Tallinna Ülikool

Digitehnoloogiate Instituut

Infotehnoloogia juhtimine

ERP SÜSTEEMI PÄÄSUÕIGUSTE HALDUSE ANALÜÜS ETTEVÕTTE ÄRIVAJADUSTE NÄITEL

Magistritöö

Autor: Ave Kang

Juhendaja: Hillar Põldmaa

Autor:……..……...…..“……..“……. 2017

Juhendaja:……..……“……..“……. 2017

Instituudi direktor:…….……...…“……..“……. 2017

Tallinn 2017

Autorideklaratsioon

Deklareerin, et käesolev magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

…… …….

(kuupäev) (autor)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina Ave Kang (sünnikuupäev: 20. august 1975)

1. Annan Tallinna Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose:

   "ERP süsteemi pääsuõiguste halduse analüüs ettevõtte ärivajaduste näitel**“,** mille juhendaja on Hillar Põldmaa, säilitamiseks ja üldsusele kättesaadavaks tegemiseks Tallinna Ülikooli Akadeemilise Raamatukogu repositooriumis.

2. Olen teadlik, et nimetatud õigused jäävad alles ka autorile.

3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, _____

allkiri ja kuupäev

SISUKORD

Mõisted ja lühendid

ABAC - inglise keeles *Attribute Based Access Control.* Aatribuudil põhinev pääsupoliitika, rollipõhisest reguleerimisest paindlikum granulaarsematel atribuutidel põhinev (ametikoht, allüksus, sertifitseeringud, koolitus jm) meetod.

ACL - inglise keeles *Access Control List*. Pääsupiiramisloend on loetelu kasutajatest, programmidest ja/või protsessidest ning neile kinnistatud pääsuõiguste andmetest.

Autentimine - protsess, millega üks kasutaja, süsteem või muu olem saab kontrollida teise olemi väidetava identiteedi tõesust.

COBIT - inglise keeles *Control Objectives for Information and related Technology*. Info- ja sidustehnoloogia juhtimiseesmärgid algselt ISACA loodud ja praegu ITGI edasiarendatav infotehnoloogia valitsemise ja juhtimise üldtunnustatud raamstruktuur.

DAC - inglise keeles *Discretionary Access Control*. Diskretsionaarne pääsu reguleerimine, mis põhineb pääsu taotlevate subjekti(rühma)de identiteedil; infovara omanik delegeerib oma pääsuõigusi teistele subjektidele.

Facebook - populaarne (üle miljardi külastaja) ülemaailmne interneti-põhine sotsiaalvõrguteenus.

GUI - inglise keeles *Graphical User Interface*. Graafiline kasutajaliides.

Häkkimine – inglise keeles *hacking*. Tegevus infosüsteemi või võrgu turvamehhanismidest möödumiseks või nende murdmiseks.

Identiteedi haldus - mingi konteksti (näiteks süsteemi, organisatsiooni, võrgu, riigi) piires vajalike identiteetide atribuutide elutsükli, väärtuste ja võimalike metaandmete haldamise protsessid ja poliitikad.

Infoturve - riskihalduslik tegevus teabe turvalisuse säilitamiseks vastavalt organisatsiooni tegevuse eesmärkidele, sealhulgas andmekaitse realiseerimise vahend.

ISACA - inglise keeles *Information Systems Audit and Control Association*. Infosüsteemide Auditeerimise ja Juhtimise Assotsiatsioon, peaaegu kõigi majandusharude infosüsteemide audiitoreid, siseaudiitoreid, konsultante, koolitajaid, infoturbe spetsialiste ühendav autoriteetne kutseühing.

IoT - inglise keeles *Internet of Things.* Füüsiliste objektide (seadmete, toodete, taimede jms) ühese automaatse identifitseerimise ja nende virtuaalesituste võrgustuse kontseptsioon, RFID-tehnoloogia rakendamise edasiarendus; on suunatud inimese osaluse minimeerimisele andurite ja arukate liideste kasutamise laiendamise teel.

ITIL - inglise keeles *Information Technology Infrastructure Library*. Infotehnoloogia haldamise tavade ja protsesside standardite kogu.

LAN - inglise keeles *Local Area Network*. Kasutaja territooriumil piiratud geograafilisel alal (enamasti ühes hoones) paiknev arvutivõrk.

MAC - inglise keeles *Mandatory Access Control*. Mandatoorne pääsu reguleerimine, operatsioonisüsteemi puhul on subjektiks harilikult protsess või lõim, objektideks failid, kataloogid, pordid, seadmed jms, andmebaasihalduse süsteemis on objektideks tabelid, vaated, protseduurid jms;

PIN - inglise keeles *Personal Identification Number.* Isiku identifitseerimisnumber, lühike ainult kümnendnumbritest koosnev parool, laialt kasutusel rahandusasutuste süsteemides

Platvorm - tehnoloogiline alus, millele saab rajada muid tehnoloogiaid, protsesse või rakendusi.

Pärandsüsteem - kasutusel olev süsteem, mida ei täiustata ega uuendata, sest on juba saadaval või väljatöötamisel teda tulevikus asendav süsteem.

Teenusepõhine ärimudel - tarkvara tarnimise meetod: klient saab kaugpääsuga kasutada teenuseandja rakendusi.

Turvapoliitika - arvutiturbe kindlustamiseks kohaldatav plaan või tegevuskava (ISO/IEC 2382)

Sissejuhatus

Infotehnoloogia osatähtsus organisatsioonides on viimasel aastakümnel kasvanud ja võimaldab paljudes valdkondades saavutada eesmärke kiiremini ja väiksemate kuludega. Uudsete lahendustega kaasnevad teist tüüpi riskid sundides organisatsioone mõtlema, kuidas infosüsteemides sisalduvat teavet paremini kaitsta. Infosüsteemile mõjuda võivate ohtudega tuleb arvestada juba projekteerimise ajal ning turvameetmete rakendamine võimaldab vähendada ning ära hoida kahjusid organisatsiooni informatsioonile.

Organisatsiooni ressursside planeerimise süsteem (*Enterprice Resource Planning*, edaspidi ERP) süsteeme peetakse viimase dekaadi kõige suuremaks infotehnoloogia arenguvaldkonnaks. ERP süsteemid pakuvad võimalusi analüüsida organisatsiooni eri tegevusvaldkondadest kokku integreeritud andmeid. Pidevalt kasvava konkurentsi tingimustes on organisatsioonid sunnitud optimeerima äriprotsesse ja alandama kulusid. Nende ülesannete üheks kõige efektiivsemaks vahendiks on ERP süsteem, mis on ette nähtud arvestuse ja juhtimise automatiseerimiseks. ERP süsteemi juurutamise eesmärk seisneb organisatsiooni töö kvaliteedi tõstmises läbi organisatsiooni tegevuse läbipaistvuse suurendamise, tootmisprotsesside optimeerimise, organisatsiooni tegevuse majanduslike tulemuste saamise automatiseerimis- ja planeerimissüsteemide kasutamise arvelt. ERP süsteem võimaldab andmeid kuvada tähenduslikult, ehk anda andmetele tähenduse, mis lihtsustab juhtimisotsuste tegemist.

Viimastel aastatel on oluliselt kasvanud organisatsioonides mure, et IT süsteemide või lahenduste kasutamisel võib lekkida konfidentsiaalne info. IT riskide mõistmise olulisusest saadakse üha paremini aru. ERP süsteemi juurutamine on keeruline projekt, mis on ajamahukas, kallis ja riskantne. Kõik ERP lahendused on organisatsiooni spetsiifilised, mis teevad süsteemi eriti keerukaks ja raskesti hallatavaks. Selliste lahendustega kaasnevad alati riskid, millele tuleks juba projekti alguses tähelepanu pöörata. Paraku, nagu kõik meie ümber, muutuvad ka ERP süsteemile seatud eesmärgid ajas, tulenevalt nii äri eesmärkide kui ärivajaduste muutumisest.

Muudatused ERP süsteemis peavad aga alati olema kooskõlas organisatsiooni standardite ja turvapoliitikatega.

Infoturve on riskihalduslik tegevus teabe turvalisuse säilitamiseks vastavalt organisatsiooni tegevuse eesmärkidele, sealhulgas andmekaitse realiseerimise vahend (Põldmaa, 2016). Pääsuõigused on infoturbe alamteema, nende haldus ja korrashoid võib olla väga mahukas organisatsioonis kus on palju töötajaid, suur tööjõu voolavus või toimub palju organisatsioonilisi muudatusi. Seadistus vead on kerged tekkima ja pääsuõiguste ülevaatuseks ei pruugi ressurssi jätkuda. Suureneb vajadus pääsuõiguste halduse korralduse lihtsustamise ja läbipaistvuse järele. Pääsuõiguste elutsükkel tuleks korralikult läbi planeerida ning vajadusel kasutusele võtta alternatiivsed pääsu reguleerimise metoodikad. Vastasel juhul võivad suure tõenäosusega realiseeruda kõrged infoturbega seonduvad riskid.

Informatsioon on iga organisatsiooni kõige väärtuslikum vara ja seda tuleks vastavalt ka kaitsta. Infoturve on kombinatsioon süsteemidest, protsessidest ja sisemistest kontrollidest tagamaks andmete käideldavuse, konfidentsiaalsuse ja tervikluse (Põldmaa, 2016). Andmed, mis on küll turvatud aga ei ole kättesaadavad autoriseeritud kasutajatele on kasutuskõlbmatud.

ERP süsteemid kajastavad organisatsioonide äritegevusega seotud informatsiooni ning tuleks käsitleda kui ärisaladust. Seega on eriti tähtis teadvustada, et ERP süsteemis sisalduv informatsioon on organisatsiooni eksisteerimiseks hädavajalik. Informatsioon on teave, mis koosneb andmetest mille tõlgendamiseks on vaja seda informatsiooni esitleda kujul, mis annab talle tähenduse (Leon, 2008).

Ettevõte tegutseb kiiresti muutuvas tegevuskeskkonnas, millest tulenevalt on pidevas muutumises nii organisatsiooni struktuur kui äriprotsessid ja infovajadused. Pääsuõiguste haldus peab selliste muudatustega käima käsikäes ja eeldab turvapoliitika olemasolu ja regulaarset uuendamist.

Tagamaks ettevõtte ERP süsteemi infoturve ning jõudmaks halduskoormust vähendava pääsuõiguste haldusprotsessini organisatsioonis püstitas autor järgmised eesmärgid:

- Anda ülevaade ERP süsteemidest, turvariskidest ning arengusuundadest.
- Anda ülevaade pääsuõiguste haldusest ja reguleerimise poliitikatest.

- Tõsta pääsuõiguste alast teadlikkust.
- Analüüsida organisatsiooni ERP süsteemi pääsuõiguste haldust ning teha saadud ülevaate põhjal ettepanekud pääsuõiguste haldusprotsessi parandamiseks.

Eesmärgist tulenevalt on töö peamised uurimisküsimused järgmised:

- Mis on ERP süsteem ning millised on enimlevinud ERP süsteemide turvariskid?
- Millega peaks pääsuõiguste elutsükli halduse puhul arvestama?
- Millised on enimlevinud pääsuõiguste halduse poliitikad?
- Kuidas toimub pääsuõiguste haldus organisatsioonis?
- Milline haldus poliitika sobib kõige paremini organisatsiooni ERP süsteemi pääsuõiguste halduseks?

Magistritöös analüüsib autor organisatsiooni pääsuõiguste halduse protsessi. Uurimuse läbiviimiseks sobib kvalitatiivne uurimismeetod, millest lähtuvalt viis autor läbi kirjanduse analüüsi ning juhtumiuuringu. Juhtumiuuring võimaldab autoril nähtust tema loomulikus keskkonnas sügavuti uurida, tuginedes mitmetele erinevatele infoallikatele. Töös tuginetakse artiklitele, raamatutele ja veebilehtedel avaldatud teabele ning tunnustatud standarditele ning metoodikatele.

Esimeses etapis teostab autor teoreetilise analüüsi, mis annab ülevaate pääsuõiguste elutsüklist, halduse protsessist ning pääsuõiguste poliitikatest.

Teises etapis viib autor läbi juhtumiuuringu mille käigus teostatakse pääsuõiguste revisjon, haldusprotsessi analüüs ning intervjuud valdkonna juhtidega. Pääsuõiguste revisjoni ning haldusprotsessi analüüsi puhul on tegu hetke-olukorrast ülevaatlikku pilti andva haldusprotsessi kaardistusega.

Magistritöö tulemuseks on terviklik pääsuõiguste halduse protsessi analüüs, mis võimaldab optimeerida halduskoormust ning vähendada infoturbe riske organisatsioonis.

Magistritöö koosneb viiest peatükist. Esimeses peatükis tutvustab autor ERP süsteeme, nende eesmärke ning põhjendab miks just ERP süsteemides pääsuõiguste eest erilist hoolt peaks kandma. Lisaks annab autor ülevaate ERP toodete pakkujatest ning toob välja mõned tuvastatud tugevused ja nõrkused. Peatüki lõpus annab autor lühiülevaate

ERP strateegiast ning arengusuundadest, eesmärgiga juhtida tähelepanu tuleviku trendidele, mis nõuavad suuremat tähelepanu pääsuõiguste osas.

Teises peatükis annab autor ülevaade ERP süsteemide riskidest, tutvustab ERP turvaraamistikku, selgitab riskide üldist jagunemist ning enimlevinud riskifaktoreid. Samuti toob autor välja mõned näited pilvepõhise ERP süsteemi turvariskidest.

Kolmandas peatükis selgitab autor pääsuõiguste mõistet ning annab ülevaate pääsuõiguste halduse printsiipidest ning raampõhimõtetest. Autor kirjeldab pääsuõiguste elutsükli haldust ning etappe. Peatüki eesmärk on tutvustada kasutajakonto halduse soovitusi ning jõuda otsuseni kuidas organisatsioonis neid soovitusi rakendada.

Neljandas peatükis kirjeldab autor erinevaid pääsuõiguste poliitikaid ning kirjeldab pikemalt rollipõhise pääsupoliitika (*Role-Based Access Control*, edaspidi RBAC) taksonoomiat, mis koosneb neljast mudelist: tuumik RBAC, hierarhiline RBAC, staatiline piiratud RBAC ja dünaamiline piiratud RBAC. Peatüki lõpus annab autor ülevaate pääsuõiguste strateegiast, mis võiks olla turvapoliitika väljatöötamise aluseks. Peatüki eesmärk on valida organisatsiooni jaoks sobivaim pääsu reguleerimise poliitika, mis võimaldaks pääsuõiguste järelevalve koormust vähendada.

Viiendas peatükis annab autor ülevaate juhtumiuuringu käigus läbi viidud pääsuõiguste revisjonist, rakendatud metoodikast ning uuringu tulemustest. Uuringu tulemusena teeb autor seitse ettepanekut organisatsiooni ERP süsteemi pääsuõiguste haldustegevuste parendamiseks.

1. ERP süsteemid

Peatükis antakse ülevaade ERP süsteemidest ning nende eesmärgist ning ülemaailmselt tuntumatest ERP toodete pakkujatest. Peatüki eesmärk on lisaks ERP süsteemide tutvustamisele, rõhutada ERP süsteemides sisalduva informatsiooni konfidentsiaalsuse ja tervikluse vajadust ning juhtida tähelepanu ERP süsteemide arengusuundadele, kus infoturbel on veelgi suurem tähtsus.

ERP on ärijuhtimise tarkvara, mis võimaldab organisatsioonil kasutada ühtsesse süsteemi integreeritud infosüsteeme ning hallata oma tegevust (Leon, 2008). ERP süsteemid integreerivad kõik organisatsiooni osakonnad ja funktsioonid ühtsesse arvutisüsteemi. Selline reaalajas integratsioon ja andmete jagamine üle organisatsiooni erinevate funktsionaalsete alade tõstab töökorraldust ning aitab juhtidel teha paremaid otsuseid (Leon, 2008). Pidevalt kasvav konkurents sunnib organisatsioone optimeerima oma äriprotsesse ja alandama kulusid. Nende ülesannete üheks kõige efektiivsemaks tööriistaks on ERP, mis on ettenähtud arvestuse ja juhtimise automatiseerimiseks.

1.1. ERP süsteemide eesmärk

ERP süsteemide eesmärk on pakkuda ühte keskset hoidlat andmetele, kindlustamaks sujuvat informatsiooni voolavust läbi organisatsiooni. See võimaldab tõsta organisatsiooni töö kvaliteeti suurendades läbipaistvust ning optimeerides tootmisprotsesse.

ERP süsteemide aluseks on ühtne andmebaas, mis sisaldab kogu korporatiivset äriinfot ja tagab sellele samaaegse juurdepääsu organisatsiooni mistahes vajalikul arvul töötajatele, kellele on antud vastavad volitused (Joonis 1).

Joonis 1. ERP süsteem (Wikipedia, ERP-süsteem, 2017)

ERP süsteemide üheks suurimaks kasuteguriks on võimekus reaalajas edasi anda organisatsioonis toimuvat. Otsesteks kasuteguriteks võib lugeda efektiivsuse kasvu ning andmete integreeritust paremate juhtimisotsuste tegemiseks. Kaudseteks kasuteguriteks võib lugeda maine kasvu ning kliendirahulolu tõusu. Selleks, et konkurentsis ellu jääda ja saavutada teatav konkurentsieelis on vaja tulevikku juhtida. Selleks aga on vaja, et juhid saaksid kvaliteetset informatsiooni juhtimisotsuste langetamiseks. Kõige paremini löövad läbi need, kes oskavad informatsiooni kasutada. Kuna informatsiooni on organisatsioonides palju ja selle läbi töötamine võtaks kaua aega, tuleb appi tehnoloogia. Iga organisatsioon kasutab mingil määral ERP süsteeme informatsiooni juhtimiseks.

1.2. ERP müüjad

Panorama Consulting Solutions poolt ajavahemikul 2012 – 2016 läbi viidud uuringust (Panorama Consulting Solutions, 2016), mille käigus koguti 1660 vastust selgus, et TOP 10 ERP müüjat ülemaailmselt jagunevad alljärgnevalt:

1. EPICOR
2. INFOR
3. SAP
4. IFS

5. ORACLE
6. NETSUITE
7. MICROSOFT
8. SAGE
9. SYSPRO
10. IQMS; (Panorama Consulting Solutions, 2016)

Samal aastal läbi viidud uuringus võrreldi lähemalt nelja ERP müüja: SAP, Oracle, Microsoft ja Infor ERP tooteid. Läbi viidud uuringus osales 519 vastanut (Panorama Consulting Solutions, 2016).

Uuringust selgus, et Oracle ERP tugevusteks peetakse eelkõige tugevat finants- ja raamatupidamis funktsionaalsust, hästi üles ehitatud IT arhitektuuri ning tootmistegevusi toetavat funktsionaalsust (Panorama Consulting Solutions, 2016, lk 4). SAP ERP puhul hinnati eriti tootmisest tellimuseni töötlemise lihtsust ning kvaliteedi tagamise funktsionaalsust (Panorama Consulting Solutions, 2016, lk 5). Samas on nii SAP kui Oracle puhul välja toodud ka mõned turvanõrkused. SAP autoriseerimise/turvalisuse mudel on kodeeritud seega ei saa turvalisust tõsta ilma koodi puutumata. Samuti ei ole sisseehitatud turvalisust kohandustele, mis võib viia probleemideni ja täiendavate jõupingutusteni turvalisuse rakendamiseks. Oracle *E_Business Suite* sisaldab endas sisseehitatud funktsioone, mida saab kasutajatele määrata vastavalt nende töökirjeldusele. Lisaks saab funktsionaalsust limiteerida defineerides välistus-nimekirju. Kui olemasolevate funktsioonide hulgas ei ole soovitud funktsionaalsust, siis ei saa arendajad moodulites seda osa ise täiendada kuna neil puudub ligipääs koodile. Nad saavad kasutada ainult standard funktsionaalsust või arendada kohandatud funktsionaalsust vahenditega, mis on Oracle poolt pakutud.

Nii SAP kui Oracle ERP tooted toetavad rolle, kuid administraator ei ole kohustatud neid kasutama. Eelnevalt määratletud või standard-rollid on väga üldised ja enamasti mitte kasutatavad. Põhjuseks fakt, et need tooted ei ole tehtud silmas pidades ühegi konkreetse organisatsiooni vajadusi ja nõudeid. (Panorama Consulting Solutions, 2016)

SAP turvalisus on täielikult tsentraliseeritud, tasub kaaluda, kas selline lahendus on parim. Oracles on turvalisuse rakendamine palju lihtsam ja paremini mõistetav, mis aitab kasutajatel planeerida, kavandada ja rakendada turvalisust.

Microsoft on tuntud oma operatsioonisüsteemide ja äritarkvara poolest, pakkudes nüüd ka ERP lahendusi igas suuruses organisatsioonidele. Tugevustena toodi välja kohanduste lihtsust, paindlikkust, tootmise ressursside planeerimise võimekust ning mitme valuuta toetust (Panorama Consulting Solutions, 2016, lk 6).

Infor pakub nii pilve- kui kliendipõhist lahendust. Infor on vähendanud kohandusi minimaliseerimaks hilisemaid probleeme haldamise ja versiooni uuendustega seetõttu on neil turul kindel positsioon. Hetkel pannakse suurt rõhku kasutusmugavusele ning nad on selles vallas saavutanud suurt edu. (Panorama Consulting Solutions, 2016, lk 6)

Epicori kõige uuem äritarkvara on Epicor ERP versioon 10, mis on eriti tugev tootmissektoris ning on nimetatud oma funktsionaalsuse ja tehnoloogia tõttu lausa järgmise põlvkonna äritarkvaraks ning on saanud mitmeid auhindu. Epicor 10-s on lisaks finantside ja logistika haldusele tervet tootmisprotsessi hõlmav tootmisprotsesside juhtimise ja haldamise lahendus. Epicor ERP on tuntud kui paindlik ja võimekas, väikese ja keskmise suurusega tootmisvaldkonnas tegutsevatele organisatsioonidele (20 kuni üle 1000 töötajat), suunatud toode. Epicor ERP põhineb täielikult Microsofti tehnoloogial ning pidevas kasvus on partnerite kompetentsi kasv, mis on tublisti suurendanud konsultantide arvu. Epicori püüdlused tõsta efektiivust ning jõudlust on kandmas vilja. Keskendutakse rohkem jõudlusele, mastaabitavusele ning tehnoloogiale kui uutele funktsionaalsustele.

