TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond

Liis Hulkko

PERSONALIARHITEKTUURI TERVIKLIKKUSE SEOS RISKIJUHTIMISE PRAKTIKATEGA EESTI INFOTEHNOLOOGIAFOOKUSEGA SUURORGANISATSIOONIDES

Magistritöö
Õppekava HAPM, peaeriala personalijuhtimine

Juhendaja: Maarit Vabrit-Raadla, MA

Tallinn 2026

Deklareerin, et olen koostanud lõputöö iseseisvalt ja
olen viidanud kõikidele selle koostamisel kasutatud
teiste autorite töödele, olulistele seisukohtadele ja andmetele,
ning ei ole esitanud sama tööd varasemalt ainepunktide saamiseks.

Töö pikkuseks on 13 202 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Liis Hulkko 02.05.2026
(kuupäev)

SISUKORD

TABELITE LOETELU

JOONISTE LOETELU

LÜHIKOKKUVÕTE

Käesolev magistritöö käsitleb personaliarhitektuuri terviklikkuse seoseid riskijuhtimise praktikatega Eesti infotehnoloogiafookusega suurorganisatsioonides. Teema on ajakohane, kuna organisatsioonide digisõltuvus, andmetöötluse maht ja küberriskid on kasvanud, samal ajal kui personalifunktsiooni käsitletakse sageli endiselt eraldi organisatsiooniarhitektuurist ja riskijuhtimisest.

Töö eesmärk oli selgitada, kuidas personaliarhitektuuri terviklikkus on seotud riskijuhtimise praktikatega ning kuidas inimeste, rollide, protsesside, andmete ja tehnoloogiate sidus käsitlemine toetab riskide ennetamist ja juhtimist. Personaliarhitektuuri terviklikkust käsitletakse organisatsioonilise tasandi omadusena, mis väljendab rollide, vastutuste, protsesside, süsteemide ja kontrollimehhanismide seotust. Teadlikkust käsitletakse individuaalse tasandi nähtusena, mis mõjutab seda, kuidas neid seoseid organisatsioonis tajutakse ja kirjeldatakse.

Empiiriline uurimus viidi läbi kvalitatiivse mitme juhtumiga juhtumiuuringuna. Andmeid koguti poolstruktureeritud intervjuude kaudu kuue Eesti infotehnoloogiafookusega suurorganisatsiooni personali-, IT- ning riski- või õigusfunktsiooni esindajatelt. Andmeid analüüsiti temaatilise sisuanalüüsi ja juhtumite võrdleva analüüsi abil. Tulemused näitasid, et personaliarhitektuuri terviklikkus ja riskijuhtimise praktikate süsteemsus on omavahel seotud, kuid selle seose tugevus erineb organisatsiooniti. Juhtumites, kus protsessid, rollid, tehnoloogia ja kontrollimehhanismid olid omavahel paremini kooskõlas, oli riskijuhtimine süsteemsem ja ennetavam. Madalama terviklikkuse korral oli riskijuhtimine hajusam ja reageerivam ning sõltus rohkem üksikisikute kogemusest.
Eri funktsioonide vaadete ebaühtlus mõjutas riskikohtade nähtavust ja juhtimist. Töö praktiline väärtus seisneb selles, et see aitab mõista, kuidas personaliarhitektuuri sidusam kujundamine toetab riskijuhtimist, funktsioonidevahelist koostööd ja organisatsiooni vastupidavust.

Võtmesõnad: personaliarhitektuur, personaliarhitektuuri terviklikkus, riskijuhtimine, organisatsiooniarhitektuur, Eesti suurorganisatsioonid

SISSEJUHATUS

Viimastel aastatel on Eesti suurorganisatsioonide igapäevast juhtimist üha enam mõjutanud digitaliseerimine, kasvavad andmemahud ja küberohud. Küberriskid ei puuduta enam üksnes IT-valdkonda, vaid organisatsiooni toimimist tervikuna. Juhid teadvustavad intsidentide võimalikku mõju, kuid paljudes organisatsioonides puudub endiselt keskne infoturberoll ja sidus ülevaade riskidest ning töötajate teadlikkus jääb oluliseks haavatavuse allikaks (KPMG Baltics OÜ, 2022, lk 2, 7–9; Riigi Infosüsteemi Amet, 2024, lk 58).

