusjuht lisas, et ta ise ei ole protseduuri täitmise kvaliteeti jooksvalt jälginud.

Standardi punkte 10.5.2 – 10.5.4 autor käesolevas töös ei käsitle, kuna punktides käsitletakse infosüsteemide operatsioonisüsteeme, standardtarkvarapakettide modifitseerimist ja koodi tehnilisi detaile. Käesoleva töö eesmärgiks on aga anda ülevaade arendus ja muudatuste protsessist ja seda ümbritsevatest kontrollidest.

Standardi punkti 10.5.5. soovitab tarkvaraarenduse väljastpoolt tellimisel arvesse võtta järgnevaid asjaolusid:

„a) litsentsilepinguid, koodi omandiõigust ja intellektuaalse omandi õigusi;

b) sooritatava töö kvaliteedi ja õigsuse tõendamist;

c) deponeerimise korraldust kolmanda osalise tõrke puhuks;

d) pääsuõigusi sooritatud töö kvaliteedi ja õigsuse auditeerimiseks;

e) lepingunõudeid koodi kvaliteedi kohta;

f) installeerimiseelset testimist trooja koodi avastamiseks. „ (EVS TK4, 2003)

Nõuete täitmise testimiseks küsisin kliendilt arendaja ja organisatsioonivahelise arenduslepingu. Siinkohal peab autor oluliseks välja tuua, et leping reguleerib ka pisiarenduste ja muudatuste tegemist infosüsteemis. Analüüsides lepingut selgus, et see kirjeldas nii organisatsiooni kui ka arendajapoolsed vastutajad. Samuti oli lepingus kirjas, et nii koodi kui ka rakenduse omandiõigus on tellijal, kelleks on praegusel juhul käsitletav organisatsioon. Lepingus ei olnud täpsustatud koodi üle andmise ja koodi säilitamise protsessi organisatsioonis. Samuti ei sätestanud leping koodikvaliteedile nõudeid. Arendusjuhi sõnul olid säilitatud vanemad versioonid koodist andmekandjal, kuid pidevat uuendamise mitte formaalset ega formaalset protsessi ei ole otseselt loodud. Samas hindas ta ohtu minimaalseks, kuna kood on suures osas dokumenteeritud. Arendusjuht ei osanud täpsustada, millise detailsuse ja täpsusega on kood arendaja poolt kommenteeritud. Samas tõi ta välja, et plaanis on tellida programmikoodi audit veendumaks koodi kvaliteedis üldiselt kui ka koodi kommenteerimises.

Lepingus ei olnud arvestatud olukorraga, kus arendaja ei ole suuteline kokku lepitud teenust pakkuma. Arendusjuhi sõnul sellist vajadust ei ole ette näha, kuna organisatsiooni hinnangul suudaks ka muu arenduspartner mõistliku aja jooksul sama infosüsteemi edasi arendada. Samuti ei peetud oluliseks lepingu sõlmimisel vajadust veenduda arendaja jooksva töö kvaliteedis. Samas ei tundunud auditi läbiviimise hetkel arendusjuhile reaalne ja ka kasulik auditeerida arenduspartneri tööprotsesse.

Installeerimise eelset testimist trooja koodi tuvastamiseks arendusjuhi sõnul läbi ei viida. Samas hindas ta vastava riski suhteliselt madalaks, kuna serverite operatsioonisüsteemidesse on installeeritud ka viirusetõrje ning arendaja poolt viiruse sisse programmeerimist pidas ta ebatõenäoliseks.

2.5 Tähelepanekud ja hinnangud suutvusküpsusmudeli alusel

Käesoleva alapeatüki eesmärgiks on kokku võtta eelnevates peatükkides tuvastatud puudused lähtudes ISO/IEC 17799 põhivaldkondadest. Igast puudusest vormistab autor riski kirjelduse, hindab hetke olukorda suutvusküpsusmudeli alusel ning esitab soovitused ja ettepanekud puudus(t)e kõrvaldamiseks. Lisaks palub autor mõlemal eksperdil anda hinnang kirjeldatud riskiprofiilile ja vastavusele standardis sätestatule suutvusküpsuse mudeli alusel ning samuti välja tuua suuremad puudused ja ettepanekud protsesside paremaks korraldamiseks. Alapeatüki eesmärk on kokku võtta läbiviidud töö ning sõnastada tuvastatud tähelepanekud auditeeritavale organisatsioonile sobivas vormis.

Hinnangute andmisel kasutatava suutvusküpsusmudeli jaotiste selgitused on esitatud tabelis 1. Iga analüüsitava valdkonna juures esitatud suutvusküpsusmudeli tabelis on antud hinnang kõigi nelja kriteeriumi lõikes. Eraldi on välja toodud autori ja ekspertide personaalsed hinnangud ning lõpuks on nende alusel moodustatud koondhinnang. Lõpliku hinnangu valdkonnale annab madalaim väärtus, mis on ühtlasi kõrgeim tase, kus kõik kriteeriumid on täidetud. Viie palli süsteemis antud hinnangute selgitused on välja toodud käesoleva töö lisas 1.

Tabel 2

Suutvusküpsusmudeli valdkondade selgitused

Hinnang			
A	**B**	**C**	**D**
Probleemi teadvustamine ja edastamine; Allikas:/autor/	Poliitika;	Poliitika juurutamise/täitmise jaoks vajalikud protsessid ja koolitused;	Poliitikate ja seotud protsesside tulemuslikkuse mõõtmine ning toetudes mõõdetule parenduste tegemine.

2.5.1 Süsteemide turvanõuded

Standardi punkti 10.1.1 kohaselt tuleks iga uue tarkvara või uue funktsionaalsuse korral viia läbi riskianalüüs tuvastamaks olulisemad riskikohad ning ühtlasi kulu ühe või teise riski realiseerumisel. Tarkvara disainidokumentatsiooni analüüsimise käigus selgus, et eraldi riskianalüüsi ei ole läbi viidud, kuid riske oli analüüsitud tarkvara kasutamislugude alusel. Selles tulenevalt elimineeriti põhilised riskikohad eelkõige süsteemi kasutamise seisukohast. Rahalisi mõõtmeid ühe või teise riski realiseerumisel arvesse ei võetud. Detailse riskianalüüsi puudumine loob ohu, et maandamata on riskid, mille realiseerumisel võib olla kahju organisatsioonile äärmiselt suur.

Tabel 3

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.1.