IFS on avatud standarditel põhinev toode ning sisaldab üle 60 komponendi praktiliselt kõikide organisatsiooni tegevusvaldkondade haldamiseks. IFS nähtavus ja ülemaailmse tarne võimekus paranevad ning IFS näitab tugevat kasvu trajektoori. IFS tegevuskava on tugev, ühendades rohkem kaasajastamis meetmeid, mis teeb sellest tootest ühe kõige kasutajasõbralikuma ERP süsteemide turul.

Iga pakkuja ERP süsteemil on omad eelised ja tugevused. Enne valiku tegemist tasuks eelnevalt tutvuda võimalikult paljude erinevate süsteemidega ning välja töötada oma ERP strateegia.

1.3. ERP strateegia

Juhtiva analüüsifirma Gartner poolt 186 rahvusvahelise suurorganisatsiooni seas läbi viidud uuringust selgus, et ERP-süsteemist tulenevat ärilist kasu mõõdavad ainult 37% firmadest (Rayner & Woods, 2011). Seega puudub enamikul organisatsioonidest strateegiline lähenemine ERP süsteemi kasutamisele ning tarkvara töötab igapäevatöö vajadustest lähtuvalt. Üks sage viga ERP süsteemi kasutuselevõtul on, et projekti juhitakse lähtuvalt IT osakonna vajadusest – vähendamaks infotehnoloogia alaseid kulutusi ja lihtsustamaks IT protsesse. Kindlasti on see oluliseks ERP-süsteemi kasutuselevõtu eeliseks, kuid ühe osakonna huvisid ei tuleks tõsta ettepoole kogu organisatsiooni strateegilistest ärieesmärkidest. (Rayner & Woods, 2011)

ERP strateegia on igale organisatsioonile rätsepalahendus, mille koostamisel tuleb muuhulgas arvesse võtta nii organisatsiooni tegutsemisvaldkonda, ärilisi eesmärke, kui ka organisatsiooni suurust. Organisatsioonil tuleb defineerida, milliseid äriprotsesse ERP toetama hakkab. Mõned organisatsioonid kasutavad ERP-süsteemist ainult administratsiooni aspekte (finantsid, personal), seda iseäranis teenindus- ja avalikus sektoris. Tootmisettevõtete puhul laiendatakse ERP kasutusala reeglina ka tellimuste ja tarnijatega tehtava töö korraldamisse, maksimeerimaks tegevusefektiivsust. ERP-strateegia peaks lähtuma aga just äriskoobist, mitte tarkvara poolt pakutavate moodulite funktsionaalsusest. Süsteem tuleb kujundada organisatsiooni vajadustest lähtudes, mitte vastupidi. Äritarkvara valikul tuleks määratleda protsessid, mida organisatsioonis tahetakse katta, mitte äritarkvara moodulid. Seda põhjusel, et tarkvara pakub suuremaid eeliseid, kui ta suudab katta ära kogu protsessi.

Äritarkvara kasutuselevõtul peaks organisatsioon võtma aluseks strateegilise tähtsusega protsessid, eelkõige need, mis on organisatsiooni konkurentsieeliseks. Strateegiliste äriprotsesside puhul peaks ERP-süsteem olema piisavalt paindlik, et see lisaks igapäevatööle toetaks ka strateegilisi arengusuundi. Kui konkreetne ERP-toode ei suuda olulisi äriprotsesse piisava funktsionaalsusega toetada, võib tekkida vajadus lisalahendite leidmiseks väljaspool ERP süsteemi. Mittestrateegiliste äriprotsesside puhul ei ole täisfunktsionaalsus nii oluline. Gartner soovitab lisaks strateegilisele-mittestrateegilisele jaotusele jagada äriprotsessid kolmeks: ühed, mille puhul on

vajalik lihtsalt info talletamine, teised, mis eristavad turul organisatsiooni tooteportfelli ning kolmandad, mis on organisatsioonile innovaatilise tähendusega (Gartner, Inc., 2014). Oluline on, kuidas kahe viimase puhul tarkvara maksimaalselt ära kasutada. Rahvusvahelise organisatsiooni puhul on vaja eelnevalt otsustada, kas võetakse kasutusele ühine platvorm või kasutatakse ka lokaalseid lahendusi. Mõlemal on omad eelised ja leida tuleb oma organisatsioonile sobivaim lahendus.

Määratleda tuleb ERP süsteemist tulenev konkreetne kasu, mida organisatsioon ERP süsteemi kasutuselevõtust saab. Üks kasu on tüüpiliselt IT-operatsioonide efektiivsus, mis väljendub reeglina ühtse süsteemi sünergia poolt loodavast säästuefektist. Teine ERP-süsteemi kasu on info koondumine, selle läbipaistvus ja reaalajas kättesaadavus. Ärianalüüs võimaldab juhtkonnal planeerida paremini nii igapäevategevust kui töötada välja plaane järgmisteks aastateks. (Rayner & Woods, 2011)

Tähelepanu tuleks pöörata ka n-ö mitte käega katsutavatele eelistele – näiteks võib äriprotsesside standardiseerimine kärpida paberi hulka kontoris ja muuta organisatsioon seeläbi "rohelisemaks". Kõige edukamad ERP-projektid on Gartneri kogemuse põhjal sellised, mis on organisatsiooni äristrateegiaga läbi põimunud ning, mis ei ole pelgalt IT-osakonna vajaduste poolt juhitavad projektid (Gartner, Inc., 2014). Edukates organisatsioonides on ERP süsteemi kasutuselevõtul pühendunud juhtkond: juhtkonna liikmed pole lihtsalt suurprojekti reklaamnäod, vaid tegelevad sellega igapäevaselt (Rayner & Woods, 2011). Edulugudes esineb läbivalt ka ERP süsteemi kasutuselevõtu eest vastutava juhtimiskeha olemasolu (Linkies & Karin, 2011), mis koosneb organisatsiooni erinevate valdkondade ja tippjuhtkonna esindajatest ning väljastpoolt maja appi võetud ERP-konsultantidest. Viimaste puhul on oluline, et nad peavad olema piisavalt hästi kursis organisatsiooni toimimisega.

Gartner on välja toonud ka tüüpilised riskikohad, mis võivad suurtele plaanidele saatuslikuks saada. Standardimisel, mis on ühelt poolt suureks ERP süsteemi eeliseks, on ka omad riskid, sest see ei pruugi alati olla sobivaim lahendus. Oluline on tuvastada need valdkonnad ja kitsaskohad, mille puhul on vajalikud hoopis rätsepalahendused. Üks peamisi riskikohti on kasutajate poolne vastuseis ERP süsteemile, mistõttu on kriitilise tähtsusega juhtkonna pühendumus ja eeskuju näitamine. Kolmanda tüüpilise

veana kipuvad organisatsioonid ERP süsteemi tasuvusepiirini jõudmisel unustama tarkvara väärtuse ja edasised investeeringud sellesse. (Rayner & Woods, 2011)

Organisatsiooni strateegiliste ärieesmärkide toetamiseks tuleb määratleda ERP-süsteemi piirid. Defineerima peab strateegilised ja mittestrateegilised äriprotsessid. Kui osutub vajalikuks, tuleb leida ERP-väliseid lisalahendusi organisatsiooni strateegiliselt olulistele äriprotsessidele. Loetlema peaks kasu, mida organisatsioon ERP abiga saavutama peaks, ja määratlema peamised riskikohad, mis seda takistada võivad. (Rayner & Woods, 2011)

ERP, nagu ka organisatsiooni strateegia, ei saa kunagi lõplikult valmis ja peab olema pidevas muutumises lähtudes organisatsiooni ja kogu majanduse arengust.

1.4. ERP arengusuunad

Üha enam organisatsioone investeerib ERP lahendustesse eesmärgiga tagada jätkusuutlikkus konkurentsis. Lisaks suurtele organisatsioonidele kogub ERP lahendus üha enam populaarsust ka äri alustavate ja keskmise suurusega organisatsioonide seas. ERP lahenduse arengusuunad on:

Mobiilsus - IDC (*IDC Research, Inc*) poolt läbi viidud uuringust selgus, et üle 105,4 miljoni inimese kasutab mobiilset tehnoloogiat aastaks 2020 (Business Wire, 2015). Nutiseadmeid kasutatakse ärides ja töörollides, mille tulemusena turustatakse neid rohkem kui tavaarvuteid. On üsnagi tavapärane, et töömeilidele vastatakse mobiiltelefonidest, kasvanud on nõudlus töörakenduse mobiiltelefonides kasutamise järele. Enamus pakutavatest ERP süsteemidest võimaldavad kasutajaliideseid või rakendusi tahvelarvutitele või mobiiltelefonidele. Mida rohkem organisatsiooni töötajaid suudetakse ERP lahendusega siduda, kasvõi mobiilseid vahendeid kasutades, seda suurem on tootlikkus lahenduste kasutamistest. Selleks, et organisatsioonid käiksid ajaga kaasas pakuvad mobiilsed lahendused võimalust võtta vastu äriotsuseid või lahendada kriitilisi ülesandeid sõltumata asukohast. Seda nii juhtimisotsuste vastuvõtmiseks kui ka kliendi andmete või tööpostil mõõteandmete sisestamiseks.

Pilvepõhised lahendused ehk teenusepõhine ärimudel - Hiljutine rahvusvahelise uuringufirma Gartner poolt läbi viidud uuring väidab, et *ca* 2018. aastaks juurutavad või täiendavad vähemalt 30% organisatsioonidest oma ERP lahendused nö pilvepõhiselt (Gartner, Inc., 2014). Traditsiooniliste ERP lahenduste soetusmaksumused (nt litsentsid, tarkvara kindlustamine) on liiga kulukad, kasulikum (odavam) on oma strateegiad ja lahendused siduda n-ö teenusepõhiste lahendustega. Teenusepakkujad on nõudlusest tingituna juba välja töötamas erinevaid lahendusi, laiendades oma teenuste portfelli rahuldamaks erinevaid vajadusi. IT osakondadele on teenusepõhine ärimudel kergenduseks säästes neid pidevatest versiooniuuendustest ning suure hulga rakenduste haldamisest. Lisaks väikestele soetuskuludele kaob vajadus installeerimiste, käitamiste ja sisemiste süsteemide halduse järele. Kiire kasutuselevõtt ja madal soetusmaksumus meelitavad ligi väiksed ja keskmise suurusega organisatsioonid, tehes turul ruumi ka väikesematele ERP müüjatele. See omakorda on sundinud suuremaid tegijaid välja tulema uute toodetega nagu SAP *Business ByDesign* ja Oracle *on Demand*, mille sihtgruppideks on just väiksemad organisatsioonid.

Asjade internet - IoT (*Internet of Things*) ehk asjade internet on ülemaailmne trend (Jankowski, Covello, Bellini, Ritchie, & Costa, 2014), kus üha enam erinevaid tooteid või ka teenustega seotud objekte on varustatud spetsiifiliste sensoritega, mis võimaldavad lähetada vajalikku teavet, ilma inimese otsese vahelesegamiseta. See loob vajaduse, et organisatsioonid omaksid väga häid ERP lahendusi, mis suudavad seda informatsiooni voogu, mis tuleb erinevatest seadmetest süstemaatiliselt analüüsida ning seeläbi vajalikke äriprotsesse korraldada. Andmete suur hulk on organisatsioonidele suureks väljakutseks ja enne vastavate lahenduste kasutuselevõttu, tuleks kõik faktorid hoolikalt planeerida. Faktorite hulka kuuluvad nii turvalisusega seotud teemad, kui ka kulukas soetusmaksumus. ERP lahendused muutuvad n-ö trendi prognoosijateks *vs* traditsioonilise kuvandiga andmete kogujad.

Interaktiivsed kasutajaliidesed koos sotsiaalmeedia võimalustega - ERP lahenduste disain liigub suunas, et sõltumata seadmest millega seda kasutada, on lahendused kasutajasõbralikud (Boyd, 2017). Lisaks võimalused vastavalt oma rollile kujundada ise lahenduse väljanägemist. Eesmärgiks on üha rohkem organisatsiooni inimesi väiksema kuluga meelitada kasutama kogu organisatsiooni struktuurkapitali hüvesid ning seeläbi tootlikust parandada. Seda suuresti tänu veebipõhistele

lahendustele, mis võimaldavad vastavalt oma vajadustele kujundada sisestusvorme, aruandeid või graafikat.

ERP lahendusi on hakatud siduma ka sotsiaalmeedia ja võrgustiku võimalustega, mis ühendab organisatsiooni nii siseselt kui ka väliste klientidega. Tegemist on ERP sisese turvalise keskkonnaga, mis võib välja näha nagu nt Facebook, kuid on välisvõrgust turvaliselt eraldatud. Eelistena võib välja tuua nii organisatsiooni sisese kui ka klientidega kommunikatsiooni kasvu, protsesside efektiivistumise ning teadmuse säilimise organisatsioonis.

Trend liigub üha enam pilve-tehnoloogiate suunas, et luua rohkem innovatsiooni erinevate rakenduste kasutamiseks, vähendada lahenduste haldus (administreerimis) kulusid ning anda ettevõtjatele võimalus oma ärikorraldust paindlikumaks muuta. Uudsete lahendustega kaasnevad ka uued turvariskid.

Peatükis andis autor ülevaate ERP süsteemidest eesmärgiga põhjendada ERP süsteemides sisalduva informatsiooni tähtsust organisatsioonile. Eelkõige seetõttu, et ERP süsteemid annavad andmetele tähenduse, võimaldades organisatsiooni juhtidel juhtimisotsuseid teha. On väga oluline tutvuda ERP riskidega juba projekteerimise faasis ning arvestada ka ERP arengusuundadega.

2. ERP riskid

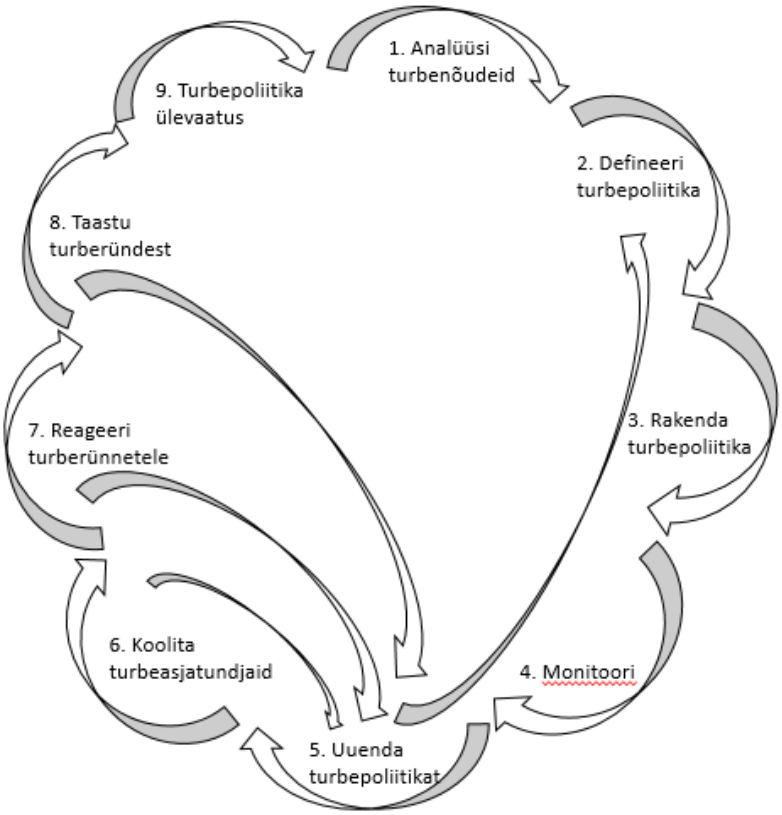
Teine peatükk keskendub ERP turvariskidele rõhutades turvaraamistiku olulisust ning ERP riskifaktoreid. Peatüki eesmärk on juhtida tähelepanu olulisusele kaasata infoturve juba süsteemi projekteerimise faasis ning tuua välja faktorid, millele tuleks süsteemi projekteerimise faasis tähelepanu pöörata. Pilvepõhise ERP süsteemi turvariskide peatükk annab ülevaate turvariskidest, mis on iseloomulikud pilvepõhist teenust kasutades.

ERP süsteemide kasutuselevõtt toob endaga kaasa mitmeid kasutegureid nagu näiteks konkurentsieelis, juhtimisotsuste kvaliteedi tõus, finantsilised kasutegurid ning sellest tulenevalt on ERP süsteemid leidnud väga laialdast kasutust. Ligipääsetavus ERP süsteemidesse käib tavaliselt läbi LAN (*Local Area Network*) arvutivõrgu või veebipõhiselt. Selliste lahenduste puhul ei ole pääsuõigused jagatud allsüsteemidele, vaid tööülesannetest lähtuvalt, seega on süsteem avatud mitmetele turvariskidele. Turvariske mõjutavad muudatuste juhtimise puudulikkus, andmete omandiõigused, kohandatud moodulid, kasutajarollide keerulisus, volitamata ligipääs andmetele ja häkkimine (*hacking*). Turvariskide ennetamiseks ja maandamiseks tasub tutvuda turvaraamistikega.

2.1. ERP turvaraamistik

ERP turvaraamistik tagab, et infoturve oleks tihedalt seotud ERP süsteemi projekteerimise, juurutuse ja talitlusega selleks, et süsteemi poolt pakutav informatsioon oleks usaldusväärne (Marnewick & Labuschagne, 2006).

Näide kõrgetasemelisest turvaraamistiku vaatest, mis on välja töötatud *Triware Networld Systems* (TNS) poolt (Joonis 2).



Joonis 2. Turvaraamistik (Triware Networld Systems, kuupäev puudub)

Turvaraamistik peaks olema kohandatud organisatsiooni ja süsteemide vajadustest tulenevalt, kaasates võimalikult palju erinevaid osapooli, eesmärgiga teha süsteem vabaks turvariskidest ja ohtudest andmete privaatsusele. Turvaraamistiku väljatöötamise eelduseks on ülevaade ERP riskidest ning nende jagunemisest.

2.2. ERP riskide jagunemine

ERP süsteemide riske saab üldises plaanis jagada vähemalt seitsmesse erinevasse kategooriasse.

1. Sisemised ja välised ohud - organisatsiooni sisesed ohud on kõrgema riskiga kuna nende esinemistõenäosus on suurem. Organisatsiooni sisesed ohud ei pruugi olla alati seotud tahtliku tegevusega, vaid võivad olla tingitud teadmatusest.
2. Rakenduse arhitektuur - Platvormid pakuvad palju võimalusi, kuidas arendada ja juurutada organisatsiooni aplikatsioone. Uued teenusele orienteeritud aplikatsioonid kasutavad veebiteenuseid arendamaks iseseisvaid

moodulipõhiseid aplikatsioone, mis on kergesti integreeritavad loomaks dünaamilisi ja vahest ka ajutisi aplikatsioone. Need aplikatsioonid on keelest ja platvormist sõltumatud, aga muudavad organisatsiooni ohtudele vastuvõtlikumaks ja mis veel tähtsam, nad ei pruugi ühilduda organisatsiooni turvapoliitikatega.

3. Probleemid kolmanda osapoole tööriistadega - ERP tooted sisaldavad endas pahatihti kolmandate osapoolte tooteid, mis kõik koos moodustavad ühe integreeritud toote. Kahjuks sellised integratsioonid ei pruugi hästi toimida eriti turvaaspektide halduse kohapealt.
4. Muudatuste halduse puudulikkus - muudatuste haldust peetakse ERP toodete puhul üheks suuremaks probleemiks, mis potentsiaalselt mõjutab ka turvalisust. Muudatuste tegemine programmis ja konfiguratsioonis tuleks alati logida ning dokumenteerida. Arendus ja töökeskkonnad peavad olema selgelt eraldatud, testimise protsess peaks sisaldama ka infoturbega seonduvaid aspekte sh muudatuste mõju pääsuõigustele.
5. Rohkete integreerimistega kaasnevad väljakutsed - ERP süsteem vahetab palju informatsiooni teiste süsteemidega läbi integratsiooni vahevara, seega võib sellest liidesest saada potentsiaalne turvanõrkus.
6. Turvalisuse väljakutse - ERP süsteemid sisaldavad endas väga palju erinevat informatsiooni personali, klientide ja partnerite kohta. Seega peab olema välja töötatud tõhus identiteedi ja pääsuõiguste halduse protsess.
7. Väljakutsed väljastpoolt ERP tarkvara kontrolli - kui ERP kasutab integreeritavat autentimist siis on kasutajanimede ja salasõnade kaitsmine selle teenuse osutaja käes. Nõrgast võrgu infrastruktuurist tingitud ohud, tulemüüri seadistused, andmevahetusest või mõnest teisest tarkvarast/seadmest tingitud ohud, arvutiviirused, nuhkvara jne, võivad põhjustada tõsiseid kahjusid ERP süsteemile.

Välja toodud riskide jagunemine ei sisalda kõiki võimalikke riskikohti, kuid peaks illustreerima riskikohtade tuvastamise vajadust. Lisaks eelnevale, on tähtis omada ülevaadet ERP juurutusprojektiga seonduvatest riskidest, sest riskijuhtimine peab olema kaasatud juba projekti projekteerimise faasi.

2.3. ERP riskifaktorid

Tavapärastele infosüsteemidest tulenevatele riskidele lisaks, tuleb arvestada ka ERP kontekstist sõltuvate riskifaktoritega (Lisa 1). Neid riske saab kategoriseerida mitmel moel. Näiteks inimestega seotud riskid, protsessidega seotud riskid, tehnoloogilised riskid, rakendamisega seotud riskid ja halduse riskid.