Selle lõhe taga on sageli struktuuriline probleem: rollid, vastutused, protsessid ja tehnoloogilised lahendused ei ole organisatsioonis piisavalt sidusalt seotud. Killustunud seosed toovad kaasa olukorra, kus riskid jäävad märkamata, vastutus hajub ning kontrollimeetmed ei toimi järjepidevalt. Põhjus ei seisne enamasti tahte puudumises, vaid ühise arhitektuurilise loogika kujunematuses.

Varasem teaduskirjandus on käsitlenud organisatsiooniarhitektuuri, andmekaitset ja riskijuhtimist, kuid personalivaldkonna roll nende seoste kujundamisel on jäänud tagasihoidlikumalt uurituks. GDPR-i rakendamise käsitlused näitavad, et andmekaitsenõuete täitmine ei piirdu õigusliku vastavusega, vaid eeldab tehniliste, organisatsiooniliste ja regulatiivsete nõuete sidumist protsesside, poliitikate, süsteemide ja vastutustega (McMenemy et al., 2017; Hjerppe et al., 2019, lk 1–2; Smirnova & Travieso-Morales, 2024, lk 326–327, 334–338). Küberoskuste nappuse ja kasvava riskisurve tingimustes muutub see seos veelgi kriitilisemaks (Lorenz, 2024, lk 9–10; Vrhovec & Markelj, 2024, lk 10–11, 14).

Uurimisprobleem seisneb selles, et Eesti infotehnoloogiafookusega suurorganisatsioonides ei ole piisavalt selge, kui terviklikult on personaliarhitektuur kujunenud ning kuidas see seostub riskijuhtimise praktikatega. Töö keskmes on personaliarhitektuuri terviklikkus ehk rollide, vastutuste, protsesside, süsteemide ja kontrollimehhanismide sidusus, ning see, kuidas individuaalse tasandi teadlikkus mõjutab nende seoste tajumist ja kirjeldamist organisatsioonis.

Magistritöö eesmärk on selgitada personaliarhitektuuri terviklikkuse seoseid riskijuhtimise praktikatega Eesti infotehnoloogiafookusega suurorganisatsioonides ning mõista, kuidas inimeste, rollide, protsesside, andmete ja tehnoloogiate sidus käsitlemine toetab riskide ennetamist ja juhtimist.

Sellest lähtuvad järgmised uurimisküsimused:

1. Kuidas avaldub personaliarhitektuuri terviklikkus uuritud organisatsioonides ning kuidas kirjeldavad juhid ja võtmeisikud selle rolli organisatsiooni toimimises?
2. Millised tegurid toetavad või takistavad personaliarhitektuuri terviklikkust erinevates organisatsioonilistes rollides ja funktsioonides?
3. Millisel viisil avaldub personaliarhitektuuri terviklikkus riskijuhtimise protsessides, otsustes ja praktikates?
4. Millised juhtumitevahelised mustrid viitavad personaliarhitektuuri terviklikkuse ja riskijuhtimise süsteemsuse seosele?

Uurimisobjektiks on personaliarhitektuuri terviklikkus ja selle seosed riskijuhtimise praktikatega Eesti infotehnoloogiafookusega suurorganisatsioonides. Uuring viidi läbi kvalitatiivse mitme juhtumiga juhtumiuuringuna. Andmeid koguti poolstruktureeritud intervjuude abil kuuest organisatsioonist, kokku 15 osalejalt personali-, IT- ning riski- või õigusfunktsioonist. Organisatsioonides, kus eraldi riskifunktsioon puudus, käsitleti seda vaadet vastava vastutusala kaudu personali- või IT-funktsioonis. Andmete analüüsimisel kasutati temaatilist sisuanalüüsi ja juhtumite võrdlevat analüüsi.