Testitud standardi punkt	**Hinnang**				
Süsteemide turvanõuded (10.1)	**A**	**B**	**C**	**D**	**Lõplik**
Nõue: *Kõik turvanõuded, kaasa arvatud taandemeetmete vajadus, tuleks piiritleda projekti nõuetejärgus ning põhjendada, kokku leppida ja dokumenteerida ühe osana infosüsteemi üldisest tööülesandest.*	**3**	**3**	**2**	**2**	**2**

Allikas: /autor/

Soovitus nr. 1: *Uute tarkvarade kasutuselevõtmise, tarkvara arenduse ja suuremate muudatuse sisseviimise korral soovitame kaaluda riskianalüüsi läbiviimist, et tagada süsteemi käitlemisega kaasnevate riskide piisav maandamine ning vastavus standardile ISO/IEC 17799.*

Ekspert 1

Ekspert leiab, et hetkel kasutusel olev mitteformaalne riskianalüüs võib jätta mõne olulise riski tähelepanuta. Ekspert leiab, et metoodiline lähenemine tagaks kõikide ohukohtade kaalumise ja analüüsimise. Tema hinnangul annab korralik analüüs ka kindluse, et organisatsioon omandab teadmised uute funktsionaalsuste mõjust süsteemis juba rakendatud kontrollidele. Muus osas leiab ekspert rakendatud kontrollide taseme olevat rahuldava.

Tabel 4

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.1.

Testitud standardi punkt	**Hinnang**				
Süsteemide turvanõuded (10.1)	**A**	**B**	**C**	**D**	**Lõplik**
Nõue: *Kõik turvanõuded, kaasa arvatud taandemeetmete vajadus, tuleks piiritleda projekti nõuetejärgus ning põhjendada, kokku leppida ja dokumenteerida ühe osana infosüsteemi üldisest tööülesandest.*	**3**	**3**	**3**	**2**	**2**

Allikas: /autor/

Ekspert 2

Ekspert tõi peamise probleemina välja asjaolu, et analüüsi faasis pööratakse liiga vähe tähelepanu kontrollfunktsioonidele ja nende disainile. Nimelt leiab ekspert, et analüüsi faasis riskidele vähene tähelepanu pööramine võib organisatsioonile osutada hiljem äärmiselt kulukaks. Põhjusena toob ekspert välja asjaolu, et kontrolljälgede hilisem lisamine võib osutada liiga ajamahukaks ja kulukas või tehniliselt mitterakendatavaks. Samas märgib ta, et kontrollide mitterakendamine võib tähendada suuremat manuaalse kontrolli osakaalu ehk suuremat palgakulu organisatsioonile.

Tabel 5

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.1.

Testitud standardi punkt	**Hinnang**				
Süsteemide turvanõuded (10.1)	**A**	**B**	**C**	**D**	**Lõplik**
Nõue: *Kõik turvanõuded, kaasa arvatud taandemeetmete vajadus, tuleks piiritleda projekti nõuetejärgus ning põhjendada, kokku leppida ja dokumenteerida ühe osana infosüsteemi üldisest tööülesandest.*	**2**	**2**	**2**	**2**	**2**

Allikas: /autor/

Kokkuvõte

Autor ja eksperdid olid ühel nõul standardi punkti 10.1 rakendamise peamise puuduse osas, milleks oli vähene analüüs infosüsteemi kontrollifunktsioonidele analüüsi faasis. Sellekohane soovitus on juba sõnastatud autori poolt, kuid ekspert 2 poolt välja toodud täpsustus kontrolljälgede hilisema rakendamise kulukuse kohta on autori arvates oluline asjaolu, mida soovitus ei kajasta. Autor täiendas soovitust nr 1 vastavalt ning lõpptulemus vastavast soovitusest on esitatud peale suutuvusküpsusmudeli kokkuvõtet. Hinnang standardi rakendatuse tasemest oli autoril ning ekspertidel erinev, kuid lõplik hinnang oli siiski kõigil analüüsijatel sama.

Tabel 6

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.1.

Testitud standardi punkt	**Hinnang**				
Süsteemide turvanõuded (10.1)	**A**	**B**	**C**	**D**	**Lõplik**
Nõue: *Kõik turvanõuded, kaasa arvatud taandemeetmete vajadus, tuleks piiritleda projekti nõuetejärgus ning põhjendada, kokku leppida ja dokumenteerida ühe osana infosüsteemi üldisest tööülesandest.*	**3**	**3**	**2**	**2**	**2**

Allikas: /autor/

Soovitus nr. 1: *Soovitame läbi viia riskianalüüs uute tarkvarade ning suurte muudatuste korral olemaolevatesse tarkvaradesse tagamaks, et süsteemi käitlemisega kaasnevad riskid on piisavalt maandatud ning tagada seeläbi vastavus standardile ISO/IEC 17799. Soovitame riskianalüüsi läbi viia peale igat suuremat muudatust ning analüüsida ka kontrollfunktsioonide vajadust hetkel ja tulevikus. Kontrollfunktsioonide disaini varajasem planeerimine ja analüüs tagab kontrollide toimivuse ning ka madala rakendamise kulu .*

2.5.2 Turve rakendussüsteemides

Standardi punkt 10.2. ja selle alapunktid kirjeldavad nõudeid, mida tuleks rakendada kontrollimaks infosüsteemi sisestatud andmete kvaliteeti sisestamise ajal ja sisestamise järgselt. Kontrolle teostades selgus, et süsteemi on sisse ehitatud erinevaid kontrolle andmete sisestamisel ja järelkontrolle ning need on ka reaalselt toimivad. Siiski iga infosüsteemi elutsükli juurde kuulub pidev uuendamine ja arendamine, et olla vastavuses organisatsiooni töökeskkonna muudatustega nii protsessides kui pakutavas teenuses. Sellest tulenevalt on oluline kontrollida ka sisseehitatud kontrollide toimivust peale uute arenduste või muudatuste rakendamist süsteemides.

Tabel 7

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.2.

Testitud standardi punkt	**Hinnang**				
Sisemise töötluse reguleerimine (10.2)	**A**	**B**	**C**	**D**	**Lõplik**
Nõue: *Rakendussüsteemidesse, sealhulgas kasutajate kirjutatud rakendustesse, tuleks kavandada sobivad turvameetmed ja kontrolljäljed või tegevuselogid. Need peaksid hõlmama sisendandmete, sisemise töötluse ja väljundandmete valideerimist.*	**4**	**3**	**4**	**3**	**3**

Allikas: /autor/

Soovitus nr. 2: *Suurte muudatuste ning arenduste korral olemaolevasse infosüsteemi soovitame testida ka sisseehitatud kontrollide toimivust tagamaks, et süsteemi rakendatud muudatused ei ole kontrollide funktsionaalsust muutnud või halvanud. Lisaks tagab tegevuse läbi viimine vastavuse standardile ISO/IEC 17799.*

Ekspert 1

Suurima puudusena tõi ekspert välja infosüsteemi töökiiruse pideva jälgimise puudumise. Jälgimine tuleks tema hinnangul automatiseerida ja muuta nähtavaks kõigile IT osakonna töötajatele, kasutades selleks spetsiaalset monitooringu tarkvara. Ekspert hindab monitooringu tarkvara kasutuselevõtu kulu suhteliselt madalaks, kuna võimalik on kasutada ka vabavaralisi lahendusi. Veel juhib ekspert tähelepanu ühele kitsaskohale, milleks on serverisse faili laadimine. Ekspert soovitab kasutusele võtta meetmed, mis tõkestaksid serverisse laadimist peale eelseadistatud limiidi täitumist. Meetmete rakendamine on eksperdi hinnangul oluline, kuna piirangute mitteseadmine loob ohu, et pahatahtlikud isikud võivad sooritada ründe, laadimaks serverisse suuremahulisi faile eesmärgiga võrguliiklust liigselt koormata.