2.3.1. Inimestega seotud riskid

Töötajad on ERP projektiga seotult kõige olulisemad inimesed. Tähtis on, et need inimesed mõistaksid paremini ERP süsteeme ja nendest tulenevaid kasutegureid, vastasel juhul võib kogu ERP projekt ebaõnnestuda (Leon, 2008).

Koolituste puhul on oluline, et eristataks administraatorite ja kasutajate tööspetsiifikast tulenevaid vajadusi. Kasutusjuhendid sisaldavad endas pahatihti vaid vajalikke toiminguid, kuid informatsioon süsteemi arhitektuuri ning ülesehituse kohta on puudulik. Seega puudub paljudel administraatoritel arusaam süsteemist kui tervikust ning organisatsiooni hierarhilisest ülesehitusest tulenevatest ohtudest, mis mõjutavad andmete konfidentsiaalsust. Kasutajate koolitusvajadused tulenevad paljuski kasutajate teadmatusest süsteemi ülesehituse loogika kohta. Tavapärane on pääsuõiguste tellimine teadmatuses, millele täpsemalt ligipääsu vajatakse ning millised on süsteemi spetsiifikast tulenevad parameetrid, mis peaks olema tellimusse kaasatud. See aga pikendab pääsuõiguste valideerimise protsessi ning tekitab viivitusi äriprotsessides.

2.3.2. Protsesside riskid

ERP süsteemide juurutamise üks olulisemaid eesmärke on parandada äriprotsesse muutes nad efektiivsemaks, täpsemaks ja produktiivsemaks. On väga tähtis, et eriti tootmises tegutsevatel organisatsioonidel oleks ajakohane info operatiivjuhtimiseks, kuna see on alus efektiivseteks juhtimisotsusteks. ERP süsteem peaks kaitsma andmete terviklikkust ja tagama informatsiooni siis kui vaja ja nii nagu vaja (Leon, 2008; Seo, 2013).

ERP süsteemid eeldavad, et organisatsiooni äriprotsesse parandatakse või tehakse ümber sobitumaks süsteemiga. Tõenäosus on suur, et sellised muudatused võivad viia läbikukkumiseni kuna kõik hakkab sõltuma ERP süsteemist. Peale muudatuste jõustamist on väga raske minna tagasi, seega mõjutab see kogu organisatsiooni (Leon, 2008; Sumner, 2000).

Muudatuste haldus on organisatsiooni ja IT-süsteemide, protsesside jm muudatuste ohje, suunamise ja dokumenteerimise kõigi tegevuste kogum (AKIT, kuupäev puudub). Muudatused süsteemis võivad mõjutada andmetele ligipääsetavust ning peavad seetõttu käima käsikäes infoturbega. Tähtis ei ole ainult muudatuste dokumenteerimine, vaid ka informatsiooni juhtimine ning kindlate protseduuride välja töötamine. Muudatuste planeerimisse ja testimisse peaks alati kaasama ka pääsuõigustega seotud aspektid, kuna ERP süsteemi pääsuõigused tuginevad atribuutidel, mis tagavad ligipääsu andmetele. Samuti tasub ettevaatlik olla kohandustega, kuna ERP süsteemi pääsuõigused on ülesehitatud põhinedes juurutuse käigus kaardistatud informatsioonile, seega hilisemad kohandused süsteemis peaksid seda lahendust edasi arendama. Pahatihti aga ei arvestata selliste muudatuste võimaliku mõjuga andmete konfidentsiaalsusele, käideldavusele ja terviklusele.

2.3.3. Tehnoloogilised riskid

Tehnoloogia areneb iga päevaga ja organisatsiooni jaoks on tähtis nende muudatustega kaasa minna. ERP süsteemid pakuvad suurel hulgal erinevat funktsionaalsust. Kuna organisatsiooni jaoks ei pruugi kogu pakutav funktsionaalsus vajalik olla, siis tasuks konsulteerida ERP ekspertidega milline funktsionaalsus paigaldada ja kasutusele võtta. See võimaldab süsteemi ja pääsuõiguste keerukuse ja kasutajate hirmu vähendamist uue süsteemi kontekstis (Leon, 2008; Ghosh, 2012).

Samuti on tähtis, et igat ERP süsteemi hoitakse ajakohasena, paigaldades versiooniuuendusi, et süsteemist maksimaalset kasu saada. Hooldus-meeskond peab vastutama süsteemi uuendamise eest kui uuendused on saadaval.

2.3.4. Rakendamise riskid

Kuna paljud ERP projektid ebaõnnestuvad, siis on tähtis omada ülevaadet asjaoludest, mis võivad juurutuse käigus valesti minna. Panorama Consulting Solutions poolt 2014. aastal läbi viidud uuringust selgus, et peaaegu iga viies vastanutest (16%) väitis oma organisatsiooni ERP juurutuse projekti läbikukkunuks (Panorama Consulting Solutions, 2014). Põhilisteks läbikukkumise põhjusteks toodi müüja juurutuse teenus (35% rahulolematu või väga rahulolematu) ja teostatud dokumentatsioon (34% rahulolematu või väga rahulolematud). Tõenäosus on, et organisatsioonid, mis ei ole täpselt kaardistanud oma vajadusi tunnevad sagedamini, et ERP müüja on esitanud ebatäpseid lubadusi (Panorama Consulting Solutions, 2014). Prototüüpimine annab arendajatele parema arusaamise ootustest süsteemile, kuid kuna ERP süsteemid on mahukad ja keerukad, siis pahatihti jäetakse prototüüp tegemata (Leon, 2008).

ERP süsteemi oodatavad tulemused võivad erineda sellest, mida ta tegelikult pakub. Seega on oluline, et tippjuhid oleksid kursis pakutavate toodete võimaluste ja puudustega. See mõjutab otseselt projekti ajakavas püsimist ja kulu.

2.3.5. Halduse riskid

ERP süsteem ei ole kunagi valmis juurutusfaasi lõppedes. Kasu süsteemist tuleb alles selle kasutamisel. Uuenduste ja täienduste installeerimine, uue tehnoloogia kasutuselevõtt, uute kasutajate koolitus, protsesside välja töötamine ning turvapoliitika täiendamine on tegevused, mida tuleb teha terve süsteemi eluea jooksul. Tippjuhid, süsteemi kasutajad ning administraatorid peavad pühenduma süsteemi hooldusele ja töös hoidmisele.

Eduka ERP süsteemi juurutamise aluseks on põhjalik eelnev äriprotsesside kaardistus, projekti skoobi määratlemine ning riskianalüüsi teostus. ERP projektid on väga ajakulukad ning ressursimahukad, seega tasub ERP riskidega tutvuda enne projektiga alustamist. Riskianalüüsi vajadus on veelgi suurem, kui organisatsioonil on plaanis otsustada pilvepõhise ERP süsteemi kasuks.

2.4. Pilvepõhise ERP süsteemi turvariskid

Viimase aja trend on pilvepõhised ERP süsteemid, sellest tulenevalt peaks sellise lahenduse turvariskidega arvestama juba projekteerimise faasis (Leon, 2008). Pilvepõhised ERP süsteemid on süsteemid, mis on paigutatud pilve keskkonda. Need süsteemid pakuvad paindlikku, tõhusat, sobitatavat, skaleeritavat ja soodsat lahendust ning nad on saavutanud suurt edu. Vaatamata hüvedele on oluline, et organisatsioonil oleks selge arusaam riskidest, mis on seotud pilvepõhise lahenduse arhitektuuriga.

Palju seotud osapooli, rakendusi ja seadmeid, mis on kaasatud pilve keskkonda suurendavad juurdepääsude arvu. Seetõttu on tõenäoline, et kõrvalised isikud võivad proovida andmetele ligi pääseda, mõjutades nii andmete konfidentsiaalsust ning terviklust. Jagatud omand on iseloomulik ressurssidele nagu mälu, võrk, andmed ja programmid. Pilves jagatakse ressursse läbi võrgu, serveri ja rakenduse tasandi. Kuigi kasutajad on eraldatud virtuaalsel tasandil siis riistvara ei ole. See võib põhjustada tõsiseid nõrkusi. Pilveteenuseid kasutades ei eristata kasutajaid riistvara põhiselt, selle tulemusena võib andme jäljend viia privaatsete andmete paljastamiseni (Leon, 2008). Andme jäljend viitab kustutatud või eemaldatud andmetele.

Kasutaja autentimine võimaldab tuvastada, kas kasutaja on see, kes ta väidab ennast olevat. Nõrk kasutaja autentimine võib põhjustada autoriseerimata ligipääsu kasutajakontodele, mis omakorda põhjustab privaatsuse rikkumisi. Pilveteenuseid kasutades peab kasutaja usaldama oma andmete turvalisuse teenusepakkuja kätte. Kui andmed on pilves, on organisatsiooni andmed salvestatud teenusepakkujate serveritesse ja mitte organisatsiooni serveritesse. Need serverid võivad aga asuda erinevates riikides, mis võib põhjustada probleeme erinevast õiguslikust regulatsioonist tulenevalt.

Terviklus tähendab andmete kaitsmist volitamata kustutamise, muutmise ja tootmise eest. Vähene autentimise ja autoriseerimise mehhanism võib kahjustada andmete terviklikkust. Infoturbe kontekstis tuleb jälgida, et lisaks andmetele ei oleks volitamata muudetud ka andmete loojat, loomisaega jms. Andmed, riist- ja tarkvara peavad olema kättesaadavad volitatud kasutajatele siis kui nad seda vajavad. Seega peaks süsteem olema võimeline töötama ka võimaliku ründe korral.

Üks on kaitsta infot, mis on andmebaasis, hoopis erinevat lähenemist nõuab infole ligipääsu kaitsmine läbi rakenduse, mis annab nendele andmetele tähenduse. Suurem osa turva intsidentidest leiab aset oma töötajate poolt. 61% - 81% arvutiga seotud kuritegudest teostatakse selliste rikkumiste tõttu. Need töötajad võivad olla ebaausate kavatsustega või ärritatud kopeerides, varastades või saboteerides informatsiooni ilma, et neid tegevusi avastataks (Dhillon & Backhouse, 2000). Sellise olukorra tekkimise tõenäosuse vähendamiseks on oluline välja töötada ning rakendada turvapoliitika, mis sisaldab endas ka kasutajate pääsuõiguste poliitikat.

3. ERP pääsuõigused

Käesolev peatükk uurib tähtsamaid pääsuõiguste halldusprintsiipe ning kasutajakonto elutsükli haldusprotsessi. Peatüki eesmärk on välja selgitada kuidas tõhusamalt rakendada kasutajakonto halduse soovitusi ning jõuda otsuseni, kuidas organisatsioonis neid soovitusi rakendada.

Pääsuõigused on infoturbe alamteema ja andmekaitse realiseerimise vahend. Infoturve on riskihalduslik tegevus teabe turvalisuse säilitamiseks vastavalt organisatsiooni tegevuse eesmärkidele (AKIT, kuupäev puudub). Pääsuõigused on õigus juurdepääsuks mingitele varadele ja ettemääratud toimingute sooritamiseks nendega (AKIT, kuupäev puudub). ISACA (*Information Systems Audit and Control Association*) definitsioon pääsuõigustele on kasutajaile, programmidele või tööjaamadele antav õigus või eesõigus andmete ja failide loomiseks, muutmiseks, kustutamiseks või vaatamiseks süsteemis, määratletult andmete omanike ja infoturvapoliitika kehtestatud reeglitega (Hanson, Buldas, Veldre, Laur, & Krasnosjolov, 2011).

Pääsuõiguste haldus ja korrashoid võib olla väga mahukas organisatsioonis, kus on palju kasutajaid, suur tööjõu voolavus või toimub palju organisatsioonilisi muudatusi. Vead on kerged tekkima ja pääsuõiguste ülevaatuseks ei pruugi jätkuda ressurssi, mis omakorda soodustab turvaintsidentide teket. Suureneb vajadus pääsuõiguste halduse korralduse lihtsustamise ja läbipaistvuse järele. Selleks aga tuleks pääsuõiguste elutsükkel korralikult läbi planeerida ning välja töötada pääsupoliitika. Vastasel juhul võivad suure tõenäosusega realiseeruda kõrged infoturbega seotud riskid.

Enamus kommertssüsteeme ja – rakendusi sisaldavad pääsu reguleerimise vahendeid, mis on tihtipeale sõltumatud operatsioonisüsteemist või andmebaasisüsteemist, kuhu need paigaldatakse (Ferraiolo, Kuhn, & Chandramouli, 2007). Infosüsteeme tuleb kaitsta volitamata juurdepääsu eest selleks, et kaitsta andmete terviklust, konfidentsiaalsust ja käideldavust. Erinevad aset leidnud intsidendid on peaaegu alati olnud seotud vähemalt ühe komponendiga nendest (O'Connor, & Loomis, 2010).

Samuti on oluline selgelt kindlaks määrata, kes peaks vastutama süsteemile juurdepääsu õiguste autoriseerimiste eest (Loh & Koh, 2004). Kui tähtsa ja

konfidentsiaalse informatsiooni juurde on ligipääs volitamata inimestel, võib see kaasa tuua teabe lekkeid ja äri kriisi (Yosha, 1995). Selliste riskide põhjusteks võivad olla organisatsiooni halb andmekaitse ja pääsuõiguste poliitika ning nõrk IT turvalisus (Wilding, 2003; Loh & Koh, 2004). Lisaks võib konfidentsiaalne informatsioon lekkida ka konkurentidele ja teistele volitamata isikutele oma töötajate poolt, kellel on madal lojaalsust organisatsioonile (Wilding, 2003).

On oluline, et organisatsioonid omaksid selget poliitikat, mis määratleb, milliseid andmetele juurdepääsu õigused võib anda kasutajatele vastavalt nende osakondadele ja tööfunktsioonidele (Loh & Koh, 2004).

3.1. Autentimine ja autoriseerimine

Ligipääs süsteemile saab alguse kasutaja autentimisest. Autentimine viitab kasutaja identifitseerimisele, ehk tuvastamisele ning kinnitamisele, et nad on, kes nad ütlevad ennast olevat. Pangaautomaadid nõuavad nii pangakaardi kui PIN koodi olemasolu selleks, et taotleda juurdepääsu pangakontodele ning teha tehinguid. Enamikes organisatsioonides on kasutaja identifitseerimisel kõige levinum meetod kasutajanimi ja parool.

Identifitseerimisele ja autentimisele järgneb autoriseerimine ehk juurdepääsu kontroll, mis on oluline osa identiteedi ja juurdepääsu haldusest. Autoriseerimine viitab pääsuõiguste kindlaks tegemisele ning nende õiguste jõustamisele, täpsustades, millistele objektidele on kasutajal ligipääs ning milliseid toiminguid ta võib sooritada. Autoriseerimise eest vastutab tihti ligipääsu pakkuv teenus. Näiteks, kui subjekt soovib ligi pääseda failile, mis asub failiserveril, siis on see failiteenuse kohustus määratleda, kas antud subjekt pääseb failile ligi või mitte. Autoriseerimine võib olla mitmekülgne ja võib teha vahet sellistel tegevustel, nagu lugemine, kirjutamine, kustutamine ning käivitamine.

Autoriseerimine puudutab kõiki IT süsteeme ning see kujutab paljudele organisatsioonidele suurt administratiivset väljakutset. Kuigi pealtnäha segavad pääsu reguleerimise süsteemid info jagamist, siis tegelikkuses toetab hästi korraldatud ja hallatud pääsu reguleerimise süsteem info jagamist (Ferraiolo et al., 2007).

3.2. Pääsuõiguste haldus

Vajadus hästi rakendatud haldusprotsessi järele on seda suurem, mida keerukamad on kasutaja pääsuõigused ning muudatused, eriti keskkondades, kus toimuvad pidevad rolli muutused, pääsuõiguste vajaduste muudatused ning on suur tööjõu voolavus. See rõhutab vajadust rakendada kasutaja pääsuõiguste kogu elutsüklit hõlmavat haldusprotsessi leevendamaks liigsete või liiga väheste pääsuõiguste küsimusi. Kuid samuti ka tagandus protsesse töösuhte lõppemisel, samas tagades, et kasutaja pääsuõiguste muudatused toovad endaga kaasa minimaalse mõju äritegevusele. Liigsete pääsuõigustega kasutajal on õigusi rohkem, kui on vajalik töökohustuste täitmiseks ja see kujutab endast turvariski. Samas liiga väheste pääsuõigustega kasutaja võib oma töökohustuste täitmiseks paluda kolleegilt abi andmetele ligipääsemiseks, mis teeb raskeks kasutajate tegevuste tuvastamise. Seega on tähtis leida õige tasakaal pääsuõiguste andmisel.

Suur osa infoturbe haldusest kontrollib juurdepääse rakendustele või andmetele. Pääsuhalduse kohustus on tegeleda kasutajate juurdepääsu taotlustega. Protsess hõlmab kasutajanime ja salasõna kontrolli, pääsuõiguste kasutajaga sidumist, aga ka gruppide ja rollide loomist ning neile pääsuõiguste määratlemist. Lisaks pääsuõiguste andmisele sisaldab pääsuõiguste haldus ka pääsuõiguste lõpetamist kasutaja lahkumise või sisemise liikumise tõttu. Pääsuõiguste haldus hõlmab ka perioodilist seiret gruppide ja rollide pääsuõiguste osas, veendumaks, et nad sisaldavad ainult rollidele/gruppidele määratud õiguseid ning vältimaks rollide vahelisi konflikte. Pääsuõiguste haldus peab arvestama kahe printsiibiga: minimaalõiguste printsiip ning teadmistarve.

3.2.1. Minimaalõiguste printsiip

Minimaalõiguste printsiip on pääsupoliitika põhimõte, mis nõuab, et igale subjektile (isikule, üksusele, protsessile) antaks mingite objektide kasutamiseks minimaalsed volitatud tegevuseks vajalikud õigused. Minimaalõiguste printsiip on üks põhinõue iga pääsu reguleerimise süsteemi puhul. Kasutajate pääsuõiguste kontekstis tähendab see kasutajatele ainult nende pääsuõiguste andmist, mis on nende tööks vajalikud. Kui kasutajale on ette nähtud teatud aruannete vaatamine, siis ei peaks talle andma õigusi,

mis võimaldavad neid andmeid muuta. Leida tuleb selge tasakaal liiga rangete või liiga leebete reeglite kehtestamisel, tähtis on, et see läheks kokku organisatsiooni ärieesmärkidega (Nwafor, Zavarsky, Ruhl & Lindskog, 2012, 151).

3.2.2. Teadmistarve

Minimaalne tööülesannete täitmiseks vajalik teave on lubade andmise alus vaikimisi keelava pääsupoliitika rakendamisel. Teadmistarve on turvaprintsiip, mis käib käsikäes minimaalõiguste printsiibiga. Ta viitab ligipääsu meetodile, mis kindlustab, et isikutel on ainult need õigused, mis on tööfunktsioonide täitmiseks vajalikud. Kasutajakonto/informatsiooni turvaliigituse skeemi defineerimine võimaldab teadmistarvet kergemalt tuvastada, põhinedes kasutajakonto ja informatsiooni tundlikkusele millele soovitakse ligipääsu. See võimaldab kindlustada, et isikul on ainult minimaalõiguste printsiibi põhine ligipääs informatsioonile, millele neil on teadmistarve, säilitades tundliku (salastatud) informatsiooni konfidentsiaalsuse ja tervikluse. (Nwafor et al., 2012, 151)

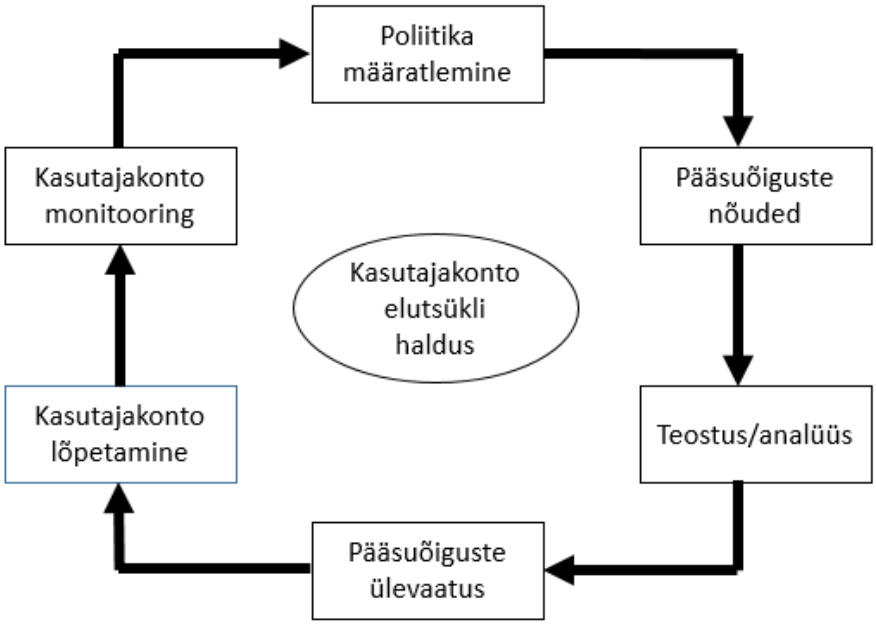
3.2.3. Tehnilised vs mittetehnilised turvameetmed

Eduka kasutajate pääsuõiguste haldusprotsessi väljatöötamine võib olla suur saavutus, kuid protsessi ebakorrektsel teostamisel ei pruugi see oodatavaid tulemusi tuua. Pahatihti on fookus turvameetmete eesmärkide (*control objective*) saavutamisel tehniliste vahenditega, ilma inimfaktorit arvesse võtmata. See võib viia olukorrani, kus autoriseeritud kasutaja väär-kasutab neid õigusi, kas teadmatusest või omakasu eesmärgil. Seega on väga tähtis leida tasakaal tehniliste ja mittetehniliste pääsumehhanismide vahel, teostades pääsuõiguste elutsükli haldusprotsessi (Nwafor et al., 2012, 152).