Töö koosneb kolmest peatükist. Esimeses peatükis esitatakse teoreetiline raamistik, mis käsitleb personaliarhitektuuri, organisatsiooniarhitektuuri ja riskijuhtimise seoseid. Teises peatükis kirjeldatakse uurimuse metoodikat ning esitatakse empiirilise analüüsi tulemused. Kolmandas peatükis seotakse tulemused teoreetiliste lähtekohtadega ning esitatakse järeldused ja praktilised soovitused.

1. TEOREETILINE RAAMISTIK

Personaliarhitektuur on uurimuse keskne mõiste, mis võimaldab analüüsida, kuidas rollid, kompetentsid ja personaliprotsessid toetavad strateegia elluviimist ning kujundavad personaliga seotud riske (Lepak & Snell, 1999, lk 31–32; Becker & Huselid, 2006, lk 899–901). Infotehnoloogiast sõltuvates suurorganisatsioonides on selle roll eriti oluline, kuna personaliprotsessid toimuvad suures osas digitaalsetes süsteemides ning personaliga seotud otsused mõjutavad töövoogude, õiguste ja vastutuste toimimist. Organisatsiooniarhitektuuri vaates sõltub toimivus äriprotsesside ja IT-taristu kooskõlast (Ross et al., 2006, lk 8–9), samal ajal kui küberturbeotsustajate teadlikkus mõjutab riskide mõistmist ja juhtimist (Vrhovec & Markelj, 2024, lk 1, 14).

Seetõttu on oluline mõista personaliarhitektuuri teoreetilisi käsitlusi ja selle ülesehituse põhimõtteid, mis loovad aluse analüüsiks, kuidas personaliarhitektuuri terviklikkus seostub riskijuhtimise praktikatega ning kuidas individuaalse tasandi teadlikkus seda seost nähtavaks teeb (Lepak & Snell, 1999, lk 32–34; Becker & Huselid, 2006, lk 899–901).

1.1. Kasutatud põhimõisted

Käesolevas töös kasutatakse mitut omavahel seotud mõistet, mis pärinevad strateegilise personalijuhtimise, organisatsiooniarhitektuuri ja riskijuhtimise kirjandusest. Kuna nende tähendus varieerub autoriti, täpsustatakse nende kasutus käesoleva uurimuse kontekstis ning seotakse need töö analüütilise raamistikuga.

Organisatsiooniarhitektuur tähistab organisatsiooni toimimise tervikloogikat, mis seob äriprotsessid, andmed, infosüsteemid ja tehnoloogilise taristu viisil, mis toetab organisatsiooni toimimis- ja juhtimismudelit. Ross et al. (2006) käsitlevad organisatsiooniarhitektuuri kui äriprotsesside ja IT-taristu organiseerivat loogikat, mis peegeldab organisatsiooni operatsioonimudeli integratsiooni- ja standardiseerimisvajadusi (lk 8–9, 47–51). Käesolevas töös käsitatakse personaliarhitektuuri selle loogika ühe osana, kuna rollid, vastutused, kompetentsid,

personaliprotsessid ja kasutatavad süsteemid mõjutavad otseselt organisatsiooni töövoogude toimimist ning riskide nähtavust.

Personaliarhitektuur tähendab organisatsiooni strateegilist ja süsteemset lähenemist sellele, kuidas töötajagruppe, rolle, kompetentse ja personalipraktikaid kujundatakse ning seotakse organisatsiooni eesmärkide ja toimimisloogikaga. Mõiste tugineb Lepaki ja Snelli käsitlusele inimkapitali diferentseerimisest ning Beckeri ja Huselidi vaatele personalisüsteemide strateegilisest kooskõlast (Lepak & Snell, 1999, lk 31–34; Becker & Huselid, 2006, lk 899, 903–905).