Tabel 8

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.2.

Testitud standardi punkt	**Hinnang**				
Sisemise töötluse reguleerimine (10.2)	**A**	**B**	**C**	**D**	**Lõplik**
Nõue: *Rakendussüsteemidesse, sealhulgas kasutajate kirjutatud rakendustesse, tuleks kavandada sobivad turvameetmed ja kontrolljäljed või tegevuselogid. Need peaksid hõlmama sisendandmete, sisemise töötluse ja väljundandmete valideerimist.*	**4**	**3**	**3**	**3**	**3**

Ekspert 2

Ekspert leidis rakendatud meetmed olevat piisavalt head, kuid peamise probleemina nägi järelkontrolli puudumist. Infosüsteemis tuleks standardi kohaselt ning eksperdi hinnangul testida rakendatud kontrollide toimivust peale arendusi ja suuremaid muudatusi, kuna muudatused võivad halvata rakendatud kontrollide disaini ja/või ülesehitust. Sama puuduse tuvastas ka töö autor.

Tabel 9

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.2.

Testitud standardi punkt	Hinnang				
Sisemise töötluse reguleerimine (10.2)	**A**	**B**	**C**	**D**	**Lõplik**
***Nõue**: Rakendussüsteemidesse, sealhulgas kasutajate kirjutatud rakendustesse tuleks kavandada sobivad turvameetmed ja kontrolljäljed või tegevuselogid. Need peaksid hõlmama sisendandmete, sisemise töötluse ja väljundandmete valideerimist.*	**4**	**4**	**3**	**3**	**3**

Kokkuvõte

Kokkuvõtvalt tuvastasid autor ja eksperdid peamise puudusena kontrollide toimivuse valideerimise puudumist peale arendusi ja suuremaid muudatusi infosüsteemis. Autori hinnangul on tegemist ühe olulisema puudusega, kuna kirjeldatud kontrolli mitteläbiviimine loob võimaluse, et muudatus annulleerib kõik või osa infosüsteemis rakendatud kontrollidest organisatsiooni teadmata. Lisaks tuvastas ekspert 1 olulise puudusena, et puudub infosüsteemi päringute kiiruse pidev jälgimine. Eelpool nimetatud puudusega on nõus ka autor, kuid autor ei sõnasta puudust soovitusena, kuna viimane ei ole otseselt seotud käesoleva töö temaatikaga ja käsitletava standardi punktiga. Lisaks tuvastas ekspert 1 puuduse faili serverisse laadimisel. Nimelt leidis ekspert 1, et üles laadimine tuleb katkestada, kui on jõutud faili suuruse piiranguni. Kuna autor ei ole läbi viidud testide käigus veendunud, kuidas rakendub mahu piirang, jääb tuvastatud puudus lahtiseks ja sellest autor soovitust ei sõnasta. Autori ja kahe eksperdi hinnang suutvusküpsusmudel alusel erines kohati, kuid lõplik hinne oli kattuv.

Tabel 10

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.2.

Sisemise töötluse reguleerimine (10.2)	A	B	C	D	Lõplik
***Nõue**: Rakendussüsteemidesse, sealhulgas kasutajate kirjutatud rakendustesse, tuleks kavandada sobivad turvameetmed ja kontrolljäljed või tegevuselogid. Need peaksid hõlmama sisendandmete, sisemise töötluse ja väljundandmete valideerimist.*	**4**	**3**	**3**	**3**	**3**

2.5.3 Arendus- ja tugiprotsesside turve

Standardi punkt 10.5.1 kirjeldab kontrolle ja nõudeid muudatuste ohje protseduurile. Auditi protseduure läbi viies selgus, et organisatsioon oli loonud muudatuste halduse protseduuri, mis katab enamuse standardis esitatavaid nõudeid ja kirjeldab protsessi kontrollikohtasid. Testides protsessi reaalset toimimist, tuvastas autor mitmeid vajakajäämisi standardi ja organisatsioonis kehtestatud protseduuri nõuete täitmisel. Muuhulgas ei analüüsitud muudatuse tellimise faasis mõju infosüsteemis rakendatud kontrollidele ning muudatuste tellimusi esitati tagantjärele.

Lisaks ei dokumenteeritud muudatuste funktsionaalsuste testimiste tulemusi ning protsessi piisavalt detailselt, mis loob ohu, et rakendatakse infosüsteemi töökeskkonda muudatusi, mille funktsionaalsuse korrektses toimimises ei ole piisavalt detailselt organisatsiooni poolt veendutud.

Kaks eespool kirjeldatud juhtumit loovad autori hinnangul ohu, et rakendatud muudatused halvavad infosüsteemi olulise(d) kontrolli(d) ning sellest tulenevalt võib organisatsioon saada vigaste andmete või andmete paljastumise tõttu mainelist ja/või rahalist kahju. Autori hinnangul on oluline testida kriitilised kontrollid, rakendades selleks automaatseid funktsionaalsuse teste, kuna funktsionaalsuste manuaalne täielik testimine peale igat muudatust oleks organisatsioonile liiga aja- ja ressursikulukas. Autori hinnangul aitaks infosüsteemi arenduste ja muudatuste halduse protseduurist tulenevaid riske maandada uute muudatuste või arenduste võimaliku mõju analüüsi metoodika välja töötamine ja juurutamine.

Auditi käigus tuvastati ka üks muudatus, mille oli kiitnud heaks arendusjuht, kuid arvestades muudatuse rahalist väärtust, oleks selle pidanud kiitma heaks muudatuste haldus- ja arenduskomitee. Vastav heakskiitmise nõue oli kirjeldatud organisatsiooni muudatuste haldus- protseduuris. Nõude mitterakendamine loob ohu, et ressursse kasutatakse ebaotstarbekalt, kuna tellitakse kulukaid muudatusi, mida organisatsioon tegelikkuses ei vaja.

Tagamaks väheste vigadega ning kvaliteetset muudatuste halduse protsessi on autori hinnangul oluline täita kõiki standardi nõudeid.

Standardi punktis 10.5.5 on välja toodud kriitilisemad kohad tarkvaraarenduse teenuse sisseostmise korral. Nõuete täitmise kontrolli käigus selgus, et määratud oli omandiõigus käsitletava organisatsiooni kasuks, kuid määramata koodi üleandmise viis ja protseduur. Lisaks ei olnud lepingus määratud nõudeid koodi kvaliteedile ega ka arvestatud juhtu, kui oleks vajadus vahetada teenusepakkujat. Tuvastatud puudujäägid

loovad ohu, et organisatsioonil tekib sõltuvus konkreetsest teenusepakkujast, kuna organisatsioon ei oma uuendatud koodi või ei ole kood arusaadav alternatiivsele teenusepakkujale. Eelnimetatud probleemid võivad omakorda luua seisaku infosüsteemi tavapärases arendus- ja muudatuste halduse tsüklis. Leping ei sisaldanud ka organisatsioonipoolset õigust arendaja tööprotsesse auditeerida, mis omakorda läbi mittekvaliteetse arendamise loob võimaluse salajaste andmete ja või koodi avalikustumiseks ning ka planeerimata tööseisakute tekkeks.