3.3. EUALMF Raampõhimõtted

Organisatsiooni kasutajakonto elutsükli haldus (*Enterprise User Account Lifecycle Management,* edaspidi EUALMF) on välja töötatud aitamaks väikese ning keskmise suurusega organisatsioone tõhusamalt rakendada kasutajakonto haldussoovitusi, mis

sisalduvad NIST SP 800-53 standardis, COBIT 4.1/5 raamistikus ja ka teistes standardites ja parimates praktikates (Joonis 3) (Nwafor et al., 2012, 151).



Joonis 3. Kasutajakonto elutsükli haldus raampõhimõtted (Nwafor et al., 2012, lk 152)

Joonisel 3 on näha kavandatud kontseptuaalne raamistik, mis katab kõik kasutaja elutsükli etapid, tõstes esile vajaduse soovituste järele, mis sisalduvad EUALMF/NIST SP 800-53/COBIT 4.1 kaardistuses (Nwafor et al., 2012, 150). Järgnevalt tutvustatakse raamistiku erinevaid etappe.

3.3.1. EUALMF Elutsükli haldus

Pääsuõiguste elutsükkel sisaldab endas mitut etappi: kasutajakonto nõuded, rakendamise kord, ülevaatus protsess, konto lõpetamise protseduurid ning pidev seire veendumaks, et kasutaja pääsuõigused vastavad hetkel kehtivale organisatsiooni pääsupoliitikale.

Poliitika määratlemine (*account requirements*)

Pääsuõiguste poliitika määratlemise etapp määratleb töötajate/tööandjate vastutusalad ning määrab pääsuõiguste elutsükli juhtimise edu. Etapp peaks käsitlema eesmärki, skoopi, rolle ja vastutust, nõudeid pääsuõiguste loomiste, aktiveerimiste, muutmiste, blokeerimiste ja eemaldamiste kohta, lisaks sisaldama nõuete vastavuste, regulatiivsete nõuete ning õiguslike nõuete käsitlust. Määratleda tuleb ka

distsiplinaarsed protseduurid, mis rakenduvad poliitika rikkumise korral. Hästi välja töötatud pääsuõiguste poliitika välistab olukorrad, kus pääsuõiguseid küsitakse stiilis „Palun mulle samad õigused, mis on …“ mida nimetatakse ka kloonimiseks ja mis on väga tüüpiline lähenemine paljudes organisatsioonides selleks, et aega kokku hoida. Meetod võib küll tunduda aja kokkuhoiuna, kuid ei ole soovituslik. Sellise lähenemisega kaasneb risk anda kasutajale liiga palju või liiga vähe õigusi, mis on otseselt vastuolus minimaalõiguste ja teadmistarbe printsiipidega. Isegi kui töötajate tööiseloom on väga sarnane, ei pruugi seda olla nende pääsuõigused, mida nad oma töö tegemiseks vajavad. Pikema töösuhtega töötajatele võivad aja jooksul kuhjuda erinevad pääsuõigused, mis ei pruugi vajalikud olla uuele töötajale kelle pääsuõigused kopeeritakse kellegi näite pealt. Pääsupoliitika, mis keelab kasutamast kloonimise meetodit aitab pääsuõigusi määrata ja hallata vastavalt nõuetele.

Pääsuõiguste nõuded (*account requirements*)

Uue töötaja lisandumisel on esmaseks vajaduseks pääsuõiguste andmine. Tavaliselt põhineb pääsuõiguste tuvastamine töötaja rollil/töökohustustel. Kaasnevad kooskõlastamised näiteks personaliosakonna, andmeomanike ja otsese juhiga. Selleks, et eelmises peatükis välja toodud kloonimise meetodit vältida, oleks soovituslik välja töötada miinimum pääsuõigused, mis võimaldavad teostada baastoiminguid ajal, kui töökohustuste täitmiseks vajalikud pääsuõigused on täpsustamisel.

Nimekiri kasutajatest ja nende pääsuõigustest peab olema kogu muudatuste halduse protsessi vältel hallatud kindlustamaks, et kõik muudatused pääsuõigustes on registreeritud ja dokumenteeritud kogu kasutajakonto elutsükli jooksul.

Teostus/analüüs (*Implement/Assess*)

Peale pääsuõiguste nõuetele kinnituste saamist, järgneb tavaliselt pääsuõiguste teostus. Teostuse protsess peaks realiseerima nõuete etapis kooskõlastatud pääsuõigused. Etapp on väga tähtis, kuna vead selles staadiumis võivad organisatsioonile kalliks maksma minna, kui neid ei avastata enne kasutajale üleandmist. Olukorra leevendamiseks tuleks välja töötada analüüsiprotseduur, mis aitab kindlustada, et teostatud pääsuõigused vastavad nõuetes sätestatule. Sama protseduur kehtib ka olemasolevate kasutajate pääsuõiguste muudatuste puhul. Kõik muudatused tuleks dokumenteerida muudatuste halduse protsessi vältel.

Pääsuõiguste ülevaatus (*review account*)

Üks pääsuõiguste elutsükli osa on regulaarne pääsuõiguste ülevaatus veendumaks, et need vastavad nõuetele. Regulaarsus sõltub organisatsiooni poliitikast, kuid soovitav on siiski teatud intervalli tagant teostada pääsuõiguste audit, kas organisatsiooni siseselt või kaasata väline audit. Pääsuõiguste regulaarne audit aitab välistada olukorda, kus kasutajale lisatakse aja jooksul õigusi aina juurde, kuid ei pöörata tähelepanu pääsuõigustele, mis on juba aegunud. Sellised olukorrad tekivad organisatsiooni siseste liikumiste, ametikõrgenduste ning osakonna vahetamise puhul. Ilma tõhusa muudatuste halduse protsessita jäävad pahatihti olemasolevad pääsuõigused üle vaatamata ning eemaldamata. Selline olukord tekitab organisatsioonile turva- ja äririske. Turvatud revisjonilogi (*audit log*) kindlustab kasutaja tegevuste jälgitavuse, pääsuõiguste korrektse teostuse ning orbudeks jäänud kasutajakontode (*orphaned user accounts*) kustutamise kooskõlas kasutajakonto lõpetamise nõuetega.

Kasutajakonto lõpetamine (*account termination*)

Kasutajakonto lõpetamine (blokeerimine või õiguste piiramine) on üks pääsuõiguste elutsükli võtme tegevustest, mis pahatihti jääb tähelepanuta. Seda juhtub eriti tihti siis kui tööjõu voolavus on väga suur või ei ole kokkulepitud protsesse. Seda kutsutakse ka taganduseks (*deprovisioning*), mis viitab protsessile mille käigus eemaldatakse kasutajakontolt pääsuõigused erinevatel kasutajakonto elutsükli etappidel, mida tööfunktsioonide täitmiseks ei ole enam vaja. See võib tähendada kasutajakonto blokeerimist, lõpetamist/kustutamist või peatamist juhul, kui töötaja viibib teatud perioodi töölt eemal. Juhul kui töötaja eemaloleku ajaks on vaja tagada ligipääs teisele kasutajale, tuleks pääsuõigused üle vaadata ja läbida kinnitamise protsess.

Töötajad lahkuvad organisatsioonist erinevatel põhjustel. Pääsuõiguste lõpetamist tuleb vaadata kahest vaatenurgast, töötajad kes lahkuvad omal soovil ja töötajad, kes on sunnitud lahkuma, pahatihti pööratakse rohkem tähelepanu esimesele. Töötajad, kes on sunnitud lahkuma, endised koostööpartnerid või kolmanda osapoole kasutajad, võivad tahtlikult rikkuda või saboteerida informatsiooni. Samas töötajaid, kes lahkuvad vabatahtlikult, võib ahvatleda informatsiooni kogumine tuleviku tarbeks ning pääsuõigused tundlikule informatsioonile võiks kuni lahkumiseni võimalusel piirata. Seega on mõlemal juhul hädavajalik kasutajakonto

läbivaatamisega/lõpetamisega seotud protsesside olemasolu, kindlustamaks kasutajakonto ja pääsuõiguste lõpetamine. Sarnane protseduur peaks kehtima ka lepinguliste ja ajutiste töötajate puhul, välistamaks olukordi, kus kasutajakontoga seotud pääsuõigused on aktiivsed ka nädalaid/kuid peale töötaja lahkumist.

Kasutajakontode monitooring (*monitor account*)

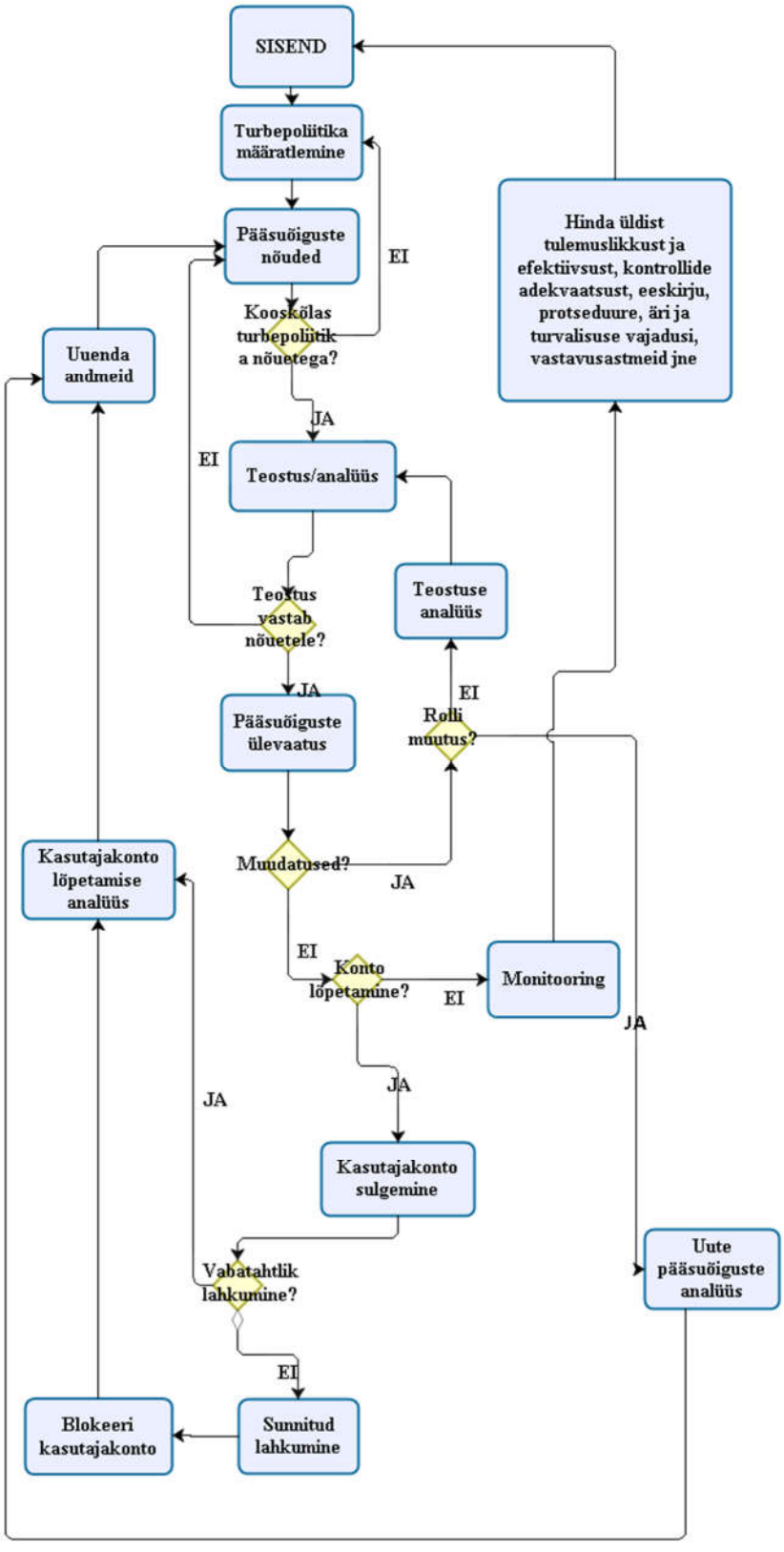
Viimane samm pääsuõiguste elutsükli protsessis on kindlustamine, et üleüldine pääsuõiguste halduse protsess on pidevalt monitooritud ja analüüsitud. Kasutajate teadlikkuse tõstmiseks tasuks kaaluda koolituste läbiviimist vastavalt vajadusele ja sõltuvalt monitooringu tulemustest. Regulaarne revisjonilogi analüüs volitatud isiku poolt koos turbe poliitika ülevaatusega peaks kuuluma sellesse protsessi. (Nwafor et al., 2012, 152-154).

3.3.2. EUALMF Rakendamise juhis

Raampõhimõtete edukaks rakendamiseks on vajalik põhimõtetest arusaamine ning olemasolevate IT keskkondadega sobitumise mõistmine. Selleks, et teostus vastaks äri ja turbe vajadustele ning kindlustamaks ressursside ning teostuse maksumuse eesmärgipärasus, tuleks läbi viia lahknevusanalüüs olemasolevate pääsuõiguste haldusprotsessi kohta.

EUALMF Vooskeemi lähenemine

Pääsuõiguste elutsükli erinevatest etappidest paremaks arusaamiseks on sobilik kasutada vooskeeme. Vooskeemiga saab illustreerida, kuidas on erinevad töövood omavahel seotud arvestades minimaalõiguste printsiipi ja teadmistarvet (Joonis 4).



Joonis 4. EUALMF näidis voodiagramm (Nwafor et al., 2012, lk 155).

Pääsuõiguste ülevaatus ja monitooring on ühed tähtsamad pääsuõiguste haldus protsessi sammud kontrollimaks nõuete vastavusi. Pääsuõiguste ülevaatusi peaks

teostama regulaarselt turvapoliitikas määratletud intervallide (3 kuud, 6 kuud, 1 aasta) tagant. Pääsuõiguste ülevaatuse ja monitooringu käigus on võimalik tuvastada passiivseid kasutajakontosid ning vajadust juurdepääsu muutmise või peatamise järele, mis tulenevad rollimuutusest või seadistusvigadest.

Edukas EUALMF raamistiku rakendamine toob organisatsioonile mitmeid kasutegureid, mis aitavad kindlustada kasutajate pääsuõigushalduse protsessi olemasolu ning muuta üleüldist hoiakut infoturbe suhtes. Samuti aitab ta vastata järgmistele küsimustele:

- Kes otsustab milliseid pääsuõiguseid kasutajale vaja on?
- Kas organisatsioon vajab klassifitseerimise menetlust iga kasutaja puhul?
- Kuidas tagada muudatuste nõuetekohane rakendamine kogu kasutajakonto elutsükli jooksul?
- Kuidas on määratletud menetlus, mis tagab ressurssidele nõuetekohase ligipääsude lõpetamise kasutajakonto elutsükli lõpus?

EUALMF ei pruugi katta kõiki nõudeid kasutajakonto elutsükli halduses ning tuleks kohandada vastavalt organisatsiooni vajadustele. (Nwafor et al., 2012, 154-155).

Autor tuvastas mitmeid puudujääke organisatsiooni haldusprotsessis ning tegi ettepanekuid nende kõrvaldamiseks. Selleks aga, et kasutajakonto elutsükli haldus protsessi veelgi tõhusamaks muuta, on vaja üle vaadata organisatsioonis kehtivad pääsu reguleerimise poliitikad.

4. Pääsu reguleerimine

Neljas peatükk annab ülevaate enamlevinud pääsu reguleerimise poliitikatest ning pääsuõiguste strateegiast, milles sõnastatud nõuded ja reeglid on aluseks pääsuõiguste haldusele. Peatüki eesmärk on tutvustada pääsuõiguste strateegia olemust ja vajadust juba planeerimise faasis ning valida organisatsiooni jaoks sobivaim pääsu reguleerimise poliitika, mis võimaldaks vähendada pääsuõiguste järelevalve koormust.

4.1. Pääsuõiguste poliitikad

Pääsuõiguste süstematiseerimine on otseselt seotud pääsuõiguste järelevalve koormuse ning pääsuõiguste haldusega. Selleks, et efektiivsemaks muuta pääsuõiguste haldusprotsessi on tähtis valida organisatsiooni vajadustest ning süsteemi keerukusest tulenevalt neid vajadusi kõige enam rahuldav reguleerimise poliitika. Ühendriikide Kaitseministeerium oli üks maailma esimesi organisatsioone, kes üritas kirjeldada oma organisatsioonis rakendatavaid pääsu reguleerimise viise. 1986. aastal andsid nad välja dokumendi nimega «*Trusted Computer System Evaluation Criteria*» (TCSEC) (Latham, 1986). Muuhulgas on seal välja toodud diskretsionaarne ja mandatoorne pääsu reguleerimine, pääsupiiramisloendid ning rollipõhine pääsupoliitika.

4.1.1. Pääsupiiramisloendid

Pääsupiiramisloendid (*access control list*, edaspidi ACL) on kõige levinum ja lihtsam juurdepääsu kontroll. ACL sisaldab endas kasutajaid või kasutajagruppe ning nende õigusi teatud ressursile.

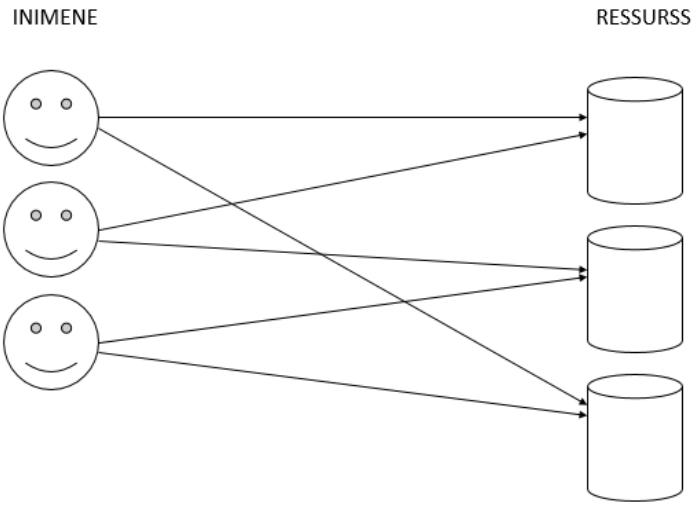
Arvutiturbes tähendab ACL objektidele kaasatavaid õiguste loendeid. Loendis määratletakse, kellel või millel on õigus objektidele ligi pääseda ning mida on sellega lubatud teha. Tavapärane ACL määratleb igas kirjes isiku ja toimetuse: näiteks, kirje (Peeter, kustuta, faili XYZ) ACL annab Peetrile õiguse faili XYZ kustutamiseks. Kui ACL põhinevas turvamudelis saadetakse objektile päring mingisuguse toimingu läbiviimiseks, siis leitakse esmalt loendist vastavad kirjed, ning seejärel otsustatakse toimetuse jätkamise üle. Peamine küsimus ACL põhineva turvamudeli määratlemisel

tekib loendite muutmisel – kellel on õigus seda teha ning millised muudatused on lubatud.

On kahte liiki ACL kasutavaid süsteeme: valikulised ja kohustuslikud. Kui süsteemil on valikuline pääsupiirang, siis on selle tekitajal või omanikul õigus täielikult piirata ligipääsu sellele objektile, muuhulgas niiviisi, et ligipääs lubatakse kõikidele teistele. Süsteemil on kohustuslik pääsupiirang, kui see allub üle terve süsteemi kehtivatele piirangutele, mis on ACL loendis määratletud õigustest tähtsamad.

4.1.2. Diskretsionaarne pääsupoliitika

Diskretsionaarset poliitikat (*discretionaly access control*, edaspidi DAC) rakendav pääsu reguleerimine, mis põhineb pääsu taotlevate subjekti(rühma)de identiteedil. Infovara omanik delegeerib oma pääsuõigusi teistele subjektidele. Turvameetmete turvapoliitika, mis erinevalt mandatoorsest poliitikast on vabalt valitav, st ei ole infoturbearhitektuuriga jäigalt määratud ning pääsu subjekt saab oma pääsuõigusi otseselt või kaudselt edasi anda teisele subjektile (Joonis 5).

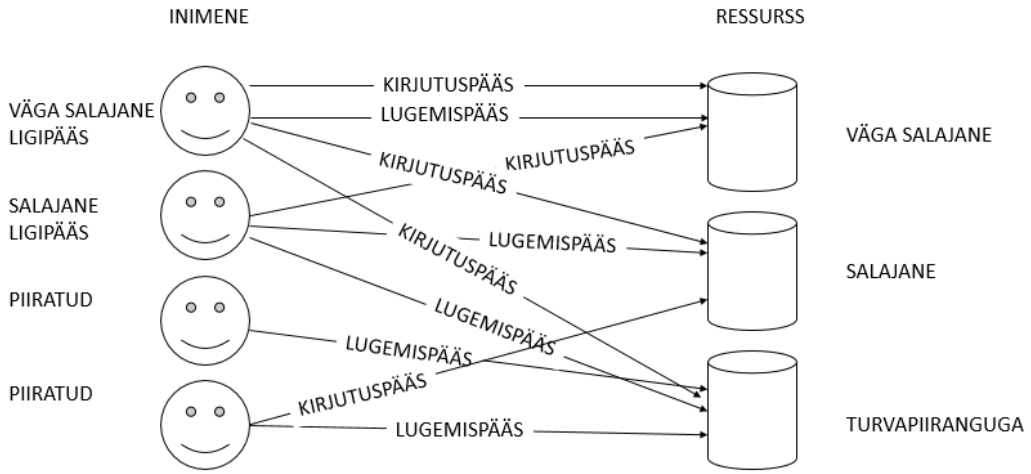


Joonis 5. Diskretsionaarne pääsu reguleerimine. (O'Connor & Loomis, 2010, lk 31)

4.1.3. Mandatoorne pääsupoliitika

Mandatoorset poliitikat (*mandatory access control*, edaspidi MAC) rakendav pääsu reguleerimine: operatsioonisüsteemi puhul on subjektiks harilikult protsess või lõim (*thread*), objektideks failid, kataloogid, pordid, seadmed jms, andmebaasihalduse

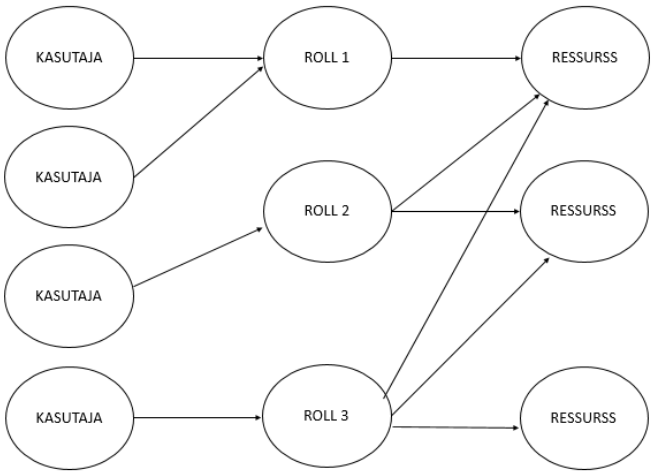
süsteemis on objektideks tabelid, vaated, protseduurid jms. Infoturbearhitektuuriga (eriti operatsioonisüsteemi ja/või andmebaasisüsteemi mehhanismidega) tsentraalselt määratud ja tundlikkusmärgenditel põhinev turvapoliitika (Joonis 6).