Personalisüsteemid viitavad personalijuhtimise põhimõtete ja praktikate tervikule, mille kaudu juhitakse töötajate värbamist, arendamist ja hoidmist. Neid käsitatakse tervikliku süsteemina, mitte üksikute praktikate kogumina (Arthur & Boyles, 2007, lk 78–80). **Personaliprotsessid** on nende süsteemide operatiivne väljendus konkreetsete töövoogude ja tegevuste jadadena.

Riskijuhtimise praktikad hõlmavad organisatsioonis kasutatavaid põhimõtteid ja tegevusi riskide tuvastamiseks, hindamiseks, käsitlemiseks, seireks ja ülevaatuseks (International Organization for Standardization, 2018, lk 8–14). Käesolevas töös käsitatakse riskijuhtimist lisaks formaalsetele protseduuridele ka organisatsioonilise teadlikkuse ja otsustusvõimekusena, mis mõjutab seda, kuidas riske igapäevases tegevuses mõistetakse ja juhitakse (Aven, 2016, lk 1–3).

Personaliarhitektuuri teadlikkus viitab käesolevas töös individuaalse tasandi mõistele, mis väljendab, mil määral juhid ja võtmeisikud mõistavad personaliga seotud rollide, protsesside, süsteemide ja andmekasutuse omavahelisi seoseid ning nende mõju organisatsiooni toimimisele ja riskidele. Mõiste tugineb arusaamale, et oluline on suutlikkus näha seoseid rollide, protsesside, tehnoloogiate ja juhtimisloogika vahel (Becker & Huselid, 2006, lk 903–905; Ross et al., 2006, lk 8–9). Riskijuhtimise vaates seostub see teadmiste kvaliteedi ja võimega märgata ebakindlust ning võimalikke haavatavusi (Aven, 2016, lk 2–3, 5–6).

Personaliarhitektuuri terviklikkus on käesolevas töös organisatsiooniline omadus, mis kirjeldab, kui sidusalt on personaliga seotud rollid, protsessid, süsteemid, andmekasutus ja kontrollimehhanismid omavahel seotud ning juhtimisse integreeritud. Selle mõiste taustaks on organisatsiooniarhitektuuri käsitlus, mille järgi organisatsiooni toimivus sõltub protsesside, rollide, infosüsteemide ja andmete kooskõlastatud ülesehitusest (Ross et al., 2006, lk 8–9, 27–28).

Sama loogikat toetab personalisüsteemide kirjandus, mille järgi kujuneb personaliga seotud mõju praktikate koosmõjust, mitte üksikute praktikate eraldi rakendamisest (Arthur & Boyles, 2007, lk 78–80; Boon et al., 2019, lk 2498–2502).

Infotehnoloogiafookusega suurorganisatsioon tähendab käesolevas töös organisatsiooni, mille toimimine sõltub olulisel määral infosüsteemidest ja andmetöötlusest ning kus personaliprotsessid on tihedalt seotud tehnoloogiliste lahendustega.

Seega käsitatakse käesolevas töös organisatsiooniarhitektuuri laiemana raamistikuna, personaliarhitektuuri selle alamsüsteemina ning personaliarhitektuuri teadlikkust ja terviklikkust teguritena, mis mõjutavad riskijuhtimise praktikate kujunemist.

1.2. Personaliarhitektuuri olemus

Personaliarhitektuuri mõiste lähtub arusaamast, et kõik töötajad ega nende teadmised ei ole organisatsiooni jaoks võrdse strateegilise tähtsusega. Lepak ja Snell (1999, lk 35–36) rõhutavad, et inimkapitali väärtus sõltub selle panusest organisatsiooni konkurentsieelisesse ning selle unikaalsusest ehk sellest, kui raskesti on vastavaid teadmisi ja oskusi võimalik asendada või turult omandada. Seetõttu ei saa tööjõudu käsitleda ühtse ressursina, vaid organisatsioon peab tegema teadlikke valikuid selle kohta, keda arendada organisatsiooni sees, milliseid teadmisi tuua sisse turult ning millistes valdkondades kasutada lepingulisi või koostööl põhinevaid suhteid (Lepak & Snell, 1999, lk 33–42).