Tabel 11

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.5.

Testitud standardi punkt	**Hinnang**				
Arendus- ja tugiprotsesside turve (10.5)	**A**	**B**	**C**	**D**	**Lõplik**
***Nõue**: Infosüsteemide rikkumise vältimiseks peaks muutuste teostamine olema range kontrolli all. Tuleks kehtestada formaalsed muutuseohje sundprotseduurid. Need peaksid tagama, et ei rikutaks turbe- ja ohjeprotseduure, et tugiprogrammeerijatele antaks juurdepääs ainult neile süsteemi osadele, mis on vajalikud nende tööks, ning et iga muudatuse kohta saadaks formaalne nõusolek ja kinnitus.*	**4**	**4**	**4**	**2**	**2**

Soovitus nr. 3: *Soovitame regulaarselt kontrollida mudatuste halduse korra reaalset täitmist. Kontrolli käigus peaks veenduma, et kõike muudatuste halduse korras sätestatut ka reaalset täidetakse.*

Soovitus nr. 4: *Soovitame kajastada protseduurid partneri vahetuseks ka lepingus tarkvaraarendajaga. Lisaks peaks protseduur sisaldama ka koodi üleandmise viisi ja regulaarsust. Samuti peaks sisalduma ka õigus auditeerida arenduspartneri tööprotsessi ning koodi kvaliteeti reguleerivad parameetrid. Analüüsida soovitame ka võimalikku mõju süsteemis rakendatud kontrollidele tagamaks, et testitakse nii uut funktsionaalsust kui ka viimase mõju juba olemasolevale keskkonnale. Suurema kindluse saamiseks standardfunktsionaalsuste toimivuses soovitame testimised automatiseerida.*

Ekspert 1

Ekspert 1 leidis, et rakendada tuleks kõiki standardi punktis 10.5.1 loetletud nõudeid, kuna tema hinnangul moodustavad need olulise osa muudatuste halduse protsessist. Ekspert leidis, et oluline oleks täiendada muudatuste halduse protseduuri või välja töötada teine protseduur, mis kirjeldaks kiirmuudatuste protsessi. Põhjenduseks tõi ekspert asjaolu, et reaalsuses on vajadus teha kiireloomulisemaid muudatusi, mille heakskiitmise kiirusest võib sõltuda süsteemi töötamine või mittetöötamine ehk ka äriline kahju. Kiirmuudatus tuleb siiski kiita heaks ja autoriseerida nagu tavapärane muudatus. Tagamaks seda, et kiirmuudatusi ei viidaks läbi autoriseerimata või autoriseerituna selleks mittevolitatud isikute poolt, tuleb defineerida vastutusalad ja ka protsess.

Ekspert leidis, et kõiki punktis 10.5.5 loetletud alapunkte on vaja täita, kuid riskantsemad puudused tulenevad punktide c – e mittetäitmisest. Tema arvates tuleks vastavalt heale tavale ja parimale praktikale lisaks deponeerimise protsessi määratlemisele defineerida ka protsess koodi haldamiseks. Eksperdi hinnangul võib ilma haldusvahendi defineerimise ja kasutuselevõtuta koodist arusaamine ja ühtlasi seoste tekitamine osutuda väga keeruliseks ning aeganõudvaks protsessiks.

Tabel 12

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.5.

Testitud standardi punkt	**Hinnang**				
Arendus- ja tugiprotsesside turve (10.5)	**A**	**B**	**C**	**D**	**Lõplik**
***Nõue**: Infosüsteemide rikkumise vältimiseks peaks muutuste teostamine olema range kontrolli all. Tuleks kehtestada formaalsed muutuseohje sundprotseduurid. Need peaksid tagama, et ei rikutaks turbe- ja ohjeprotseduure, et tugiprogrammeerijatele antaks juurdepääs ainult neile süsteemi osadele, mis on vajalikud nende tööks, ning et iga muudatuse kohta saadaks formaalne nõusolek ja kinnitus.*	**4**	**4**	**3**	**2**	**2**

Ekspert 2

Ekspert leidis, et kõige olulisem puudujääk standardi nõuete punktis 10.5.1 on muudatuste halduse protsessi organisatsioonipoolse meetrika puudumine. Nimelt leidis analüüsija, et oluline on järjepidevalt veenduda protsessi järgimises või mittejärgmises

organisatsioonis. Protsessi jälgides ja edukust mõõtes on eksperdi hinnangul võimalik leida vajakajäämisi ning kohandada protsessi organisatsiooni käitumisele vastavaks. Teine võimalus on siduda muudatuste halduse protsessi järgimise kvaliteet töötajate edukusnäitajatega ja tekitada seeläbi töötajates motivatsioon käituda vastavalt kehtestatud protseduurile.

Eksperdi arvates on standardi punktis 10.5.5 olulisem puudujääk koodiauditi järjepidevuses. Nimelt leiab analüüsija, et usaldades täielikult arenduspartnerit koodi kvaliteedis võib tulemuseks olla ebakvaliteetne kood ning ühtlasi aeglaselt toimiv või mittefunktsionaalne infosüsteem. Ekspert leiab, et organisatsioonil tuleks sisemiselt hinnata aastast koodi mahtu ning jagada see mõttelisteks osadeks ning auditeerida valikuliselt eelnevalt jagatud koodi osasid, kuna kogu aasta jooksul genereeritud koodi auditeerimine võib osutuda ebaefektiivseks ning organisatsioonile äärmiselt kulukaks. Lisaks soovitab ekspert arendajast tulenevate riskide maandamiseks kaaluda funktsionaalsuste automaattestide rakendamist, kuna tema hinnangul on vaid sellisel viisil võimalik tagada infosüsteemi peamiste funktsionaalsuste toimimine.

Tabel 13

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.5.

Testitud standardi punkt	**Hinnang**				
Arendus- ja tugiprotsesside turve (10.5)	**A**	**B**	**C**	**D**	**Lõplik**
***Nõue**: Infosüsteemide rikkumise vältimiseks peaks muutuste teostamine olema range kontrolli all. Tuleks kehtestada formaalsed muutuseohje sundprotseduurid. Need peaksid tagama, et ei rikutaks turbe- ja ohjeprotseduure, et tugiprogrammeerijatele antaks juurdepääs ainult neile süsteemi osadele, mis on vajalikud nende tööks, ning et iga muudatuse kohta saadaks formaalne nõusolek ja kinnitus.*	**4**	**3**	**2**	**2**	**2**

Kokkuvõte

Standardi punktis 10.5.1 ja 10.5.5 analüüsi käigus leidsid nii autor kui ka ekspert 1, et on vaja defineerida deponeerimise protsess juhuks, kui tekib vajadus vahetada arendajat. Autori hinnangul tõi ekspert 1 välja olulise aspekti, viidates vajadusele deponeerimise protsessi käigus pöörata tähelepanu ka koodi haldamise vahendile, kuna

ilma korraliku koodihaldusvahendita ei ole võimalik koodi uuel arendajal mõistliku aja jooksul arendama hakata. Lisaks leidis ekspert 1 et on vaja defineerida kiirmuudatuste protsess, et tagada selle turvalisus. Tuvastatud puuduse ja soovitusega nõustub ka autor.