Joonis 6. Mandatoorne pääsu reguleerimine (O'Connor & Loomis, 2010, lk 31)

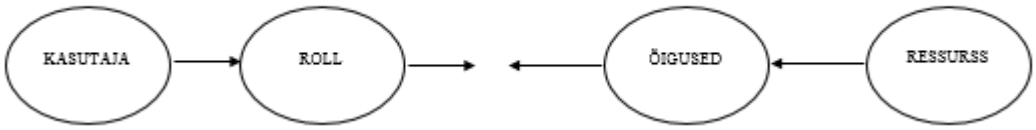
4.1.4. Rollipõhine pääsupoliitika

Alternatiiviks MAC ja DAC pääsupoliitikatele on rollipõhine pääsupoliitika (*role based access control,* edaspidi RBAC). Viimastel aastatel on aina rohkem levinud RBAC, milles sisaldub teatud määral diskretsionaarse pääsupoliitika komponente ning mis teoorias sobib kokku nii DAC kui MAC mudelitega (Benantar, 2006). RBAC põhineb täielikult „rollidel", mis on süsteemis seadistatud vastavalt kasutaja funktsioonidele organisatsioonis. Õiguseid jagatakse rollidele, mis omakorda määratakse kasutajatele (Joonis 7). Seega pärivad kasutajad õigused oma rollilt. Roll on abstraktsioon, mis toimib vahekihina kasutajate ja õiguste profiilide vahel.



Joonis 7. Rollipõhine pääsu reguleerimine. (O'Connor & Loomis, 2010, lk 31)

Igale rollile määratakse teatavad õigused, mis on seotud ressursiga ning rakenduvad kasutajatele läbi rolli (Joonis 8).



Joonis 8. Rollipõhine pääsuõiguste poliitika (Windley, 2005)

Rollipõhise pääsupoliitika rakendamisega võib kaasneda oht, et rollide arv kasvab liiga suureks. Seda olukorras, kus mängu tulevad mingi atribuudi põhised, näiteks asukoha pääsupiirangud. See mitmekordistab kasutusel olevate rollide arvu ning organisatsiooni kasvades võib tekkida taas olukord, kus pääsuõiguste halduskoormus kasvab ning rollide haldus muutub väga töömahukaks.

4.1.5. Atribuudil põhinev pääsupoliitika

Selleks, et vältida "rolli plahvatusi" ning pakkuda suuremat agiilsust on tehtud mitmeid katseid. Viimasel ajal on kasvanud huvi atribuudil põhineva pääsupoliitika (*attribute based access control*, edaspidi ABAC) vastu (Hu, Ferraiolo, Kuhn., Friedman, Lang, Cogdell, & Scarfone, 2013), mis viitab sellele, et atribuudid ja reeglid võivad kas asendada RBAC meetodit või muuta selle lihtsamaks ja paindlikumaks.

ABAC mudel ei ole siiani väga rangelt määratletud lähenemine. Selle keskne idee on, et juurdepääsu on võimalik kindlaks määrata tuginedes erinevatele andmesubjekti

tunnustele. Inimeste puhul võib atribuudiks lugeda pikkuse, silmade värvi jne. Seega reeglid määravad tingimused, mille alusel pääsuõigus kas antakse või mitte.

ABAC mudeli definitsioon võiks olla „Loogilise juurdepääsu kontrolli metoodika, kus luba täita toimingute kogumit määrab subjekti, objekti, soovitava toimingu ja mõnel juhul ka keskkonna tingimuste võrdlemine poliitika, reeglite või seostega, mis kirjeldavad lubatud toiminguid valitud atribuutidega“ (Hu, et al., 2013 ,8).

Selline lähenemine võib esmapilgul tunduda paindlikum kui RBAC kuna erinevate rollide määratlemine ei ole vajalik ning reegleid on võimalik väikese vaevaga luua ja vajadusel muuta. Arvestama peab aga selliste reeglite arvukusega, mis suuremas organisatsioonis võivad tekkida.

Kuna mudel ja selle rakendamine on veel arenemisjärgus, ei ole ABAC väga laialdaselt veel omaks võetud., Teema on aktuaalne, sest on avaldatud palju artikleid, aga puudub ühene teadmine mida ABAC ikkagi tähendab.

4.1.6. RBAC vs ABAC

Mõlemal lähenemisel on oma spetsiifilised plussid ja miinused. RBAC nõuab rollide väljatöötamist administreerimise lihtsustamiseks ning ABAC puhul on vastupidi, seadistamine võib olla lihtne aga hilisem analüüs ja audit selle võrra keerulisem (Kuhn, Coyne, & Weil, 2010, 79-80).

Mõlemaid lähenemisi tuleks vaadelda kui osana millestki suuremast. Kindlasti ei kasutata alati puhtalt ainult RBAC või ABAC lähenemist, vaid atribuudid kasvatavad või parametreerivad rolle. Neid saab kasutada sõltumatult määramaks ressursse digitaalsetele identiteetidele, mis ei ole seotud organisatsiooni funktsioonidega. Seega võiks mõelda, kui palju RBAC või ABAC lähenemist peaks kaasama oma xBAC mudelisse, et saavutada oma eesmärke (Walther, 2015).

Hindamaks milline pääsupoliitika on kasutajale kehtiv, peab olema võimalik pääsuõigusi analüüsida. Tähtis ei ole mitte ainult nimekiri kasutaja pääsuõigustest vaid arusaamine, mida need õigused võimaldavad kasutajal teha. Otsuste tegemiseks on vaja aru saada, milliseid õiguseid kasutaja oma funktsioonide täitmiseks enam ei vaja. Selline tegevus on väga ajakulukas ja kui seda teha regulaarselt kõikidele kasutajatele, suureneb oluliselt järelevalve koormus.

Üheks oluliseks otsustuskohaks on kasutajate kinnistamine, seda eelkõige kohustuste lahususe seisukohalt ning seda tutvustab töö järgnev peatükk.

4.2. Kasutaja kinnistamine

Oluline on otsustada kuidas kasutajatele rolle määratakse. Kasutajatele võib määrata rolle tsentraliseeritult administraatori poolt või on teatud kasutajatel luba määrata ise mõningaid rolle (Sandhu, Coyne, Feinstein, & Youman, 1994).

Tsentraliseeritud lähenemise eeliseks on kontroll ning kohustuse tsentraliseeritus. Puuduseks on suurenenud administratiivne koormus, eriti süsteemi kasvades. Taotlus kasutaja lisamiseks rollidesse saab alguse kasutaja poolt ning hea süsteem peaks võimaldama valitud kasutajatel teha seda ise, ilma administraatori sekkumiseta. Siin saab kasutada RBAC rolli, mis lubab kasutajatele pääsuõigusi anda, kuid ainult süsteemis defineeritud rollide nimekirja alusel (Sandhu et al., 1994).

On kaks pealtnäha erinevat aspekti kasutajatele rollide määratlemisel. Esimene aspekt on küsimus, kas esineb mingeid piiranguid rollide osas kuhu kasutaja kuuluda võib. Paljudes rakendustes on mõned rollid, mida peetakse teineteist välistavaks kohustuste lahususe (*separation of duties*) tõttu. Näiteks pearaamatupidajal on õigus väljamakseid kinnitada ja raamatupidajal on õigus arveid koostada. Määrates kasutajale mõlemad rollid, suureneb vastuvõtlikkus pettustele volitatud õiguste väärkasutamise tõttu. Sellise võimaluse vältimiseks peavad need kaks rolli olema üksteist välistavad nii, et ükski kasutaja ei saa kuuluda mõlemasse rolli.

Teine aspekt on seotud piirangutega, mis määratlevad, millised kasutajad võivad kuuluda teatud rolli. Näiteks piirang, kus raamatupidaja rolli saab määrata ainult kasutaja, kes kuulub finants rolli. Sellisel juhul saab finants rolli kasutajaid määrata tsentraalselt aga raamatupidaja rolli saavad määrata ka selleks volitatud kasutajad. (Sandhu et al., 1994).

4.3. Rollipõhine pääsupoliitika ja piirangud

RBAC taksonoomia koosneb neljast mudelist: tuumik RBAC, hierarhiline RBAC, staatiline piiratud RBAC ja dünaamiline piiratud RBAC (Hu, Ferraiolo, & Kuhn, 2006, 16). Tuumik RBAC hõlmab põhilisi süsteemi kantud funktsioone. See on tunnuste kogumi kaasamine, mis eristab RBACi teistest pääsuhaldus meetoditest. Hierarhiline RBAC lisab mõiste rolli hierarhia, kus kasutatakse päritavaid seoseid. Piiratud RBAC sisaldab staatilisi ja dünaamilisi töökohustuste lahususe omadusi. Staatiline piiratud RBAC lisab piirangu seostele, mis tekivad koos rollide seostega. Dünaamiline piiratud RBAC seab piirangud rollide aktiveerimisele, mis võivad olla ka kasutaja atribuudid (Ferraiolo, Sandhu, Gavrila, Kuhn, & Chandramouli, 2001).

Alljärgnevalt annab autor ülevaate kõigist neljast RBAC funktsionaalsest mudelist.

4.3.1. Tuumik RBAC

Tuumik RBAC (*core RBAC)* koosneb viiest halduskomplektist: kasutajad, rollid, pääsuõigused, tegevused ja objektid, mille õigused koosnevad toimingutest, mis rakendatakse objektidele (Hu et al., 2006, 17). Tuumik RBAC funktsioone saab jaotada järgmiselt:

- haldamisega seotud ülesandeid, mis hõlmavad kasutajate ja rollide loomist ning kustutamist ja kasutajate rollidesse ning rollidele pääsuõiguste määramist;
- süsteemi toimingud, mis sisaldavad endas kasutaja sessiooni loomist, mis aktiveerib kasutaja rollid ning tuvastab kasutaja pääsuõigused vastavalt kasutajale määratud rollidele;
- kohustuslik ülevaatus, mis sisaldab endas rollidele määratud kasutajate ning kasutajale määratud rollide ülevaatust. (O'Connor, & Loomis, 2010)

4.3.2. Hierarhiline RBAC

Paljudes rakendustes on kasutusel hierarhiline rollide ülesehitus, mis põhineb üldistustel ja spetsialiseerumistel. Näiteks inseneri roll võib olla jagunenud riistvara inseneriks ja tarkvara inseneriks, samas võib ta ka ise olla spetsialiseerunud kõrgemast

tasemest. Puustruktuur on üks võimalikke variante rollide hierarhia kuvamiseks (Sandhu et al., 1994, 5). Hierarhiliste grupeeringutega kaasnevad turvapoliitikat puudutavad küsimused. Näiteks, võib eristada rollide õigused ja pääsuload, mis on päritud teistelt rollidelt nendest, mis on antud rollile ainuomased ja ei saa olla päritavad. Vahest võib osutuda vajalikuks kaaluda keeldumisi (negatiivne autoriseerimine) lisaks tavalistele positiivsetele autoriseerimistele.

Hierarhiline RBAC võimaldab luua rollide hierarhiaid, kus emarollid pärivad lapsrollide õigused. Selline lähenemine võimaldab kasutajale määratud rollide ning rollidele määratud pääsuõiguste hulka vähendada. Lähenemise eelduseks on organisatsiooni hierarhiline ülesehitus, vastasel korral võib süsteemi lisanduda keerukust, mis oodatavate kasutegurite mõju vähendavad. RBAC võimaldab rollidel omada kattuvaid õiguseid, seega kasutaja, kes kuulub erinevatesse rollidesse teostab suure tõenäosusega teatud üldiseid toiminguid. Mõningaid üldiseid toiminguid teostatakse tõenäoliselt kõikide kasutajate poolt (Ferraiolo et al., 2001). Seega ei ole üldiseid toiminguid mõttekas paigutada igasse rolli, vaid kasutada võiks rolli hierarhiaid. Rolli hierarhia määratleb rollid, mis on unikaalsete omadustega ning võivad endas sisaldada ka teisi rolle.

4.3.3. Staatiline piiratud RBAC

Selle asemel, et algatada kulukas auditeerimine juurdepääsude jälgimiseks, võivad organisatsioonid kasutada pääsu piiranguid – staatiliselt piiratud RBAC meetodit. Toimingute reeglitega sidumine võimaldab luua komplekti üksteist välistavad rolle, et ei tekiks olukorda, kus kasutajale on määratud ohtlik kombinatsioon õiguseid (kohustuste lahususe tõttu).

4.3.4. Dünaamiline piiratud RBAC

RBAC raamistik annab administraatoritele voli reguleerida tegevusi, mis on rolli liikmetele lubatud. Näiteks võib olla piiratud kasutajate rollidesse määramine. Mõned rollid võivad olla ette nähtud vaid teatud arvule töötajatele. Näiteks võib rolli „direktor“, määrata ainult ühele töötajale korraga. Kasutaja võib saada rolli uueks liikmeks niikaua kuni liikmete arv ei ületa lubatud piiri. (Hu et al., 2006, 18). Erinevus

on selles, et kasutajatele võib määrata üksteist välistavad rolle; aga kasutajad ei saa aktiveerida mõlemat ülesannet samaaegselt. Näiteks võib kasutajal olla võimalik tellida ja kinnitada oste, kuid ta ei saa seda teha ühe ja sama ostu puhul.

Pääsupoliitika valik tuleneb organisatsiooni vajadustest ning süsteemi keerukusest. Tähtis on, et pääsupoliitika valikusse ning analüüsi panustatakse piisavalt ressurssi ning mõistetakse valiku mõju nii infoturbele kui ka hilisemale pääsuõiguste halduse keerukusele. Lisaks pääsupoliitika valikule on tähtis otsustada kuidas seda rakendada ning kuidas rolle hooldada.

4.4. RBAC rakendamine

Rollitehnika ühendab endas organisatsiooni erinevad üksused, sest parim teadmine organisatsiooni ja tehnilise infrastruktuuri kohta pärineb just nendelt (O'Connor, & Loomis, 2010, 43).

Rollitehnika *(role engineering)*

Esimene rollitehnika samm on rollidele nimetuste andmine. See on oluline kuna võimaldab ärikasutajatel paremini mõista rollitehnika protsessi.

Ülevalt alla tehnika *(Top-Down Role Engineering)*

Ülevalt alla rollitehnikat rakendatakse protsesside kirjeldamisena ärikasutaja poolt. Pääsuõiguste analüüsiga tuvastatakse protsessi läbiviimiseks vajalikke volitusi, mille tulemusena määratakse pääsuõigused rollile. Selline lähenemine võib osutuda tööjõu kulukaks, kuid määratleb ärikasutaja vajadusi kõige paremini.

Alt üles tehnika *(Bottom-Up Role Engineering)*

Alt üles tehnika kasutab olemasolevaid pääsuõigusi ning kasutades algoritme grupeerib neid rollideks. Selline lähenemine võimaldab saavutada edu pääsuõiguste turvapoliitikaga vastavusse viimiseks. Kui organisatsioonis ei ole kasutusel soovitav pääsupoliitika, võib tekkida olukord, kus luuakse mittesoovitav pääsupoliitika, mida administreeritakse läbi rollide.

Ärifunktsioonid ja rollid *(Business Function and IT Roles)*

Rollid kujundatakse pääsuõiguste gruppide põhjal, mis peavad olema mõistetavad ka ärikasutajale. Ärifunktsioonidest võib kujundada sarnaseid rolle, nt sekretär ja assistent täidavad erinevaid tööülesandeid, kuid pääsuõigused on neil samad. Siinkohal on mõistlik rollide ökonoomne kasutamine kuigi see võib tekitada segadust.

Rolli elutsükkel *(Role Life-Cycle Management)*

Loodud rolle tuleb regulaarselt hooldada. Sarnaselt pääsuõigustele, tuleb ka rolle kogu elutsükli jooksul analüüsida ja eemaldada rollidest aegunud pääsuõigused. Vastasel juhul võidakse kasutajale omistada ohtlikke kombinatsioone pääsuõigustest, ning soovitud rollidest tulenev kasu ja pääsupoliitika jäävad saavutamata.

RBAC rakendamise, nagu ka pääsuõiguste halduse, raampõhimõtete ning pääsupoliitika aluseks on pääsuõiguste strateegia väljatöötamine.

4.5. Pääsuõiguste strateegia

Planeerimise faasis tuleks määratleda strateegia, määrates pääsuõigustele rakendatavad turvanõuded, mis integreeritakse turvapoliitikaga. Pääsuõiguste strateegias sõnastatud nõuded ja reeglid on aluseks pääsuõiguste haldusele, mis peavad arvestama konkreetse organisatsiooni spetsiaalsete vajadustega. Pääsuõiguste strateegia peaks arvestama alljärgnevate punktidega.

Funktsionaalsus - kasutajatele tuleb garanteerida tööks vajalikud õigused. Rakendada tuleks minimaalõiguste ning teadmistarbe printsiipi.

Risk - riskidega tuleb arvestada pääsuõiguste projekteerimise faasis, samuti peaks riskianalüüs käima koos funktsionaalsete aspektidega, olles kesksel kohal pääsuõiguste määratlemises ja rakendamises. See võimaldab tuvastada potentsiaalseid riske ning pääsuõigustega neid neutraliseerida, piirata ja kontrollida.

Strateegia - tähtis on omada ühtset kontseptsiooni. Komponendid ja nõuded nagu riskijuhtimine, muudatuste haldus, rakendatavuse lihtsus, administreerimise lihtsus, juhtimise lihtsus, täielikkus, läbipaistvus, auditi lihtsus, kulud ja visioon, peavad kõik olema osa strateegiast. Väga tähtis roll on autoriseerimise tiimil, IT ja äriüksuste

koostöö projekteerimise ja rakendamise faasis ning äriüksuste vastutuse võtmine pääsuõiguste juhtimise ja lahenduse jätkusuutlikkuse eest.

Tehniline lahendus - enne tehnilist teostust tuleks tutvuda tootjapoolsete võimalustega tuvastamaks riske, loomaks rolle ja pääsuõigusi ning teostamaks vajalikke administratiivseid- ja kontrollülesandeid, kombineerides neid vajadusel lahendustega teistelt tootjatelt.

Kontseptsioon - rollide väljatöötamisel tuleks järgida selget loogilist kontseptsiooni. Kontseptsiooni toimimiseks on samavõrd tähtis määratleda õiged rollide tüübid ja nende sisu. Analüüsi käigus peaks otsustama, mis on iga rolli eesmärk.

Läbipaistvus - on äärmiselt oluline, et pääsuõiguste kontseptioon ja sellega seonduvad protsessid on lihtsad, kergesti mõistetavad ja kergesti järgitavad nii IT administraatoritele, kasutajatele, äriüksustele kui ka audiitoritele. Vastutavad isikud äriüksustes, protsessiomanikud, andmeomanikud ja rollide omanikud peavad omama selget arusaamist oma rollist ja vastutusalast. Seega, mida läbipaistvamad on protsessid ja tegevused, seda edukam on sisekontrolli süsteem.

Kasutajate administreerimine - kasutajate administreerimine on konfidentsiaalne ja vastutusrikas tegevus ning tuleks teostada ettevaatlikkusega. Kasutaja andmete loomine ja muutmine ning pääsuõiguste jagamine peaks olema automatiseeritud nii palju kui võimalik.

Nimetuste määratlemine - igale autoriseeritavale komponendile nime andmine käib üldise projekteerimise protsessi alla. Oluline on, et pääsuõiguste komponentidele antakse kindlate reeglite alusel nimetused, võttes arvesse ka hilisema hallatavuse.

Peatükis kirjeldatud pääsu reguleerimise poliitikaid analüüsides tundus esmapilgul rollipõhine lähenemine organisatsioonile kõige sobivam kuid lõplikule tulemusele jõudmiseks tuleb teostada pääsuõiguste analüüs.

5. Pääsuõiguste analüüs

Magistritöö praktilise uuringu eesmärk oli välja selgitada hetkel kehtivad pääsuõiguste haldusprotsessid organisatsioonis, võrrelda neid dokumendianalüüsis tuvastatud parimate praktikate ning soovitustega ning jõuda halduskoormust vähendava tulemuseni. Kui ajakohased on kasutajate õigused, milline on rakendatav pääsuõiguste muutmise ja halduse protsess, millised on ilmnenud tüüpvead.

Organisatsioonides töötab üha enam inimesi, mis võib viia pääsuõiguste kaoseni ning ülemääraste õigustega töötajad tõstavad infoturbe riske. Pääsuõiguste efektiivne administreerimine on üks suuremaid väljakutseid tänapäeval. Muutuvad töökohustused ja rollid mõjutavad pääsuõiguste keerukust ja tekitavad probleeme nende haldamisel. Suured turvariskid kaasnevad manuaalse pääsuõiguste haldusega, mille tulemusel võidakse kasutajatele aja jooksul omistada tunduvalt suuremad pääsuõigused, kui neil oma töökohustuste täitmiseks vaja on.