Personaliarhitektuur kirjeldab seda, kuidas personalipraktikad, protsessid ja juhtimisviisid moodustavad organisatsiooni eesmärke toetava terviku. Arthur ja Boyles (2007, lk 78–80) käsitlevad personalisüsteemi mitmetasandilise süsteemina, mis hõlmab põhimõtteid, poliitikaid, programme, praktikaid ja personalikliimat. Boon et al. (2019, lk 2498–2500, 2500–2504, 2517–2518) rõhutavad samuti personalipraktikate süsteemset koosmõju ning vajadust selgelt määratleda, millised praktikad süsteemi kuuluvad ja kuidas neid tervikuna mõõdetakse. Käesolevas töös käsitatakse personaliarhitektuuri piiritletud süsteemse loogikana, mis seob personalipraktikad organisatsiooni eesmärkide, strateegiliste võimekuste ja põhitegevusega (Becker & Huselid, 2006, lk 899, 903–905).

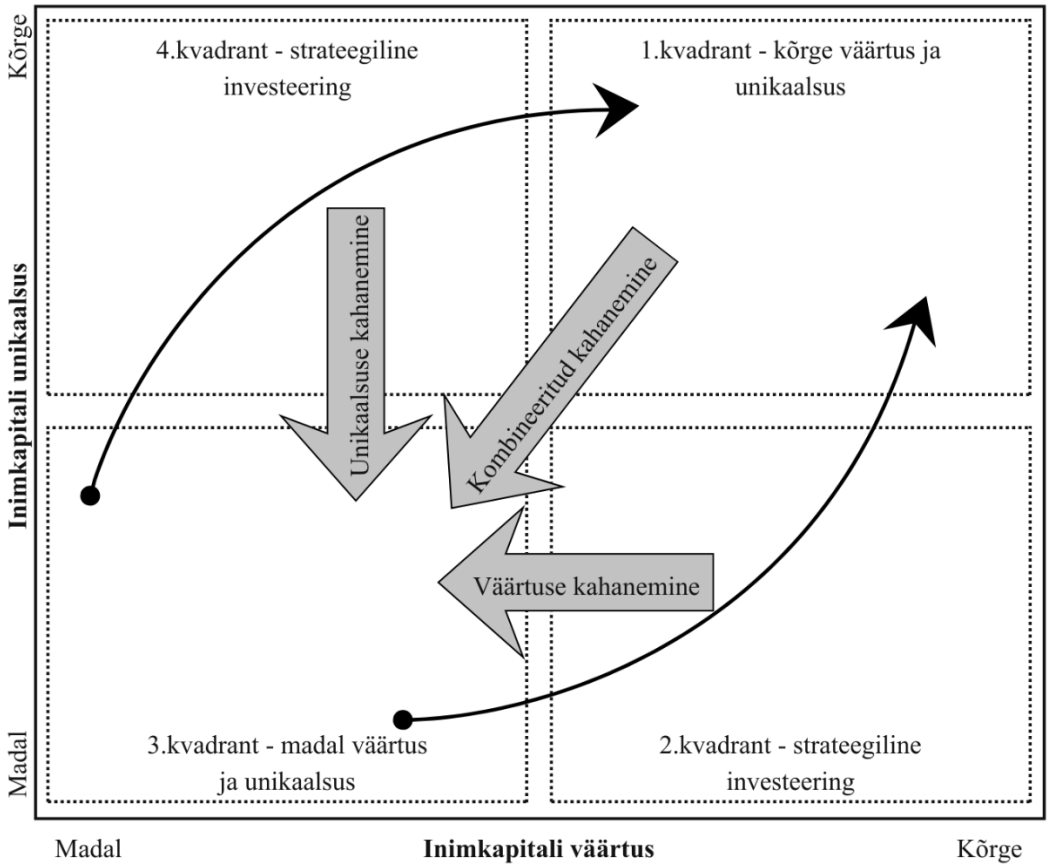
Personaliarhitektuur ei ole staatiline. Hansen, Güttel ja Swart (2019, lk 648–649, 651–653, 663–665) rõhutavad, et organisatsioonid vajavad eri keskkondades erinevaid personaliarhitektuurilisi lahendusi sõltuvalt sellest, kuidas tasakaalustatakse olemasolevate võimekuste kasutamist ja uute võimaluste arendamist. See aitab mõista, miks personaliarhitektuuri kujunemine võib organisatsiooniti erineda.