Ekspert 2 leidis esimese vajakajäämisena järjepideva kontrolli puudumise muudatuste halduse protsessi üle. Sarnase puuduse leidis ka autor ning see on esitatud juba eelpool autoripoolse soovitusena. Ekspert 2 leidis, et välise arenduspartneri puhul tuleks koodi auditit teha tihemini. Efektiivsemaks auditeerimiseks soovitas ekspert jagada aasta peale genereeritud kood mõttelisteks osadeks ning auditeerida koodi osasid valikuliselt. Autor nõustub koodi auditeerimise vajadusega ning lubab soovituse organisatsioonile edastada. Kuna koodiaudit on üsna ajamahukas ja kulukas teenus, siis autor kahtleb, et organisatsioon selle ette võtab.

Järgnevalt esitab autor ekspertide lisasoovitused ning lõpliku hinde suutvusküpsusmudeli alusel. Arvesse on võetud ekspert 1, ekspert 2 ja autori poolt suutvusküpsusmudeli alusel antud hinnanguid. Kõikidest antud hinnetest on võetud aritmeetiline keskmine. Tulemus ümardatakse alates 0,5 suurema väärtuse kasuks.

Tabel 14

Hinnang suutvusküpsusmudeli alusel standardi punktile 10.5.

Testitud standardi punkt	**Hinnang**				
Arendus- ja tugiprotsesside turve (10.5)	**A**	**B**	**C**	**D**	**Lõplik**
***Nõue**: Infosüsteemide rikkumise vältimiseks peaks muutuste teostamine olema range kontrolli all. Tuleks kehtestada formaalsed muutuseohje sundprotseduurid. Need peaksid tagama, et ei rikutaks turbe- ja ohjeprotseduure, et tugiprogrammeerijatele antaks juurdepääs ainult neile süsteemi osadele, mis on vajalikud nende tööks, ning et iga muudatuse kohta saadaks formaalne nõusolek ja kinnitus.*	**4**	**4**	**3**	**2**	**2**

Soovitus nr. 5: *Soovitame välja töötada ja juurutada tarkvara koodi deponeerimise protsess. Protsessis tuleks arvesse võtta ka koodi haldamise vahendi kasutuselevõtmist vähendamaks arenduspartnerist sõltuvust ja koodi ülesehitusest arusaamist.*

Soovitus nr. 6: *Soovitame välja töötada ja juurutada protsess kiirete muudatuste haldamiseks. Protsessi väljatöötamine ja protsessi täitmise jälgimine tagab, et ka tavapärasest kiiremaloomulised muudatused rakendatakse töökeskkonda turvaliselt.*

Soovitus nr. 7: *Soovitame kehtestada nõude koodi järjepidevalt auditeerida.*
Koodi järjepideva auditeerimisega on võimalik veenduda arenduspartneri töö ja ühtlasi koodi kvaliteedis. Töömahu vähendamiseks soovitame kood jagada aasta peale mõttelisteks osadeks ning valikuliselt neid osasid auditeerida.

2.6 Analüüsi tulemused ja ettepanekud

Analüüsi käigus tuvastasid autor ja mõlemad eksperdid mitmeid puuduseid. Standardi punkti 10.1 peamise puudusena leidsid analüüsijad vähese analüüsi infosüsteemi kontrollifunktsioonidele tarkvara arendamise analüüsi faasis. Ekspert 2 täiendas puudust täpsustusega, et hilisem kontrollifunktsioonide rakendamine infosüsteemis võib osutada äärmiselt kulukaks. Kõik eelpool välja toodud puudused formuleeriti ettepanekutena (soovitustena) organisatsiooni protsesside paremaks korraldamiseks. Lõplik hinne suutvusküpsusmudeli alusel oli 2.

Standardi punktis 10.2 leidsid autor ja ekspert 2 peamise puudusena järelkontrolli puudumise peale suuremate muudatuste ja arenduste rakendamist infosüsteemi. Standardi kohaselt peaks veenduma järelkontrolli raames infosüsteemi rakendatud kontrollide toimivuses, kuid auditi hetkeseisuga organisatsioon sellist kontrolli ei olnud läbi viinud. Ekspert 1 tõi välja olulise puudusena infosüsteemi monitooringu manuaalsuse. Tema hinnangul ei pruugi süsteemiadministraator reageerida olulistele sündmustele piisavalt kiirelt, kuna viimane ei jõua kõiki parameetreid jälgida. Kõik eelpool välja toodud puudused formuleeriti ettepanekutena (soovitustena) organisatsiooni protsesside paremaks korraldamiseks. Lõplik hinne suutvusküpsusmudeli alusel oli 3.

Standardi punktis 10.5 tuvastasid autor ja ekspert 1 vajakajäämise deponeerimise protsessi puudumises. Nimelt leidsid eelpool nimetatud analüüsijad, et tuleb välja töötada deponeerimise protsess juhuks, kui on vaja tarkvaraarendamise partnerit vahetada. Lisaks leidis ekspert 1, et organisatsioon peab looma kiirmuudatuste haldamise protseduuri, kuna auditi käigus tuvastati kiireloomulisi muudatusi, mis rakendati infosüsteemi ebaturvaliselt. Testimiste käigus tuvastati autori poolt rida muudatusi, mille käsitlemine ei vastanud kehtestatud korrale ja ega ka käsitletava standardi nõuetele. Sellest tulenevalt leidsid ekspert 2 ja autor puudusena organisatsioonipoolse kontrolli puudumise

muudatuste halduse ja arenduse protsessi toimimise üle. Lisaks soovitas ekspert 2 järjepidevat koodi auditit, sest praegusel juhul oli tegemist välise teenusepakkujaga ning muul moel ei ole võimalik arendustöö kvaliteedis ja koodi kommenteerituse astmes veenduda. Kõik eelpool välja toodud puudused formuleeriti ettepanekutena (soovitustena) organisatsiooni protsesside paremaks korraldamiseks. Lõplik hinne suutvusküpsusmudeli alusel oli 2.