5.1. Planeerimine ja kontseptsioon

Süsteemi turvalisusele tuleb mõelda juba planeerimis faasis ja erilist tähelepanu tuleks pöörata kasutajate pääsuõigustele. Välja tuleks töötada kindel turvapoliitika ja lähtuda tuleks reaalsetest vajadustest. Sellest sõltub väga palju, vastasel korral valmiv lahendus ja hilisemad muudatused võivad osutuda võimatuks või väga keerulisteks.

Pääsuõigustega juhitakse kasutajate ligipääsu andmetele. Andmete turvalisus sõltub seetõttu suurel määral otseselt sellest, kuidas on tehtud erinevad pääsuõiguste seadistused. Soovitud turbe taseme tagamiseks on tähtis pääsuõiguste andmist hoolikalt planeerida ja teostada. Paljud ERP süsteemid võimaldavad pääsuõigusi seadistada rollipõhiselt, määrates rollidele kindlad ligipääsud ja volitused. Rollide kasutamata jätmine võib viia haldusprobleemideni.

5.2. Protsessid

Edukalt juurutatud infosüsteemi valmimisel on tähtis, et pääsuõiguste haldamise protsess dokumenteeritakse. Kindlasti peaks välja töötama ka muudatuste halduse protsessi, milles on kokku lepitud kindlad reeglid kuidas käsitletakse töötaja lahkumist, organisatsiooni sisest liikumist jm. Mismoodi jõuab info pääsuõiguste haldajani? Kuidas hallata töötajate sisemist liikumist? Kuidas liigub sellekohane info ning mida tuleks teha kasutaja pääsuõigustega? Kellega kooskõlastada? Täpse protsessi välja töötamata jätmine võib lõppeda erinevate pääsuõiguste kuhjumisega, mis käib otseselt miinimumõiguste printsiibi vastu. Iga kasutaja tohiks omada ligipääsu ainult sellistele andmehulkadele, mis on tema igapäevatööks vajalikud. Standardiseerimata, rakenduse põhise, kasutajate ja nende pääsuõiguste halduse tulemusel võivad tekkida suured turvariskid töötajatele liigsete õiguste andmisega (Dhillon, 2001).

Lisaks tavapärastele muudatuste haldusega seotud tegevustele, tuleb tähelepanu pöörata ka organisatoorsetele muudatustele. Muudatused organisatsiooni struktuuris puudutavad ka pääsuõigusi. Enne selliste muudatuste rakendamist tuleks alati analüüsida nende mõju infoturbele. Kuna pääsuõigused võivad olla otseselt seotud organisatsiooni struktuuriga, mille põhjal on pääsuõiguste hierarhia üles ehitatud, siis igasugused muudatused avaldavad pääsuõigustele otsest mõju. Analüüsi tegemata jätmine võib põhjustada kattuvaid profiili seadistusi, kus rakendatakse kõige väiksema piiranguga õiguseid (Hu et al., 2006).

Samuti võivad süsteemis toimuda teatud pääsuõiguste seadistustes kasutusel olevate parameetrite tunnuste muutumised. Sellisel juhul on tähtis, et see info jõuaks pääsuõiguste eest vastutavale administraatorile. Protsessid, mis otseselt mõjutavad infosüsteemi käideldavust tuleb kindlasti eelnevalt kaardistada.

Töökohustustest tulenevalt võivad infosüsteemi tekkida profiilid, mis on loodud konkreetsete kasutajate jaoks. Kasutaja kustutatakse töötaja organisatsioonist lahkudes, kuid profiilid jäetakse alles. Ajapikku võib selliste orbude nimekiri kasvada ja administraatoril tuleb üha pikemaid profiili nimekirju hallata.

Iga infosüsteem on erinev ja pääsuõiguste haldusmetoodika samuti. Tähtis on, et infosüsteemi juurutades pööratakse piisavalt tähelepanu mitte ainult pääsuõiguste

andmisele, vaid ka hilisemale haldusele, võttes arvesse kõik lahendusega kaasnevad nüansid. Paljud neist ei pruugi kohe hoomatavad olla ja ilmnevad alles aja möödudes. Kaardistatud peaksid olema kõik pääsuõigusi mõjutavad atribuudid ja protsessid kuidas see info jõuab pääsuõiguste haldurile.

5.3. Vastutajad

Ka kõige paremates turvapoliitikates ja turbefunktsioonidest pole kasu, kui neid eiratakse või ei rakendata. Kokku tuleb leppida, kes vastutab konkreetse infosüsteemi turbega seotud ülesannete eest ning kelle vastutada on pääsuõiguste regulaarse kontrolli läbiviimine. Pääsuõiguste valdkonnaga seotud tegevuste jaoks tuleb defineerida vastavad protsessid ja need omakorda detailselt välja töötada. Lisaks tuleb kõikide protsesside puhul määratleda töötajate vastutusalad. Niimoodi minimeeritakse turvaaukude tekkimine, mis on tingitud vastutuse ebaselgest kehtestamisest või vajalike protsesside poolikust väljatöötamisest (Nwafor et al., 2012).

Vastutajate alla võib klassifitseerida ka andmeomanikud. Paljudes ERP süsteemides on seadistatud andmeomanikud, kes vastutavad teatud eelnevalt määratletud andmete eest. Andmeomanikul on õigused teostada teatud toiminguid, mis ei ole lubatud teistele kasutajatele. Tähtis on omada ülevaadet vastutajatest ning kasutajate lahkumisel/liikumisel uued andmeomanikud määratleda.

5.4. Pääsuõigused

Uuringu aluseks olevas süsteemis on kasutusel rakenduse sisene pääsuõiguste haldus. Kogu pääsuõiguste süsteem on jaotatud nelja loogilisse rühma:

Kasutajad – kasutajate loomine ja haldus. Igal kasutajal on oma kasutajanimi, mis on seotud tema *Active Directory* ehk aktiivkataloogi kasutajaga.

Tiimid – tiimide loomine ja haldus. Tiimid annavad kasutajale ligipääsu töövoogudele ja tiimipõhistele dokumendikaustadele.

Ülesandepõhised profiilid – funktsionaalsete õiguste profiilide loomine ja haldus. Ülesandepõhine profiil annab kasutajale õiguse kindlateks funktsioonideks. Ülesandepõhised profiilid on rollidele võrdsed ja võimaldavad pääsuprofiilidega sidumist.

Andme pääsuprofiil – andmekaitse profiilide loomine ja haldus. Annab kasutajale õiguse näha või muuta teatud andmeregiooni andmeid. Iga profiil annab ligipääsu teatud andmeregioonile.

ERP on moodultarkvara, kus andmeid turvatakse erinevate atribuutide alusel (Joonis 9).

Turvatud	Mudel 1	Mudel 2	Mudel 3	Mudel 4	Mudel 5
Atribuut 1		x		x	
Atribuut 2		x			x
Atribuut 3	x		x	x	
Atribuut 4			x		x
Atribuut 5		x			

Joonis 9. Turvatavad atribuudid

Pääsuõigused peavad tagama/piirama iga mudeli puhul ligipääsu turvatava atribuudi komponendile.

5.5. Metoodika

Pääsuõiguste turvapoliitikale vastavuse väljaselgitamiseks teostas autor esmalt pääsuõiguste revisjoni. Seejärel viis autor läbi intervjuud turvapoliitikas määratletud pääsuõiguste valideerijatega, mille käigus lepiti kokku pääsuõiguste valideerimise metoodika.

Autori pakkus välja pääsuõiguste taotluse vormi kasutuselevõttu, mis annab suuniseid pääsuõiguse taotlejale vajaminevatest atribuutidest. Selline lähenemine kiirendab tunduvalt pääsuõiguste haldusprotsessi kuna valideerimisele kulub vähem aega (Lisa 2). Intervjuude käigus kooskõlastas autor valdkonna eest vastutava organisatsiooni töötajaga tema vastutusalasse jäävate töötajate pääsuõigused.

Peale valdkonnajuhtide poolt kinnitatud pääsuõiguste kaardistamist, testis autor nende õiguste toimivust ja viis rakenduses kajastuvad õigused vastavusse analüüsidokumendiga.
Teises etapis kaardistas autor kasutusel olevaid pääsuõiguste elutsükli haldusega seonduvaid tegevused. Protsessis tuvastas autor mitmeid puudusi, mille tulemusena täiendas turvapoliitikat.

Kasutajad tegutsevad tavaliselt oma kasutaja kontoga lubatavate pääsuõiguste piires, mis tähendab seda, et kasutajate liigsed pääsuõigused soodustavad andmete väärkasutust.

ContROLE on metoodika ja vastav tööriist, mis toetab struktureeritud identiteedi haldus protsessi (Fuchs & Pernul, 2010, 2). Eelnevalt mainitud tööriista autor ei kasutanud ja rakendas metoodikas väljatoodud ettepanekuid excelis.

Antud metoodika pääsuõiguste haldamisprotsessi saab jagada kahte gruppi: andmete kogumine ja rollide väljatöötamine. Autor rakendas andmete kogumise protsessi. Detailsemalt vaadates moodustub 6 faasi:

- kasutajakontode, pääsuõiguste, organisatsiooni struktuuri kirjeldava informatsiooni kogumine;
- andmete puhastamine;
- ühiste juurdepääsu omaduste tuvastamine ja grupeerimine;
- põhirollid;
- organisatsioonilised rollid;
- funktsionaalsed rollid.

Esmalt keskendutakse informatsiooni kogumisele, seda nii organisatsiooni struktuuri, kui kasutaja kontode ja pääsuõiguste kohta. Järgneb andmete puhastamine tuvastamaks süntaktilisi ja semantilisi vigu ning orvuks jäänud kontosid ning grupeeritakse pääsuõigused töö funktsioonidele tuginedes gruppidesse luues aluse rollipõhise pääsupoliitika rakendamiseks.

Andmete kogumine

Selleks, et alustada andmete puhastamise, ettevalmistamise ja rollide väljatöötamisega on vaja andmed ette valmistada. Andmed tuleks koguda nii organisatsiooni struktuuri,

olemasolevate rollide, tööprofiilide, kasutusel olevate kasutajakontode ja pääsuõiguste kohta.

Andmete puhastamine

Andmete puhastamise eelduseks on eelmises faasis teostatud andmete kogumine. Selle faasi peamine ülesanne on tõsta andmekvaliteeti, tuvastada vigu ja vastuolusid ning orbudeks jäänud kontosid või pääsuõiguseid, mis ületavad töötajale tarvilikke õigusi tööülesannete täitmiseks (Fuchs & Pernul, 2013, 4). Andmete puhastamiseks saab kasutada nii süntaktilisi kui semantilisi kontrolle, millest süntaktilisi on võimalik automatiseerida aga semantilisi vigu saab tuvastada vaid inimene.

Süntaktilise analüüsi eesmärgiks on tuvastada kehtetuid andmeid nagu valed atribuudiväärtused, duplikaadid ning rikkumisi viitetervikluses (*referential integrity*) (Fuchs & Pernul, 2013).

Semantiline analüüs keskendub pääsuõiguste, töötajate ja organisatsiooni hierarhia vahelistele suhetele, võimaldades tuvastada töötajaid, kelle pääsuõigused ei vasta nende töö funktsioonidele. Samuti pääsuõigustele, mis ei ole enam kasutusel, kuid on endiselt kasutajatele määratud ning pääsuõigustele, mis on määratud peaaegu kõikidele kasutajatele.

5.6. Analüüsi tulemused

Efektiivselt töötajate konfidentsiaalsele informatsioonile ligipääsetavuse administreerimine võib osutuda üheks suurimaks turvalisuse väljakutseks. Käsitsi pääsuõiguste ja kasutajate loomine, uuendamine, kustutamine, lisamine ja vähendamine võivad viia aja jooksul erinevate õiguste kuhjumiseni. Selle tulemusena ei pruugi administraatoritel olla enam võimalik käsitsi uuendada ja kontrollida ajalooliselt kasvanud pääsuõigusi selleks, et vähendada turvariske ja rikkumisi.

Uurimuse aluseks olevas organisatsioonis on toimunud palju muudatusi nii struktuuris kui protsessides. Uurimuse aluseks oleva statistika (Tabel 1).

Tabel 1. Pääsuõiguste statistika organisatsioonis.

Pääsu reguleerimise element	Kokku
Kasutajate arv	318
Tiime	29
Ülesande põhist profiili	28
Andme pääsuprofiile	466
Pääsuõiguseid	2972
Hierarhia elemente	1801

Autor teostas andmete puhastamiseks nii süntaktilisi kui ka semantilisi kontrolle. Süntaktilise analüüsi tulemusel tuvastas autor 87 kehtetut hierarhilist elementi. Sellised vead kipuvad tekkima kui organisatsioonis toimuvad struktuurimuudatused või kui kasutusel on hierarhilisi dimensioone mille muudatused ei kajastu pääsuõigustes. Kehtetud hierarhilised elemendid võivad tekkida mistahes pääsuõigustes kasutusel oleval atribuudil. Süntaktiline analüüs peaks kaasama kõik hierarhilised atribuudid, mis on pääsuõiguste kontrolliks kasutusel.

Viitetervikluse kontroll tuvastas 282 töötajat kellele oli määratud kattuvaid hierarhilisi elemente. Sellised kattuvused võivad tekkida juhul kui töötaja organisatsiooni siseselt töökohta vahetab. Samuti tuvastas autor 159 orvuks jäänud andme pääsuprofiili, mis ei olnud seotud ühegi kasutajaga. Süntaktilise analüüsi tulemusena vähenes andmete pääsuprofiilide arv 306-le ja kasutajate arv 308-le.

Semantiline andmete puhastus võimaldab tuvastada pääsuõiguseid, mis ei ole enam kasutusel või sisaldavad kehtetuid atribuute. Semantilise ja süntaktilise analüüsi mõju organisatsiooni pääsuõigustele (Tabel 2).

Tabel 2. Andmete puhastuse mõju organisatsiooni pääsuõigustele.

Pääsu reguleerimise element	Enne puhastamist	Peale puhastamist	Vähenemine
Kasutajate arv	318	308	3,14%
Andme pääsuprofiile	465	306	34,19%
Pääsuõiguseid	2872	1941	32,42%
Hierarhia elemente	1801	1714	4,83%

Infosüsteemis on seadistatud tiimid, mis on kasutajate profiili lisatud aga ei ole seotud ühegi pääsuprofiiliga. Olemasolevatesse tiimidesse tuleks lisada vastavad volitused, nii saaks kasutajate volitusi juhtida läbi nende tiimikuuluvuse.

Infosüsteemis oli valesti seadistatud 311 kasutaja profiilid kus esines duplitseerivaid volitusi ja teineteist välistavaid õiguseid mille puhul rakendub väikseima piiranguga reegel. Samuti ei arvestanud hetkel seadistatud pääsuõigused hierarhiatest tulenevate reeglitega, kus rakendatakse alati väikseimaid piiranguid. Selgus, et 318 kasutajast 254 näeb rohkem andmeid kui lubatud. See on otseselt vastuolus minimaalõiguste printsiibiga. Muuhulgas tähendab see ka seda, et ühe osakonna töötaja ei tohiks ligi pääseda teiste osakondade infole kui see ei ole just tööülesannete täitmiseks vajalik. Nendest 254 kasutajast 79 olid seadistatud volitamata kirjutamisõigused, mis võimaldavad kasutajal väljaspool oma volituste piire muudatusi teha. Kokkuvõte seadistusvigadest (Tabel 3).

Tabel 3. Kokkuvõte seadistus vigadest.

Pääsu reguleerimise element	Kasutajate arv	Ületatud õigused	Protsent
Vaatamis õigused	318	254	79,87%
Kirjutamis õigused	318	79	24,84%
Valesti seadistatud profiilid	318	311	97,80%
Seadistusvigu	318	644	202,51%

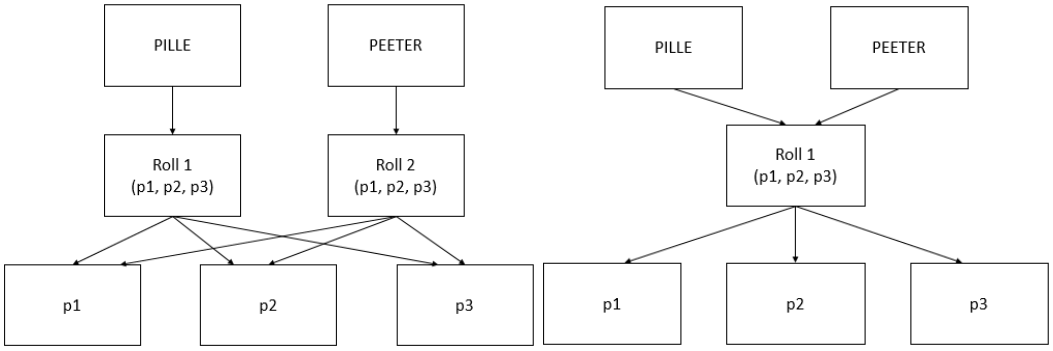
Pääsuõiguste seadistamine vajab põhjalikku analüüsi ja õiguste lisandumisel tuleks alati kasutaja olemasolevad õigused tervikuna üle vaadata. Kokku tuvastas autor 644 seadistus viga.

5.7. Pääsupoliitika valik

Pääsupoliitika valikul tuleb eelnevalt kindlaks teha, kas organisatsioonil on mingi eelnev pääsupoliitika. Kuna uuritavas organisatsioonis ei ole väljakujunenud pääsupoliitikat, siis on vajalik analüüsida, milline poliitika neile kõige paremini sobiks.

Rollitehnika sisaldab endas rollide ekstraktimist olemasolevast infrastruktuurist. Seda tegevust võib alustada nii ülevalt alla kui ka alt üles tehnikaga kus aluseks võetakse olemasolevad andme pääsuõigused ning kasutajad ja otsitakse seoseid. Autor kasutas graafilist lähenemist kuvamaks kasutajad ja nende pääsuõiguseid ning süsteemis seadistatud tiime ja nende kasutajaid. Sellise meetodiga on võimalik lihtsalt ja ilma

tehniliste vahenditeta saada visuaalne ülevaade ühistest mustritest, mis kasutajate vahel eksisteerivad (Joonis 10).

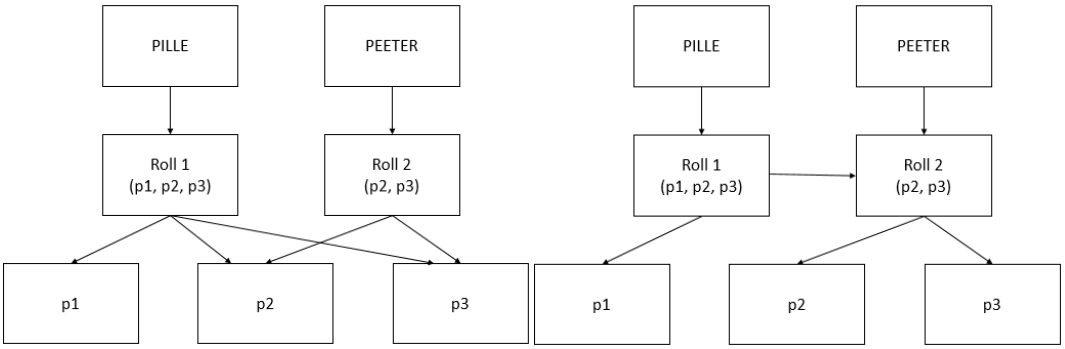


a) Enne mestimist b) pärast mestimist

Joonis 10. 2 rolli mestimine (Zhang, Ramamohanarao, & Ebringer, 2007, lk 5).

Jooniselt 10 on näha kuidas kasutajate Pille ja Peeter pääsuõigused kattuvad võimaldades kujundada rolli.

Hierarhiline RBAC võimaldab rolle hierarhiliselt üles ehitada (Joonis 11).



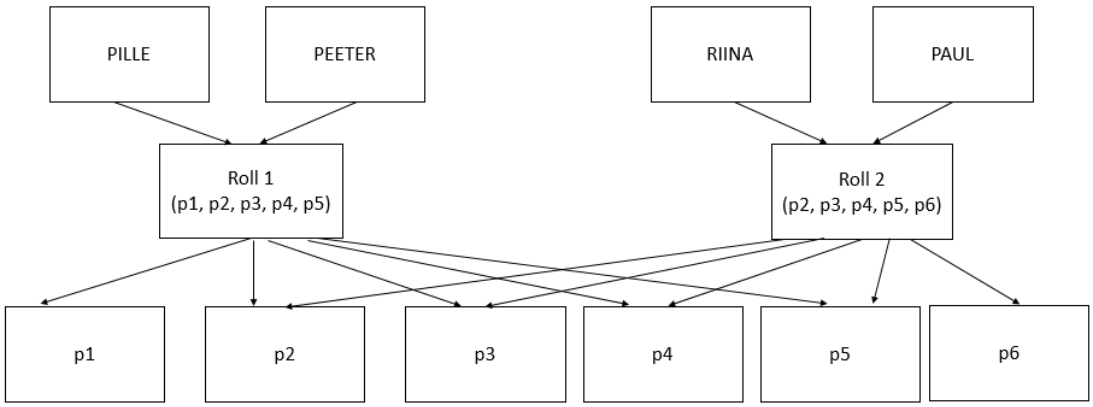
a) Enne mestimist b) pärast mestimist

Joonis 11. Üks roll on teise alamroll (Zhang et al., 2007, lk 5).[1]

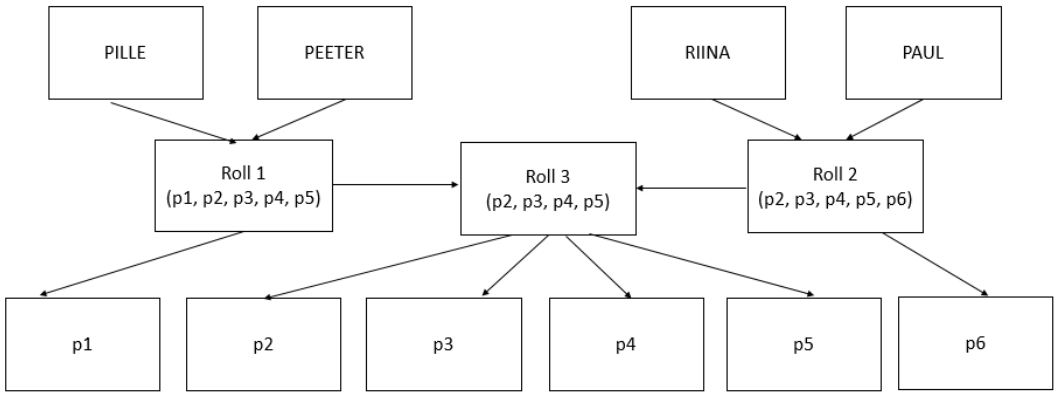
Jooniselt 11 on näha kuidas pärast mestimist on kasutaja Pillel õigus rollile 1 kuid pääsuõigused pärib ta ka rollilt 2. Kokku on kasutajal Pille ligipääs pääsuõigustele p1, p2 ja p3.