Digitaalses ja infotehnoloogiast sõltuvas organisatsioonis on personaliarhitektuur oluline, sest andmekaitsenõuded peavad kajastuma rollides, vastutustes, tööprotsessides ja tehnilistes lahendustes. Hjerppe et al. (2019, lk 1–2) rõhutavad, et andmekaitsenõuded tuleb tõlkida toimivateks tehnilisteks ja organisatsioonilisteks lahendusteks. Smirnova ja Travieso-Morales (2024, lk 334–338) seostavad GDPR-i rakendamise sisemiste protsesside kohandamise, uute protseduuride loomise, juhtimismudelite muutmise ja teenusepakkujate vastavuse tagamisega. Sama loogikat toetab personali ja GDPR-i käsitlus, mille järgi personalifunktsioonil on keskne roll töötajaandmete õiguspärase, läbipaistva ja turvalise töötlemise tagamisel ning personali, IT- ja vastavusfunktsiooni koostöö kujundamisel (Ussher-Eke, 2025, lk 717–720).

Eeltoodu põhjal võib personaliarhitektuuri määratleda kui organisatsiooni strateegilist ja süsteemset lähenemist sellele, kuidas erinevaid töötajagruppe, rolle, teadmisi ja personalipraktikaid kujundatakse ning seotakse organisatsiooni eesmärkide, protsesside ja juhtimisloogikaga. Käesolevas töös on see oluline analüütiline mõiste, mille abil mõtestada, kuidas personaliga seotud valikud mõjutavad organisatsiooni juhtimisvõimekust ja riskijuhtimise praktikaid.

1.2.1. Inimkapitali tüübid ja nende strateegiline väärtus

Inimkapital koosneb erineva strateegilise väärtuse ja unikaalsusega rollidest. Lepaki ja Snelli (1999, lk 36–37) mudel koondab selle loogika nelja inimkapitali tüübi raamistikku (vt joonis 1).



Joonis 1. Inimkapitali arhitektuuri mudel
Allikas: autori koostatud Lepak ja Snell (1999, lk 37) põhjal

Selle käsitluse kohaselt loovad kõrge unikaalsuse ja strateegilise väärtusega töötajad, näiteks tehnoloogiliste tuumkompetentside kandjad või võtmespetsialistid, organisatsioonile kestva konkurentsieelise. Selliste rollide arendamine ja hoidmine on kriitiline, sest nende asendamine on keerukas ja ajamahukas (Lepak & Snell, 1999, lk 36–38; Becker & Huselid, 2006, lk 903–905).