Kokkuvõtvalt leidsid kõik kolm analüüsijat, et standardi rakendamisel on puudusi, kuid organisatsiooni üldpilt ei ole tegelikult halb. Eksperdid leidsid, et paljud meetmed on ka tegelikus IT keskkonna korralduses väga vajalikud ning käsitletav standard sisaldab häid mõtteid erinevate riskide maandamiseks. Autor on siinkohal ekspertidega ühel nõul. Lisaks olid autor ja mõlemad eksperdid ühel nõul selles, et käsitletava standardi punktide juurutamine teenuseportaali või isegi sotsiaalset keskkonda haldavas organisatsioonis on täiesti reaalne ja seejuures mitte väga töömahukas. Käesolevas töös käsitletud standardi punktide analüüsi tulemustele tuginedes võib väita, et on kinnitust saanud hüpotees standardi ISO/IEC 17799 (uue nimega ISO/IEC 27002) rakendatavuse kohta teenuseportaali haldavas ettevõttes. Tuginedes magistritöös läbiviidud analüüsile ja tehtud järeldustele leiab autor, et analüüsitud standardit võib rakendada mistahes keskkonda haldavas organisatsioonis korraldamaks arendus –ja muudatushalduse protsesse turvalisemalt ja efektiivsemalt.

KOKKUVÕTE

Käesolevas töös käsitletava ettevõtte ISO/IEC 17799 rakendatavuse analüüsi tulemusel selgus, et suur osa standardis sätestatud nõuetest on organisatsioonis rakendust leidnud, kuid siiski ilmnes ka mitmeid olulisi puudusi.

Standardi punkt 10.1 soovitab iga uue tarkvara või uue tarkvara funktsionaalsuse lisamise korral läbi viia riskianalüüs tuvastamaks olulisemad riskikohad ning ühtlasi võimalik kulu ühe või teise riski realiseerumisel. Intervjuu ning tarkvara disainidokumentatsiooni analüüsimise käigus selgus, et analüüsi aluseks olevas organisatsioonis detailset riskianalüüsi ei ole läbi viidud, kuid riske oli analüüsitud tarkvara kasutamislugude alusel. Autor leidis suurima vajakajäämisena riskianalüüsi puudumise ning sõnastas ka tuvastatud puudusest vastavasisulise soovituse. Ekspert 1 leidis, et organisatsioonis hetkel kasutusel olev mitteformaalne riskianalüüs võib jätta mõne olulise turvaaspekti tähelepanuta. Eelnimetatust tulenevalt soovitab Ekspert 1 metoodilise riskianalüüsi läbiviimist, mis tagaks kõikide ohukohtade kaalumise ja analüüsimise. Ekspert 2 tõi välja peamise puudusena samuti riskianalüüsi puudumise, kuid pidas oluliseks juhtida organisatsiooni tähelepanu asjaolule, et hilisem kontrollifunktsioonide juurutus infosüsteemis võib osutada liiga ajamahukaks ja kulukas või tehniliselt mitterakendatavaks. Standardi punkti 10.1 rakendamise hinnang suutvusküpsusmudeli alusel oli autoril ning ekspertidel erinev, kuid koondhinnang oli siiski väärtusega kaks.

Standardi punkt 10.2. ja selle alapunktid kirjeldavad nõudeid, mida tuleks rakendada infosüsteemi sisestatud andmete kvaliteedi kontrollimisel sisestamise ajal ja sisestamise järgselt. Autor ja Ekspert 2 tuvastasid, et auditi läbiviimise hetkeks ei olnud organisatsioon rakendanud standardi nõuet infosüsteemi kontrollide toimivuse osas peale infosüsteemi tehtud suuremaid uuendusi või arendusi. Autori ning Ekspert 2 hinnangul on tuvastatud puudus oluline tagamaks infosüsteemis rakendatud kontrollide järjepideva toimivuse. Ekspert 2 ja autor hindasid standardi punkti suutvusküpsusmudeli alusel hindega 3. Suurima puudusena tõi Ekspert 1 välja infosüsteemi töökiiruse pideva jälgimise puudumise. Jälgimine tuleks tema hinnangul automatiseerida ja muuta nähtavaks kõigile IT osakonna töötajatele, kasutades selleks spetsiaalset monitooringu tarkvara. Autor ei sõnastanud tuvastatud puudusest soovitust, kuna viimane ei ole otseselt seotud käesoleva töö temaatikaga ja käsitletava standardi punktiga. Ekspert 1 lõplik

hinnang suutvusküpsusmudeli alusel oli 3. Standardi punkti 10.2 rakendatuse taseme hinnang suutvusküpsusmudelil oli erinev nii ekspertide kui ka autoril, saades siiski koondhindeks suutvusküpsusmudeli alusel 3.

Standardi punkt 10.5.1 kirjeldab kontrolle ja nõudeid muudatuste ohje protseduurile. Auditi protseduure läbi viies selgus, et organisatsioon oli loonud muudatuste halduse protseduuri, kuid protseduuri järgmises tuvastas autor mitmeid puudujääke. Autor testis muudatuste protsessi järgimist valitud muudatuste näitel ning tuvastas muudatusi, mille mõju infosüsteemis rakendatud kontrollidele ei olnud organisatsioon analüüsinud muudatuse tellimise faasis ning muudatusi, mille tellimused olid esitatud peale muudatuse valmimist. Lisaks tuvastas autor, et muudatuste funktsionaalsuste testimiste tulemusi ning protsessi ei dokumenteerita piisavalt detailselt, mis loob autori hinnangul ohu infosüsteemi töökeskkonda vigaste muudatuse rakendamiseks. Autori ning Ekspert 2 hinnangul osutavad tuvastatud puudused organisatsioonipoolse protsessi järgimise kontrolli ebaefektiivsusele. Ekspert 1 leidis olulise puudujäägina kiirmuudatuste protsessi puudumise. Ekspert 1 hindas, et tuvastatud puudused muudatuste halduse protsessis annavad indikatsiooni hetkel kasutusel oleva protsessi puudustest. Ekspert 1 soovitas välja töötada kiirmuudatuste protsess tagamaks seda, et kiireloomulisemaid muudatused saaksid samuti autoriseeritud.

Standardi punktis 10.5.5 on välja toodud kriitilisemad kohad tarkvaraarenduse teenuse sisseostmise korral. Nõuete täitmise kontrolli käigus tuvastas autor, et lepingus tarkvaraarendajaga oli määratud koodi omandiõigus käsitletava organisatsiooni kasuks, kuid määramata oli koodi üleandmise viis ja protseduur. Lisaks ei defineeritud lepingus nõudeid koodi kvaliteedile ega arvestatud vajadusega tarkvaraarenduspartnerit vahetada. Autori hinnangul viitavad puudujäägid olukorrale,, kus tarkvaraarenduspartnerist sõltuvus on äärmiselt suur. Autor hinnangul on oluline fikseerida protseduurid partneri vahetuseks tarkvaraarendajaga, kus muuhulgas tuleks reguleerida koodi üleandmise viisi ja regulaarsust. Samuti tuleks autori hinnangul lisada lepingusse punkt, mis tagab organisatsioonil õiguse auditeerida arenduspartneri tööprotsessi ning koodi kvaliteeti jooksvalt. Ekspert 1 soovitas lisaks deponeerimise protsessi määratlemisele defineerida ka protsess koodi haldamiseks. Eksperdi hinnangul võib ilma haldusvahendi defineerimise ja kasutuselevõtuta koodist arusaamine ja ühtlasi seoste tekitamine osutuda väga keeruliseks ning aeganõudvaks. Ekspert 2 leidis, et oluline on koodi järjepidevalt auditeerida tagamaks kvaliteetset koodi ning ühtlasi kiirelt toimiva ja funktsionaalse infosüsteemi.