Graafiline lähenemine võimaldab tuvastada potentsiaalseid rolle (Joonis 12).

[1] k – kasutaja; p-pääsuõigus; t-ülesandepõhine profiil



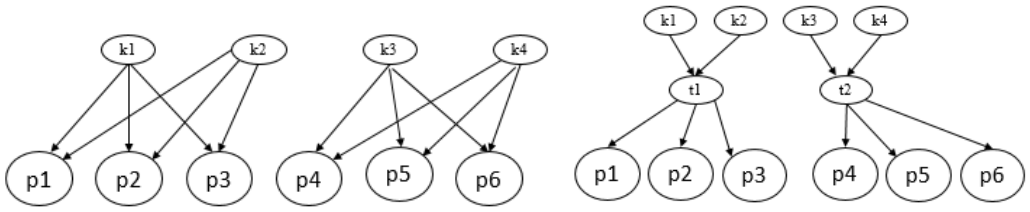
a) Enne mestimist



b) pärast mestimist

Joonis 12. Rollid, millel on sarnased pääsuõigused (Zhang et al., 2007, lk 5).

Ülesandepõhised profiilid antud kontekstis on võrdsed rollidele kuna võimaldavad siduda kasutaja pääsuõigusega (Joonis 13).



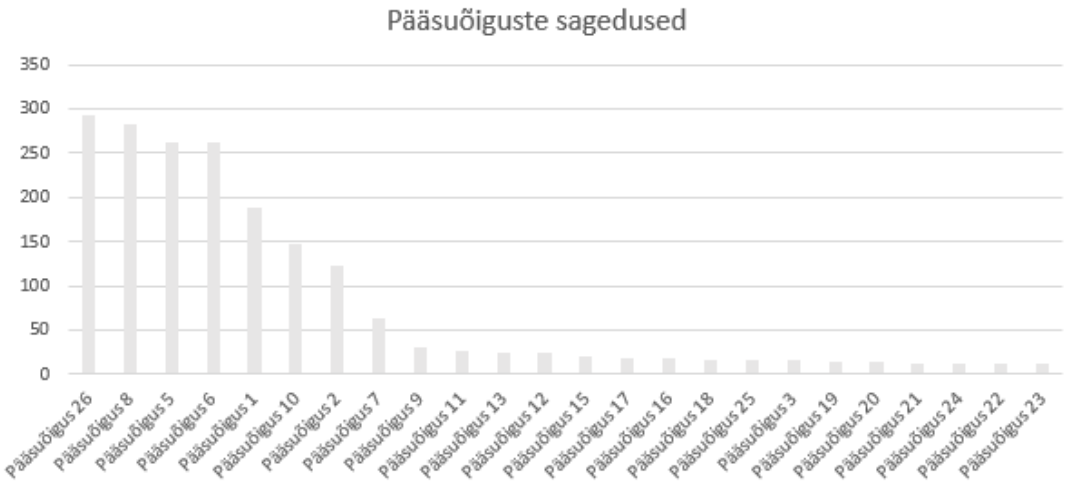
a) Kasutajatele määratud pääsuõigused b) pääsuõigused läbi profiilide

Joonis 13. Pääsuõiguste tagamine läbi profiilide

Võttes aluseks kasutajatele määratud tiimikuuluvuse ja määratud andme pääsuõigused tuvastas autor 19 potentsiaalset rolli.

Alternatiivina analüüsis autor pääsuõiguste sagedusi tuvastamaks pääsuõiguseid, mis on kõikidel kasutajatel eesmärgiga tuvastada komplekte rollidest, mis võiksid olla kasutusel kui profiilid. Selliste komplektide rollidesse jagamise eeliseks on võimalus tagada kasutajatele ligipääs süsteemile koheselt seniks kuni täpsemad nõuded on veel kinnitamisel.

Analüüsi tulemused võimaldasid tuvastada võimalikke pääsuõiguste gruppe, ehk potentsiaalseid rolle, mis tagavad ligipääsu süsteemile (Joonis 14).



Joonis 14. Pääsuõiguste esinemis sagedused kasutaja kohta

Autor tuvastas, et ainult rollipõhine pääsupoliitika ei ole lahenduseks halduskoormuse vähendamisel ning otsustas rakendada kombineeritud mudelit kus lisaks rollidele määratakse kasutajatele pääsuõiguseid ka atribuudi põhiselt nagu näiteks osakond. Seda põhjusel, et iga kasutaja kuulub ühte või enamasse üksusesse, mis suures organisatsioonis kasvataks rollide arvu haldamatuks ning oodatava kasu asemel tekiks oht rollide plahvatusele.

Rolli hierarhiate kasutamine organisatsioonis ei tundu autorile otstarbekas kuna analüüsi tulemused viitavad väga laiale ja pikale hierarhiale, mis suurendaks veelgi pääsuõiguste halduse keerukust.

Kokkuvõtvalt võib öelda, et pääsupoliitika valik on strateegiline otsus kuna võimaldab kokku hoida ressurssi, halduskulusid ning vähendab turvaintsidentide realiseerumise tõenäosust. Pealtnäha organisatsiooni vajadustele vastav pääsupoliitika ei pruugi seda olla pärast analüüsi. Sellest tulenevalt tasub panustada analüüsi ja kaaluda erinevaid alternatiive.

Ettepanekud

Tulenevalt pääsuõiguste analüüsi tulemustest ning peatükis 3 ERP pääsuõigused ning 4 pääsu reguleerimine refereeritud teoreetilisele materjalile teeb magistritöö autor järgmised ettepanekud.

1. **Pääsuõiguste turvapoliitika väljatöötamine**

Vältimaks informatsiooni kättesaadavusega kaasnevaid riske on tähtis välja töötada põhjalik turvapoliitika andmete kaitsmiseks. Üldisest turvapoliitikast ei piisa, pääsuõiguste turvapoliitika peaks olema osa üldisest turvapoliitikast sisaldades reegleid ja piiranguid pääsuõiguste andmiseks ja tühistamiseks. Autor soovitab täiendada olemasolevat pääsuõiguste turvapoliitikat määratledes vastutajad, protsessid ning pääsuõiguste valideerimise protsessi. Tähtis on turvapoliitika regulaarne täiendamine ning organisatsiooni äristrateegiaga vastavusse viimine.

2. **Muudatuste halduse protsessi täiendamine.**

Muudatused äriprotsessides ning organisatsioonis kajastuvad ERP süsteemis. Sellest tulenevalt on oluline, et muudatuste haldus protsessi käigus teostatud tegevused oleksid dokumenteeritud ning kooskõlastatud pääsuõiguste halduse eest vastutava isikuga. Tähtis on, et muudatused kajastuksid pääsuõigustes ning oleksid enne teostust analüüsitud ja testitud.

3. **Teavitused personaliosakonnast.**

Informatsioon kasutajate lahkumise kohta organisatsioonist peab jõudma ka pääsuõiguste haldajani. Kasutaja tuleks süsteemist eemaldada. Samuti tuleb kasutaja eemaldada test keskkondadest. Lisaks tuleb käsitleda töötaja liikumist teisele ametikohale või üksusesse, sellekohane informatsioon peab jõudma pääsuõiguste haldajani ning muudatused tuleks sisse viia nii töö- kui test keskkondades.

4. **Pääsuõiguste elutsükli määratlemine.**

Pääsuõiguste elutsükkel on protsess, mis peaks olema välja töötatud turvapoliitika käigus. Tähtis on määratleda kindlad protsessi sammud, tegevused, vastutajad ning tegurid, mis võimaldavad pääsuõiguste haldus protsessi optimeerida ja vähendada halduskoormust. Vastasel korral võib pääsuõiguste haldusest saada täiskoormusega

töökoht, kus põhirõhk ei ole pääsuõiguste andmisel või võtmisel vaid kasutajapöördumistega tegelemisel.

Autor tuvastas mitmeid puudujääke kasutajakonto elutsükli haldus protsessis ning soovitab rakendada töös kajastatud kasutajakonto haldus soovitusi ning kasutusele võtta pääsuõiguste taotluse vormi (Lisa 2).

5. **Pääsupoliitika valik.**

Rollide ja nendega seotud volituste defineerimine peab lähtuma organisatsiooni vajadustest. Tähtis on tagada, et kui töötaja vahetab organisatsiooni sees tegevusvaldkonda, ei saaks enam kasutada seni kehtinud volitusi. Kui organisatsioonis on kasutusel rollid siis tasuks teostada pidevat seiret minimeerimaks rollide arvu. Rollide arv suurendab süsteemi halduse keerukust ning pääsuõiguste teostamisele kuluvat aega.

Uuringust selgus, et organisatsioonis ei kasutata rolle ning autor analüüsis, kas olemasolevat pääsupoliitika haldust on võimalik optimeerida. Rollide väljatöötamine ja optimaalse lahenduse leidmine on ajamahukas ning sellest tulenevalt tasub analüüsile panustada vältimaks järelevalve koormust suurendavat lahendust.

Autor tuvastas, et rollipõhine lähenemine ei ole kõige parem lahendus antud organisatsiooni ERP süsteemile ning soovitab rakendada kombineeritud mudelit, milles baas õigused tulenevad rollidest tagades kiire ligipääsu süsteemile. Valideerimise tulemusena täiendatakse kasutaja pääsuõigusi atribuudi põhiselt. Uuringust selgus, et süsteemi kasutab suur grupp peakasutajaid kelle pääsuõigused on identsed ning võiksid sisalduda peakasutaja rollis.

6. **Pääsuõiguste haldus protsessi muutmine.**

Pärast pääsuõiguste seadistust on üheks suurimaks väljakutseks õiguste operatiivne ja strateegiline haldus. Reaalsuses seisavad paljud organisatsioonid vastamisi aegunud ja vigaste rollide seadistustega, mis põhjustavad turvanõrkusi ja rikkumisi. Efektiivne pääsuõiguste haldus eeldab turvapoliitika väljatöötamist ning protsesside optimeerimist, mis tagab nii kasutajate rahulolu kui infoturbe poliitikale vastavuse. Organisatsioonis rakendatav pääsuõiguste haldus protsess ei ole ammendav ning vajab täiendamist vähendamaks töökoormust ning seadistus vigade arvu.

7. **Tõsta infoturbealast teadlikkust.**

Intervjuudest selgus, et infoturbe alase teadlikkuse tase organisatsioonis on erinev ning oluline oleks läbi viia koolitused tippjuhtkonnale, spetsialistidele ning administraatoritele. Kui tippjuhtkonna ja spetsialistide koolitusvajadus on pigem teadlikkuse tõstmine siis administraatoritele oleks soovitatav praktiline koolitus.

Kokkuvõte

Magistritöö eesmärgiks oli anda ülevaade ERP süsteemidest, pääsuõiguste haldusest, pääsuõiguste mõistest, elutsüklist ning viia läbi uuring, et analüüsida pääsuõiguste haldust organisatsiooni ERP süsteemis. Analüüsida erinevaid pääsuõiguste poliitikaid ning valida välja sobivaim organisatsiooni ERP süsteemile. Töö eesmärgiks ei olnud kirjeldada kõike pääsuõiguste haldusega seonduvat detailselt vaid anda ülevaade ning rõhutada infoturbe olulisust.

Magistritöö teema on eriti oluline ERP süsteemi kontekstis, kuhu on koondatud kogu ettevõtet puudutav informatsioon ning milles sisalduvat infot võib klassifitseerida ärisaladuseks. ERP süsteemide üheks suurimaks kasuteguriks on võimekus reaalajas edasi anda organisatsioonis toimuvat. Turvapoliitika väljatöötamine on oluline andmete kaitsmiseks ja riskide maandamiseks. Süsteem millesse on koondatud kogu äri puudutav juhtimisinfo vajab kaitsmist nii organisatsiooni seest tulenevate riskide kui ka väliste ohtude eest. Turvapoliitikate ja protsesside puudulikkus võib põhjustada organisatsioonile tõsiseid infoturbe intsidente.

Töö praktilises osas viis autor läbi juhtumiuuringu ERP süsteemi kasutatavas organisatsioonis. Uuringu eesmärgiks oli välja selgitada kuidas on korraldatud pääsuõiguste haldus, elutsükkel ning viia läbi pääsuõiguste revisjon.

Kogutud informatsiooni analüüsimisel selgus, et organisatsiooni ERP süsteemis puudub kindel pääsuõiguste haldusprotsess ning rakendatud protsessis tuvastati mitmeid puudujääke. Autor viis läbi organisatsiooni ERP süsteemi kasutajate pääsuõiguste revisjoni ning intervjuud vastutavate isikutega tuvastatud puuduste kõrvaldamiseks. Kokku on süsteemis 318 kasutajat ning esines 644 tuvastatud seadistus viga. Tuginedes praktilisele ja teoreetilisele uuringule oli võimalik tuvastatud puudusi analüüsida.

Uuringu tulemusena kaardistas autor tuvastatud puudused ning tegi ettepanekud nende kõrvaldamiseks ning edasiseks halduskoormuse vähendamiseks.

Uuringu tulemustest võib järeldada, et pääsuõigustega tuleb tegeleda minimeerimaks infoturbe riske. ERP süsteemid liiguvad üha enam pilvepõhiste ja teenusepõhiste

lahenduste poole, mis suurendavad infoturbe riske tuues endaga kaasa täiendavaid turbenõudeid.

Magistritöö peaks andma riskianalüüsiga tegelevatele organisatsioonidele ning IT spetsialistidele ülevaate pääsuõiguste haldusest. Nende alusel peaks IT turvalisuse eest vastutavad isikud saama ettekujutuse pääsuõiguste haldustegevustest ning pääsuõiguste elutsüklist. Pääsuõigustega tuleb tegeleda olenemata infosüsteemist seega on see teema aktuaalne ning rakendatav laiemalt.

Üks magistritöö eesmärkidest oli tõsta pääsuõiguste alast teadlikkust organisatsioonis. Töö praktilises osas läbi viidud intervjuude tulemusena on autor saanud positiivset tagasisidet intervjueeritavatelt pääsuõiguste taotlus vormi kasutuselevõtu ning pääsuõiguste halduskoormuse vähenemise kohta.

Töö edasiarendusena oleks kindlasti antud teemal võimalik olulisemalt põhjalikumaid ülevaateid, analüüse ja uurimusi teostada, mis aga töö teema tundlikkust arvestades võib osutuda keeruliseks ning jäi seetõttu antud uuringu raames teostamata.

Kasutatud kirjandus

Benantar, M. (2006). *Access Control Systems - Security, Identity Management and Trust Models.* Springer.

Boyd, C., *5 ERP Trends.* (30.01.2017). Software Advisory Service. Loetud aadressil http://www.softwareadvisoryservice.com/software-solutions/erp/5-erp-trends-2017/

Business Wire. (2015). IDC Forecasts U.S. Mobile Worker Population to Surpass 105 Million by 2020. Loetud aadressil http://www.businesswire.com/news/home/20150623005073/en/IDC-Forecasts-U.S.-Mobile-Worker-Population-Surpass

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. (2007). *Role-based access control*. Artech House.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, *4*(3), 224-274.

Gartner, Inc. (2014). *Postmodern ERP – Key Trends*. Loetud 11. veebruar 2017 aadressil http://www.afsug.com/library/documents/saphila2014_presentations/Day1/CINEMA_2/Postmodern%20ERP%20-%20Key%20Trends.pdf

Ghosh, R. (2012). A comprehensive study on ERP failures stressing on reluctance to change as a cause of failure. *Journal of Marketing and Management*, *3*(1), 123.

Hanson, V., M., Buldas, A., Veldre, A., Laur, M. & Krasnosjolov, J. (2011). *Andmekaitse ja infoturbe seletussõnastik Inglise-Eesti.* Cybernetica AS.

Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Scarfone, K. (2013). Guide to attribute based access control (ABAC) definition and considerations (draft*). NIST special publication*, 800(162).

Hu, V. C., Ferraiolo, D., Kuhn, D. R. (2006). *Assessment of access control systems.* US Department of Commerce, National Institute of Standards and Technology.

ITIL (kuupäev puudub). *What is Access Management*. Loetud 25. veebruar 2017 aadressil http://www.bmc.com/guides/itil-access-management.html

Jankowski, S., Covello, J., Bellini, H., Ritchie, J., & Costa, D. (2014). The Internet of Things: Making sense of the next mega-trend. *Goldman Sachs*.

Kuhn, D. R., Coyne, E. J., & Weil, T. R. (2010). Adding attributes to role-based access control. *Computer*, *43*(6), 79-81.

Latham, D. C. (1986). Department of defense trusted computer system evaluation criteria. *Department of Defense*.

Leon, A. (2008). *Enterprise resource planning Third edition*. Tata McGraw-Hill Education.

Linkies, M., & Karin, H. (2011). *SAP security and risk management*. — 2nd ed. Galileo Press

Marnewick, C., Labuschagne, L. (2006) *A security framework for an ERP system*. Loetud 13. veebruar 2017 aadressil http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/009_Article.pdf

Nwafor, C. I., Zavarsky, P., Ruhl, R., & Lindskog, D. (2012, June). A COBIT and NIST-based conceptual framework for enterprise user account lifecycle management. In *Internet Security (WorldCIS), 2012 World Congress on* (pp. 150-157). IEEE.

O'Connor, A. C., & Loomis, R. J. (2010). 2010 economic analysis of role-based access control. *NIST, Gaithersburg, MD, 20899*.

Panorama Consulting Solutions, (2014). *2014 Erp report*. Loetud 22. märts 2017aadressil http://panorama-consulting.com/resource-center/2014-erp-report/

Panorama Consulting Solutions, (2016). *2016 2017 Top 10 ERP Systems Rankings Report*. Loetud 15. veebruar 2017 aadressil http://email.panorama-consulting.com/TCTUH0R05000gJS20x8bwX0

Panorama Consulting Solutions, (2016). *Clash of the titans 2016, An Independent Comparison of SAP, Oracle, Microsoft Dynamics and Infor.* Loetud 15. veebruar 2017 aadressil http://email.panorama-consulting.com/G5J0XH20gm8CU0wx0000RTb

Pernul, G., & Fuchs, L. (2010). Reducing the Risk of Insider Misuse by Revising Identity Management and UserAccount Data. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (JoWUA)*.

Põldmaa, H. (2016). *Infoturbe haldus.* Loeng, Tallinn.

Rayner, N., & Woods, J. (2011). ERP strategy: why do you need one and key considerations for defining one. *Gartner RAS Core Research*, *2*(4), 1-9.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1994, December). Role-based access control: A multi-dimensional view. In *Computer Security Applications Conference, 1994. Proceedings., 10th* Annual (pp. 54-62). IEEE.

Seo, G. (2013). *Challenges in implementing enterprise resource planning (ERP) system in large organizations: similarities and differences between corporate and university environment* (Doctoral dissertation, Massachusetts Institute of Technology).

Sumner, M. (2000). Risk factors in enterprise-wide/ERP projects. *Journal of information technology*, *15*(4), 317-327.

TNS, *The Security Framework for Information Technology*. (kuupäev puudub). Loetud 23. veebruar 2017 aadressil: http://www.tns.com/it_security_framework.asp

Walther H. (2015). *RBAC first – ABAC next, or what?* GenericIAM Blog. Loetud 05. märts 2017 aadressil http://genericiam.blogspot.com.ee/2015/10/rbac-first-abac-next-or-what.html

ERP-süsteem. (kuupäev puudub). *Wikipedia.* Loetud 15. aprill 2017 aadressil http://wiki.eek.ee/index.php/ERP-süsteem

Wilding, E. (2003). Corporate cybercrime trends. *Computer Fraud and Security*, *6*, 4-6.

Windley, P. (2005). *Digital Identity.* O'Reilly.

Zhang, D., Ramamohanarao, K., & Ebringer, T. (2007, June). Role engineering using graph optimisation. In *Proceedings of the 12th ACM symposium on Access control models and technologies* (pp. 139-144). ACM.

Summary

Title: Analysis of the ERP System Access Privileges Management: the Business Case.

Enterprise Resource Planning (ERP) system is an integrated, configurable, and tailorable information system, which plans and manages all the resources and their use in the enterprise, and streamlines and incorporates the business processes within and across the functional or technical boundaries in the organization. With ERP, an enterprise can automate its fundamental business applications, reduce the complexity and the cost of the collaboration, force the enterprise itself to take part in the Business Process Reengineering (BPR) to optimize its operations, and finally result in a successful business.

ERP is the technology that provides the unified business function to the organization by integrating the core processes. ERP now is experiencing the transformation that will make it highly integrated, more intelligent, more collaborative, web-enabled, and even wireless. The ERP system is becoming the system with high vulnerability and high confidentiality in which the security is critical for it to operate.

Businesses today are experiencing a problem with managing information security. The importance of technological controls should not be underplayed, but evidence suggests that the violation of safeguards by trusted personnel of an organization is emerging as a primary reason for information security concerns. These insiders could be dishonest or disgruntled employees who would copy, steal, or sabotage information, yet their actions may remain undetected.

With the complexity posed by user account management for organizations, the need to implement an effective user account management process to help address possible risks to information cannot be overstated. The need to implement a user account lifecycle management framework has resulted in the development of the EUALMF framework. With the sample implementation flow diagram as a guide, organizations can implement the various stages of the EUALMF as appropriate for their business needs.

Access management is a simple concept. Every business has information that needs to be protected from unauthorized disclosure. To protect information, companies define policies that govern who can access specific classes of business and/or personal information.

In this project, I have underlined the importance of the strategic management of access rights in order to keep the definitions up to date and minimize security vulnerabilities and compliance violations. Overlapping access rights or misconfigurations should be cleansed before change requests are handled within application systems. Additionally, managing access rights with complex organizational hierarchies can be a challenge. In those cases, interdependencies due to inheritance relationships need to be thoroughly considered in order to correctly rate and improve access rights definition quality.

ERP system now is going towards a system with more coordination/ collaboration, higher heterogeneity and integrity, more intelligent, operating on the level of knowledge, and even wireless-enabled. The security issue within ERP has been there for a long time, but most of the solutions are based on the assumption that an ERP system is a closed environment. Given current trends, where the ERP is more likely to be an open system, these solutions are insufficient to provide the security.

Over the last decades, role-based user management has become the de-facto standard in medium- and large-sized enterprises for managing employees' access to protected resources. In this project I have analyzed role-based user management as a possible solution for minimizing user management load and possible solutions.

ERP security is an ongoing process. The official process starts with the pre-implementation phase where security is designed and built into the ERP system. The official process stops with the implementation of the ERP system. However, this is not where everyone's responsibilities end. As the system is kept up to date and new technologies emerge, security must be addressed as an everyday event to keep the information intact.

Joonised ja tabelid

LISAD

Lisa 1. ERP riski faktorid

Lisaks tavapärastele infosüsteemidest tulenevatele riskidele tuleb arvestada ERP kontekstist sõltuvate riskifaktoritega. Neid riske saab kategoriseerida näiteks juurutus faaside kaudu - otsustusfaasi riskid, juurutamis faasi riskid ja rakendamise faasi riskid. ERP süsteemide riske saab jaotada ka inimestega seotud riskideks, protsessidega seotud riskideks, tehnoloogilisteks riskideks, juurutamisega seotud riskideks ja haldus riskideks.

Inimestega seotud riskid

Juhid, töötajad, arendus tiim ja haldus tiim on ERP projektiga seotult kõige tähtsamad inimesed. Tähtis on, et nemad mõistaksid paremini ERP süsteeme ja nendest tulenevaid kasutegureid, vastasel juhul võib kogu ERP projekt ebaõnnestuda (Leon A. 2008).

a. Muudatuste haldus

Muudatused inimeste töös ja protsessides on vältimatud kui kasutusel on ERP süsteem. Võimalike muudatuste hulka kuuluvad protsesside automatiseerimised ning informatsiooni integreerimine. Selliste muudatuste juhtimine on keeruline ülesanne ning kui seda korralikult ei tehta võib tulemuseks olla läbikukkumine (Leon A. 2008). Muudatuste hulka kuuluvad ka käsitlusala muudatused kus töötajad, kelle vajadused jäävad rahuldamata võivad tunda vastumeelsust projektiga jätkamiseks. Töötajad võivad osutada vastuseisu muudatustele eelkõige seetõttu, et nad ei mõista hästi ERP süsteeme. ERP projekti planeerimise faasis tuleks välja töötada muudatuste halduse mehhanism. (Leon, 2008; Ghosh, 2012).

b. Töötajate piisavus

ERP juurutusse kaasatakse suur hulk inimesi nii organisatsiooni seest kui väljast. Projektis peaks osalema võimalikult palju organisatsiooni enda töötajaid, kes suudaksid teisi koolitada vähendades sellega projekti kulusid. Kui töötajatel puudub piisav kompetents juurutatud ERP süsteemi halduseks ja arenduseks tuleb organisatsioonil palgata väliseid konsultante. See tõstab märgatavalt juurutamise kulusid (Leon A. 2008). Samuti tuleb organisatsioonil hoolikalt planeerida projekti

kaasatud töötajate ressurssi. Tähtaegades püsimiseks on äärmiselt oluline võtmeisikute kättesaadavus. Kvalifitseeritud töötajad on ERP süsteemi juurutamiseks ja halduseks hädavajalikud. Kui vajalike oskustega töötajad lahkuvad organisatsioonist juurutuse ja ülemineku faasis võivad sellega kaasneda viivitused projekti tähtaegades ja lisakulud (Leon, 2008)

c. Projekti meeskond

Kuna ERP projektide arendus on keeruline ülesanne on tähtis, et valitakse õige meeskond, kes suudab projekti eest vastutada. Õige projekti meeskond on suurepärane nii meeskonna juhtimises kui ka kommunikatsioonis ning neil on kõrge pühendumus ja algatuslikud ideed tasakaalustamaks töötajate ja väliste ekspertide koostööd. Üks suurimaid vigasid, mida juht saab teha on määrata projekti juhtima kellegi vastavalt vabale ressursile (Leon, 2008).

d. Koolitused

Koolitamine on iga projekti kõige tähtsam osa. Kui kasutajaid ei koolitata süsteemi kasutama võivad tulemusteks olla segadus ja ebatäpsused, mis takistavad organisatsioonil oodatavat kasumit ERP süsteemist saada. Oluline viga mida tehakse on koolitada välja ainult väike osa kasutajatest lootes jagada teadmist läbi nende ka teiste töötajatega (Leon, 2008). Samuti jäetakse koolitused pahatihti projekti lõppu, mistõttu on võimalik, et projekti eelarve on juba ületatud ning koolituse arvelt hakatakse kokku hoidma.

e. Juhtide toetus

Kuna ERP süsteemid on väga keerukad vajab juurutusmeeskond palju ressurssi. Selleks, et projekti eesmärke täita on vaja juhtide toetust ja osalust ressursi tagamisel (Leon, 2008; Sumner, 2000).

f. Konsultandid ja ärianalüütikud

ERP süsteemide juurutamisse kaasatakse tihti väliseid ERP süsteemide eksperdid. Panorama poolt 2014 aastal läbi viidud uuringust selgus, et vaatamata sellele, et konsultantide kaasamine projekti võib tunduda kui üks kallimatest komponentidest ERP juurutuse juures, tõestavad kasutajakogemused vastupidist (Panorama Consulting Solutions, 2014). On äärmiselt oluline organisatsiooni jaoks, et värvatavad analüütikud oleksid nii äri kui tehniliste oskustega. Ekspert analüütik suudab

analüüsida ja tuvastada organisatsiooni vajadusi ja edastada need vajadused juurutus meeskonnale (Sumner, 2000).

g. Kvalifitseeritud ERP süsteemi arendajate värbamine ja hoidmine

Tulenevalt kõrgetest turuhindadest ei soovi paljud organisatsioonid värvata kvalifitseeritud ERP süsteemi arendajaid. On oluline, et tippjuhtkond pööraks sellele tähelepanu vaatamata algsele kulule, kuna on oluline omada kvalifitseeritud juurutamise meeskonda edukaks ERP süsteemi juurutamiseks (Sumner, 2000).

h. Õige juhtimisstruktuur

Kuna ERP süsteemid on tsentraliseeritud peaks tsentraliseeritud olema ka juhtimine. Ilma korraliku keskse juhtimiseta võib esineda töö dubleerimist. Juht peab olema keegi, kes on võimeline võtma projekti eest vastutust (Sumner, 2000).

i. Kommunikatsioon

Kommunikatsioonil on tähtis roll igas projektis. Kõik projektis osalejad peaksid olema kursis projekti progressi, teemade ja probleemidega. Ebaefektiivne kommunikatsioon võib viia tööülesannete duplitseerimiseni ja mittevajalike probleemideni meeskonnaliikmete vahel, mille tulemuseks võib olla projekti ebaõnnestumine (Sumner, 2000; Seo, 2013).

Protsesside riskid

ERP süsteemide juurutamise üks olulisemaid eesmärke on parandada äriprotsesse muutes nad efektiivsemaks, täpsemaks ja produktiivsemaks. Seega on tähtis äriprotsesside juurutamist jälgida kuna see on üks projekti õnnestumise/ebaõnnestumise faktoritest.

a. Operatiivjuhtimine

ERP süsteem haldab erinevaid infosüsteeme kuhu muuhulgas võivad kuuluda finants, varahaldus, logistika, personalihaldus jne. On väga tähtis, et eriti tootmises tegutsevatel organisatsioonidel oleks ajakohane info operatiivjuhtimiseks kuna see on alus efektiivseteks juhtimisotsusteks. Seega peaks ERP süsteem kaitsma andmete terviklikkust ja tagama informatsiooni siis kui vaja nii nagu vaja (Leon, 2008; Seo, 2013).

b. Äriprotsesside ümberkorraldused

ERP süsteemid eeldavad, et organisatsiooni äriprotsesse parandatakse või tehakse ümber sobitumaks süsteemiga. Sellised muudatused võivad olla väga laiaulatuslikud ja on saavutatavad läbi organisatsiooni struktuuri-, juhtimise-, koolituste- ja töökirjelduste-, mõõdikute muutmise jne. Tõenäosus on suur, et sellised muudatused võivad viia läbikukkumiseni kuna kõik hakkab sõltuma ERP süsteemist. Peale muudatuste jõustamist on väga raske minna tagasi , seega mõjutab see kogu organisatsiooni (Leon, 2008; Sumner, 2000). Panorama Consulting Solutions 2014 aastal teostatud uuringust selgus, et orienteeruvalt 54% projektidest ületasid planeeritud eelarve, nendest pooled kulutasid 0 – 25% eelarvest organisatsiooni muutmisele ja äriprotsessidele. Samuti selgus, et 73% projektidest läksid üle tähtaja, millest 14% olid seotud organisatsiooniliste muutustega (Panorama Consulting Solutions, 2014).

c. Kasu realiseerimine

ERP süsteemi juurutuse läbiviimisel ja sellest tuleneva kasu realiseerumisel on suur vahe. Ainult projekti õnnestumisest ei piisa ERP süsteemist oodatava kasu realiseerumiseks, selleks tuleb süsteem täies mahus ka kasutusele võtta. Töötajate osalemisel, koolitustel ja tippjuhtide toetusel on oluline mõju sellele asjaolule.

Tehnoloogilised riskid

Kuna tehnoloogia areneb iga päevaga siis on organisatsiooni jaoks tähtis nende muudatustega kaasa minna. Kuid tehnoloogia arenguga kaasnevad teatud riskid.

a. Tarkvara funktsionaalsus

ERP süsteemid pakuvad suurel hulgal erinevat funktsionaalsust. Kuna organisatsiooni jaoks ei pruugi kogu pakutav funktsionaalsus vajalik olla siis tasuks konsulteerida ERP ekspertidega milline funktsionaalsus paigaldada ja kasutusele võtta. Sellisel juhul saab vähendada süsteemi keerukust ja kasutajate hirmu uue süsteemi suhtes (Leon, 2008; Ghosh, 2012).

b. Tehnoloogia vananemine

Kuna uut, tõhusat ja kiiret tehnoloogiat lisandub iga päevaga, tuleb arvestada, et paari aastaga võib olemasolev tehnoloogia olla juba vananenud. Seega tuleb ERP süsteemi

valikul arvestada toote ja tehnoloogia jätkusuutlikkuse, toote arhitektuuri, versiooniuuenduste ja tootjapoolse toe võimalikkusega tulevikus (Leon, 2008; Ray, 2011).

c. Uuendused või parandused

Igat ERP süsteemi tuleb hoida ajakohasena paigaldades versiooniuuendusi selleks et süsteemist maksimaalset kasu saada. Seetõttu on hooldus meeskonna vastutada, et süsteemi uuendatakse. Oluline on valida usaldusväärne müüja. Süsteemi kasutuselevõtul peaks allkirjastama ka vastavad lepingud vältimaks riski, et müüja lõpetab süsteemi toetamise (Leon, 2008).

d. Tehnoloogiline pudelikael

Tehnoloogiline pudelikael võib tekkida kui organisatsioonis on kasutusel palju erinevaid keskkondi. Probleemid tekivad kui ERP süsteemi disainer peab ERP mooduleid ühendama olemasolevate pärandsüsteemidega (*legacy system*). Selle tulemusena võivad lisanduda märkimisväärsed ülekulud (Sumner, 2000; Seo, 2013).

Rakendamise riskid

Paljud ERP projektid ebaõnnestuvad. Tähtis omada ülevaadet asjaoludest, mis võivad juurutuse käigus valesti minna (Panorama Consulting Solutions, 2014). Panorama Consulting Solutions 2014 aastal läbi viidud uuringust selgus, et ligilähedal üks viiest vastanutest (16%) väitis oma organisatsiooni ERP juurutuse projekti läbikukkunuks. Põhilisteks läbikukkumise põhjusteks toodi müüja juurutuse teenus (35% rahulolematu või väga rahulolematu) ja teostatud dokumentatsioon (34% rahulolematu või väga rahulolematud). Tõenäosus on, et organisatsioonid, mis ei ole täpselt kaardistanud oma vajadusi tunnevad sagedamini, et ERP müüja on esitanud ebatäpseid lubadusi. (Panorama Consulting Solutions, 2014)

a. Projekti suurus

Tavapäraste IT projektide ja ERP projektide kõige suurem vahe seisneb nende suuruses ja skoobis. Tüüpiline ERP projekt hõlmab väga palju inimesi, katab tervet organisatsiooni, mõjutab kõiki töötajaid ja võib kesta aastaid. Seega tuleb selliseid projekte põhjalikult ette valmistada ja elimineerida kõik ebaselgused.

b. Kõrge alginvesteering

ERP projektid eeldavad suurt investeeringut aga kasutegurid ilmnevad alles peale edukat juurutuse lõpetamist ja süsteemi kasutamist. Projekti ebaõnnestumisel kannab organisatsioon väga suuri kahjusid.

c. Ebarealistlikud tähtajad

Tippjuhtkond võib nõuda ebarealistlikke projekti tähtaegu. Siin tasub olla eriti ettevaatlik kuna selle tõttu võib kannatada süsteemi kvaliteet. Lõppkokkuvõttes võivad venida tähtajad ja kogu projekt ebaõnnestuda.

d. Ebapiisav rahastamine

ERP projektid nõuavad suuri finantseeringuid. Projekti eelarve koostamisel tasub konsulteerida ekspertidega ja teha palju eeltööd vältimaks varjatud kulusid, mis on ERP juurutuste puhul vältimatud. Vastasel korral võivad tekkida projekti katkestused, mis on tingitud ebapiisavast finantseeringust.

f. Liidesed

Kuigi ERP süsteemist saab peale rakendamist organisatsiooni keskpunkt, peab ta siiski suhtlema väliste partneritega, käitlema keerulisti andmeallikaid ja ühilduma *legacy* tüüpi süsteemidega. Tähtis on, et ERP süsteemi saaks integreerida, et neid tegevusi teostada.

g. Skoobi kasv

Projekti skoobi pidev suurendamine ja vähendamine võib põhjustada juurutusmeeskonna seas segadust, pikendades projekti tähtaegu ja eelarvet. Seega on tähtis selgelt määratleda projekti skoop ja projekti etapid.

h. Lahknevusanalüüs (*Gap analysis*)

ERP süsteemi oodatavad tulemused võivad erineda sellest mida valmis lahendus tegelikult pakub. Seega on oluline, et tippjuhid oleksid kursis pakutavate toodete võimaluste ja puudustega. See mõjutab otseselt projekti ajakavas püsimist ja kulu.

i. Prototüüpide puudumine

Prototüüpimine annab arendajatele parema arusaamise oodatavast süsteemist. Kuna ERP süsteemid on mahukad ja keerukad siis pahatihti jäetakse prototüüp tegemata.

j. Haldus riskid

ERP süsteem ei ole kunagi valmis peale juurutus faasi. Kasu süsteemist tuleb alles siis kui ta on kasutusel. Seega uuenduste ja täienduste installeerimine, uue tehnoloogia kasutuselevõtt, uute kasutajate koolitus jne on tegevused mida tuleb teha terve süsteemi eluea jooksul. Tippjuhid ja süsteemi kasutajad peavad pühenduma süsteemi hooldusele ja töös hoidmisele.

ERP riskide maandamine

ERP süsteemi kasutatakse peamiselt ettevõtluse kontekstis kuid on kasutusel ka teistes valdkondades nagu tervishoid ja avalik sektor. Nendes valdkondades töödeldakse kõrge turvatasemega andmeid ning sellest tulenevalt on andmete turvalisus ääretult tähtis

Võrgukihi turvariskid

Võrgukihi turvariskid tekivad, kui kasutaja suhtleb süsteemiga või erinevad infosüsteemid ERP süsteemis suhtlevad omavahel. Selliste riskide haldamine ja kontrollimine kuuluvad võrgu administraatori kohustuste alla ja ERP administraatorid ei ole tavaliselt sellega seotud.

Presentatsiooni kihi turvariskid

Presentatsiooni kiht sisaldab endas arvuteid, kuvareid ja graafilisi kasutajaliideseid. Raske on tagada süsteemi turvalisust limiteerides kasutaja ligipääsu graafilisele kasutajaliidesele (GUI *Graphical user interface*) kuna GUI pakettide edastamist ei ole võimalik piirata.

Rakenduskihi turvariskid

Rakenduskihi turvalisus keskendub andmete ja protsesside turvamisele. Turbe funktsioone, mis on andmebaasi poole peal olemas võib aktiveerida või desaktiveerida vastavalt üleüldisele turvalisuse lahendusele, mis on süsteemis kasutusel.

Üldisemad riskid

a. Turvapoliitikad

Kuna turvapoliitikad sisaldavad endas reegleid ja piiranguid pääsuõiguste andmiseks ja tühistamiseks, peaks iga organisatsioon kus on kasutusel ERP süsteem oma turvapoliitika välja töötama.

b. Kasutajate autentimine

Kuna ERP süsteemi kasutavad organisatsioonis paljud inimesed, siis peab kasutusele võtma tõhusa kasutajate autentimise mehhanismi, mis võimaldab tuvastada kasutaja identiteeti. Kui autentimisele ei pöörata piisavalt tähelepanu võivad süsteemi siseneda võõrad.

c. Töökohustuste eristamine

Õigused teostada teatud toiminguid tuleks määrata ainult teatud rollidele või töötajatele. Kui kõikidel töötajatel on võrdsed õigused näha ja muuta tundlikku informatsiooni võib juhtuda, et seda kasutatakse isiklikul eesmärgil.

d. Autoriseerimine

Süsteem peab kontrollima, kas kasutaja poolt teostatav toiming on kasutajale lubatav. Kui süsteem sellist kontrolli ei tee võib töötaja süsteemi ära kasutada.

e. Ajapiirangud

Vahest võib tekkida olukordi kus kasutajale on vaja anda ajutiselt õigused andmetele, milledele tal igapäevaselt ligipääs puudub. Administraatori kohus on need õigused anda ja ka tühistada kohe kui vajalik toiming on teostatud.

f. Logimine

Logimine ja jälgimine on vajalikud sündmuste kontrolliks. Logi faile tuleb kaitsta manipulatsiooni ja kuritarvitamise eest.

g. Administraator

Õiguste andmine ja tühistamine ning rollide ja funktsioonide defineerimine on tundlikud tegevused millega tuleks olla väga ettevaatlik. Kuna nende tegevuste eest

vastutab administraator, peab organisatsioon pöörama tähelepanu sellele, kes määratakse sellesse rolli.

h. Andmebaasi turvalisus

ERP süsteemid integreerivad terve organisatsiooni ühte tsentraliseeritud andmebaasi. Hädavajalik on pöörata andmebaasi turvalisusele tähelepanu, kaitsmata andmebaas võib olla paljude väliste rünnakute sihtmärk.

i. Olemasolevad süsteemid

Pahatihti ei saa välistada *legacy* süsteemide suhtlemist ERP süsteemiga. Sellist suhtlust tuleb pidevalt jälgida kuna olemasolevad süsteemid võivad lisada uusi vigu ja turvaaspekte.

j. Standardid ja mõõdikud

Turvameeskonnal peaksid olema selgelt määratletud standardid, et turvameetmetega piiri pidada. Liiga turvaline süsteem tekitab uusi probleeme.

k. Turvaaugud ja intsidendid

Igal tarkvaral on omad nõrkused. Seega on turvaaukudele ja intsidentidele reageerimine sama tähtis kui turvalise süsteemi loomine.

l. Teadmised turvaaukude, rünnete ja ründajate kohta jne.

Iga organisatsioon peaks planeerima teatud ressursse informatsiooni kogumiseks erinevate turva aspektide kohta nagu näiteks eelnevad rünnakud ründajad jne. Neid aspekte saab jaotada 6 gruppi:
põhimõtted, juhised, nõrkused, ründed, rünnaku mustrid ja eelnevad riskid. Süsteemide arendamine ilma mineviku kogemust arvesse võtmata soosib samade vigade tekkimist ka tulevikus.

m. Pidev täiustamine

Turvalisus on valdkond, mis areneb iga päevaga. Süsteemi arendajad peavad tõhustama ja leiutama uusi turvaprotseduure. Vanemad turvameetmed muutuvad rohkem haavatavaks.

Lisa 2. Pääsuõiguste taotlemise vormi näidis.

Kasutaja andmed

Eesnimi	
Perekonnanimi	
AD kasutajanimi	
Email	
Üksus	
Kinnitaja	

Mudel

	Lugemisõigus	**Kirjutamisõigus**	**Üksus/ettevõte või valdkond**	**Projektikood**	**Konto**
Mudel 1					
Mudel 2					
Mudel 3					
Mudel 4					
Mudel 5					
Mudel 6					
Mudel 7					
Mudel 8					