Autori ning ekspertide lõplik hinnang valdkonnale suutvusküpsusmudeli alusel oli kaks, mille tulemusel oli kogu valdkonna koondhinne samuti 2.

Kokkuvõttes leidsid autor ja eksperdid, et analüüsi aluseks oleval organisatsioonil oli standardi rakendamisel mitmeid puudusi, kuid sellest hoolimata oli üldpilt rahuldav. Autor leiab, et käesolevas töös käsitletud standardi punktide analüüsi tulemustele tuginedes võib väita, et on kinnitust saanud hüpotees standardi ISO/IEC 17799 (uue nimega ISO/IEC 27002) rakendatavuse kohta teenusteportaali haldavas ettevõttes. Lisaks leidsid autor ja eksperdid, et käsitletava standardi rakendamine aitab maandada mitmeid riske, mida standardi järgimiseta võib olla raske hoomata. Tuginedes magistritöös läbi viidud analüüsile leiab autor, et käsitletavat standardit võib rakendada mistahes virtuaalset keskkonda haldavas organisatsioonis korraldamaks arendus –ja muudatushalduse protsesse turvalisemalt ja efektiivsemalt.

Töö edasiarendusena võiks autori hinnangul proovida käsitletava standardi juurutamist mistahes teenusteportaali või sotsiaalset keskkonda haldavas ettevõttes või organisatsioonis.

KASUTATUD KIRJANDUS

1. Eesti Standardikeskuse tehniline komitee (EVS TK4) (1999). „EVS-ISO/IEC TR 13335-2:1999".

2. Eesti Standardikeskuse tehniline komitee (EVS TK4)(2003). „EVS-ISO/IEC 17799:2003".

3. Kivimaa, J. (2004). „Turvaanalüüsi metoodikate hindamine ja astmelise etalonturbe juhendmaterjal". [http://www.riso.ee/et/files/Astm_etalonturve_vers2_JK.pdf]

4. Software Engineering Institute (SEI) (1987). " „A Method for Assessing the Software Engineering Capability of Contractors"". [http://www.sei.cmu.edu/reports/87tr023.pdf]

5. Riigi Infosüsteemide Arenduskeskus (RIA)(2006). "Infosüsteemide kolmeastmelise etalonturbe süsteem ISKE". [http://www.ria.ee/public/ISKE_rakendusjuhend_2006_2_01_23112006.doc]

6. Bureau of Justice Statistics (BJS) (2005). "National Computer Security Survey". [http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=41]

7. COORDINATION OF FEDERAL INFORMATION POLICY (44 U.S.C § 3542 (b)(1))(2006).

8. National Institute of Standards and Technology (NIST) (1995). "An Introduction to Computer Security: The NIST Handbook". [http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf]

9. ISACA (2010). "Standardid, suunised ja protseduurid infosüsteemide auditeerimise ja juhtimise spetsialistidele". [http://www.eisay.ee/vvfiles/2/ISACA_standardid_suunised_protseduurid.pdf]

10. Kivimaa, J. (2008). Loengukonspekt "Infoturbe korraldamine organisatsioonis".

11. Riigi Infosüsteemide Arenduskeskus (RIA) (2004). “Infoturbe juhend “. [http://www.ria.ee/public/Infoturbe_soovituste_juhend_v1.pdf]

12. National Institute of Standards and Technology (NIST) (2003). “Guide to Selecting Information Technology Security Products”. [http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf]

Lisa 1

Suutvusküpsusmudeli hinnatavad valdkonnad ja nende tõlgendused

Iga kategooria pöörab tähelepanu järgnevatele aspektidele:

a. Probleemi teadvustamine ja edastamine;
b. Poliitika;
c. Poliitika juurutamise/täitmise jaoks vajalikud protsessid ja koolitused;
d. Poliitikate ja seotud protsesside tulemuslikkuse mõõtmine ning toetudes mõõdetule parenduste tegemine.

0 Puudub täielikult

a. Organisatsioon ei ole probleemi teadvustanud, seega ei ole probleemiga ka tegeletud (probleemi pole edastatud).
b. Probleemiga tegelemiseks ei ole olemas poliitikat.
c. Probleemiga tegelemiseks vajalikud protsessid puuduvad täielikult.
d. Probleemi jaoks ei ole olemas ühtegi mõõdikut.

1 Esialgne/Ad Hoc

a. On tõendeid, et organisatsioon on probleemi tuvastanud ja et sellega peaks tegelema, kuid puudub teabe järjekindel edastamine.
b. Viimistlemata poliitika on olemas. Seda on ebapiisavalt dokumenteeritud, avaldatud ja täide viidud.
c. Ad hoc lähenemist on kasutatud individuaalsete või üksikute eraldi juhtumite lõikes. Probleem ei ole laialdaselt kaetud.
d. Seiret viiakse läbi ainult konkreetse intsidendi puhul, kui see on tekitanud organisatsioonile kahju.

2 Korratav, kuid vaistlik

a. On olemas üleorganisatsiooniline probleemile vastav teadlikkus probleemi olemasolust.
b. On olemas selge/arusaadav poliitika
c. Seotud protsessid on ametlikul tasandil kindlaks tehtud probleemi läbivalt ning juhatus on aktiivselt seotud ja omab probleemist ülevaadet, kuid neid protsesse ei kasutata üleorganisatsiooniliselt. Standardeid puudutav koolitus ja kommunikatsioon puuduvad, vastutab üksikisik.
d. Juhatus on identifitseerinud baasmõõdikud ja hindamismeetodid- ning tehnikad, need on täiendamisel.

3 Defineeritud protsess

a. Vajadus probleemiga tegeleda on üleorganisatsiooniliselt arusaadav ja aktsepteeritud.
b. Eksisteerib selge/arusaadav poliitika mis on ühildatud teiste samalaadsete poliitikatega. Riskijuhtimist esineb mõningal määral.
c. Protsessid on üleorganisatsiooniliselt ühtlustatud, dokumenteeritud ja enamjaolt juurutatud. Juhatus on edastanud standardiseeritud protsessid ning loodud mitteametlikud koolituse alused. Kuigi mõõdetavad, ei ole protsessid kõrgetasemelised, kuid siiski omandatud praktikate formaliseerimine
d. Seotud tegevuste soorituse näitajaid säilitatakse ja järgitakse, mis omakorda tagab parenduste elluviimist. Enamust seotud protsessidest jälgitakse paralleelselt mingi (baas)mõõtesüsteemiga, kuid mistahes erinevus, kuigi individuaalsel initsiatiivil reageeritakse, jääks juhatusel märkamata. Põhjuste süvaanalüüsi viiakse läbi juhuslikult/mõnikord.

4 Juhitud ja mõõdetav

a. Olemas täielik arusaamine probleemist igal vajalikul tasemel, nõutavad tegevused on teada.
b. Eksisteerib selge/arusaadav poliitika mis on ühildatud teiste samalaadsete eeskirjadega. Riskijuhtimisega on arvestatud.

c. On selgelt arusaadav, kes on klient ja kohustused/vastutus on defineeritud. Protsessid on piisavalt defineeritud, juurutatud ja üleorganisatsiooniliselt kasutatud. Protsessi valdaja/vastutaja on välja selgitatud ja toetab ametlik koolitus. Kõik protsessiga seotud osapooled on protsessi riskidest ja tema poolt pakutavatest võimalustest teadlikud.
d. Seotud protsesside parendus/täiustus on eelkõige seotud kvantitatiivse käitumisega ning on võimalik jälgida ja mõõta protseduuride ja protsesside mõõdikute ühilduvust. Juhatus on paika pannud seotud protsesside toimimise taluvuspiirid. Paljudel, kuid mitte kõigil juhtudel, kus protsessid ei toimi tõhusalt või otstarbekalt on rakendatud erinevaid meetmeid/tegevusi. Seotud protsesse parendatakse aegajalt ning kehtestatakse/kohaldatakse parimat sisemist praktikat. Põhjuste süvaanalüüsi läbiviimist standardiseeritakse. Pööratakse tähelepanu jooksvale parendustegevusele.

5 Optimeeritud

a. Eksisteerib arenenud ja progressiivne arusaamine probleemist ja lahendusest.
b. Eksisteerib selge/arusaadav kehtiv poliitika, mis on täielikult integreeritud teiste samalaadsete eeskirjadega ning arvestab täielikult riskijuhtimisega.
c. Seotud protsessid on viimistletud parima välispraktika tasemele, võttes aluseks pideva täiustamise tulemused ja teistes organisatsioonides toimivaid suutvusküpsuse mudeleid. Seotud protsesside riskid ja aruanded on defineeritud, tasakaalus ja edastatud üleorganisatsiooniliselt. Koolitused ja kommunikatsioonid on ajakohastatud. Poliitikate juurutamine on sellisel tasemel, et organisatsioon, inimesed ja protsessid on kiired omandama ja täielikult toetama muutusi riskide struktuurides.

Seire, enesehindamine ja probleemi kommunikatsioon on (vajalikul määral) organisatsioonis laialt levinud ning mõõdikute, analüüside, kommunikatsiooni ja koolituste toetamiseks kasutatakse optimaalselt protsesse ja tehnoloogiaid. Kõigile probleemidele ja kõrvalekalletele tehakse süvaanalüüs ning leitakse ja kohaldatakse viivitamatult otstarbekas tegutsemisviis. Juhendamise/nõustamise eesmärgil kasutatakse väliseksperte ja *benchmarking*-ut.

APPLYING ISO/IEC 27002 STANDARD IN AN ORGANISATION MANAGING SERVICE PORTAL

M.MÄE SUMMARY

With the production of first personal computers and business oriented software a new phenomena in the form of cyber crime was initiated. Unfortunately, new and positive inventions often bring along the activities of destructively minded people. In IT world, these computer enthusiasts are referred to as crackers. Crackers are to be blamed for the massive spreading of computer viruses, malware and spam. According to a survey carried out in in USA in 2005, 67% of enterprises acknowledged that they had suffered from cyber crime in a way or other. Average loss for the enterprise was estimated around 10,000 USD.

The increased activity of crackers was the reason why the new IT field, called IT security was developed. Generally competing companies would not reveal information about the development of their technologies and its implementation – to this rule there is one exception - information security. In order to better and more efficiently fight hackers, big groups and companies have united their efforts to create various security forums in order to fight against cyber crime and crackers.

In order to organise and regulate the matters of information security many standards and collections of best practices have been compiled. For example ISO/IEC organisation has compiled standards with numbers 17799 and 13335. German Federal Office for Information Security (BSI) has issued guidance for organising information security, which is also the basis for Estonia's local security standard ISKE. At the moment there is no single standard that is applicable in every type of organisation.

The aim of this paper is to present the compliance analysis of a service portal managing organisations' IT development and change management processes with ISO/IEC 17799 standard and to answer the question whether this standard is applicable in this organisation. Author wishes to give insight to work process and issues of implementing and auditing a security standard. The fact that the standard was renamed into ISO/IEC 27002 after the audit had been carried out, is reflected also in the title of

the paper. As the organisation was following the old standard with the number of 17799, the old name is mentioned throughout this paper.

A sample of standard categories is followed in the course of the analyses. Info was gathered in the form of interviews and controls testing by author. Author described the situation to two experts, who like author, compared the situation against ISO/IEC 17799 standard requirements and brought out the most important problems. In order to get an idea of the current compliance with ISO/IEC 17799, every standard category analysed was evaluated against the Capability Maturity Model (CMM) by experts and author. Author summed up the results of the experts and of his own analysis and presented the final results in the form of recommendations and arithmetical average of CMM values given by author and experts for all standard categories analysed. As a result the author draw the conclusion whether the standard is implemental in such organisation. Analyzing the selection of categories of ISO/IEC standard number 17799 several deficiencies were identified:

According to the point 10.1 of the standard risk analysis should be carried out after every major change in or new software implementation in order to identify significant risk areas and possible cost if the scenario might occur. Author identified that such a risk analysis had not been carried out, the same issue was identified and pointed out by two experts. Final CMM value for area 10.1 was two.

Point 10.2 of the ISO/IEC 17799 standard suggests that various insertions and after- insertion controls should be implemented for controlling the quality of inserted data. Author and Expert 2 identified the biggest deficiency in the fact that the organisation did not check implemented controls workability after major changes implementation in system. Final CMM value for standard area 10.2 was 3.

Point 10.5.1 of the ISO/IEC 17799 standard sets requirements for change management procedure. Author tested a sample of changes implemented in live system during a year and identified that on many instances the procedure had not been followed and that the testing-results were not documented in detail. Author and Expert 2 were on the opinion that the issues identified point to weak monitoring of change-management process operational effectiveness in the organisation. Based on the issues identified, Expert 1 suggested that emergency change procedure was to be developed and implemented.

Point 10.5.5 of the ISO/IEC 17799 standard points out significant areas of risk when outsourcing development activities. Author identified that the contract between the

organisation and the developing company did not regulate program code management. Author and Expert 1 pointed out as critical factor the fact that contract did not include procedures for terminating the contract e.g. change of developing company In addition to that Expert 1 suggested that a process for managing the code in-house should be developed and implemented. Expert 2 suggested that the quality of code should be frequently audited by a third party. Final CMM value for standard area 10.5 was two.

In conclusion it can be said that despite many critical issues, that have been identified by the author and two experts the situation in the organisation can be considered satisfactory and thatb it can be possible implement the standard ISO/IEC 17799 in such an organisation.

Based on the conclusions of the analysis, performed in the paper, the author finds that this standard can be implemented in any organisation managing service portal.

Author considers that furtherer expansion for this paper could be an implementation of this standard in any other organisation that manages service portal(s) and is not following any standard or guidance as yet.