Inimkapitali diferentseerimine on personaliarhitektuuri keskne põhimõte, sest erineva väärtuse, unikaalsuse ja kriitilisusega rollid vajavad erinevaid juhtimis-, arendus- ja kontrolliloogikaid. Kui organisatsioon käsitleb strateegilisi ja toetavaid rolle liiga ühetaoliselt, võivad personalipraktikad muutuda ebatäpseks: sama ligipääsu-, arendus- või hindamismudel võib rakenduda töötajatele, kelle vastutuse ulatus, kompetentsinõuded ja riskitase on tegelikult erinevad. Lepak ja Snell (1999) seovad personaliarhitektuuri inimkapitali väärtuse ja unikaalsusega ning näitavad, et erinevad töötajagrupid eeldavad erinevaid juhtimis- ja arendusloogikaid (lk 35–38). Riskijuhtimise seisukohalt võib rollide ebapiisav eristamine suurendada välditavate riskide tõenäosust, kui

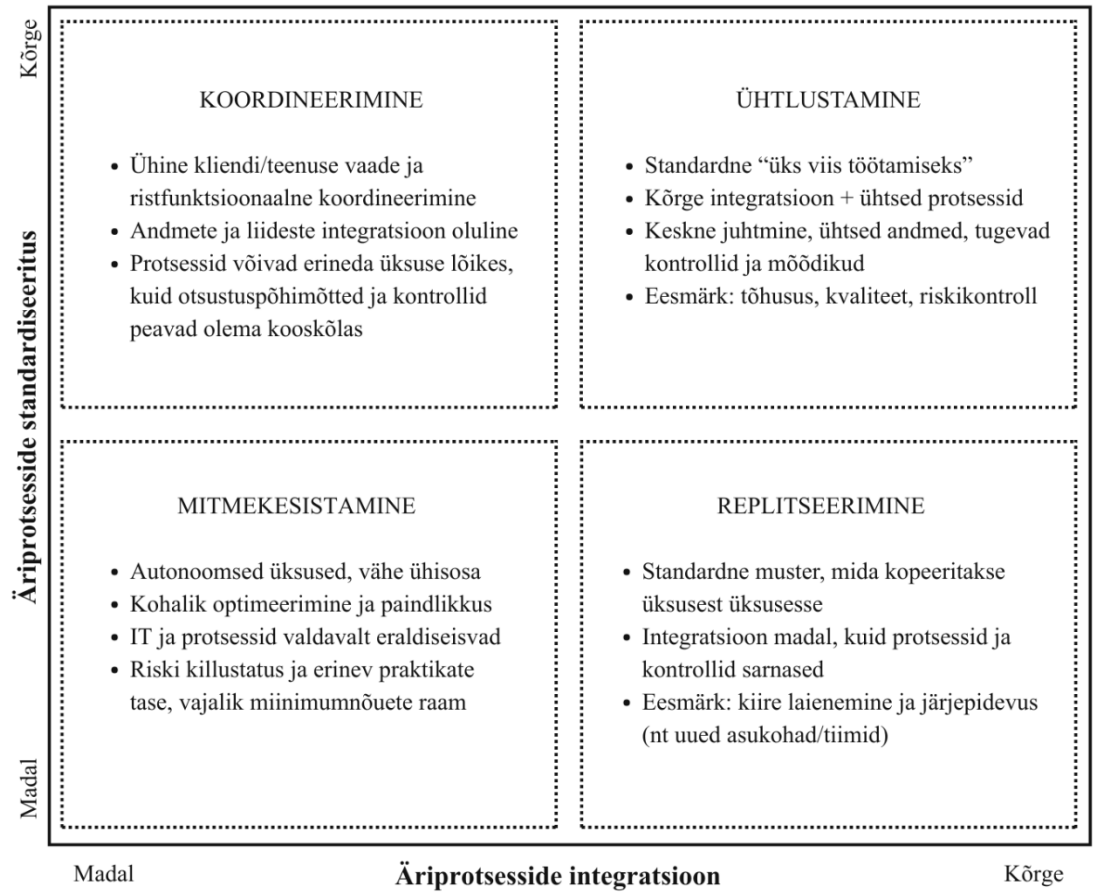
ligipääsud, vastutused ja kontrollimehhanismid ei vasta rollide kriitilisusele (Kaplan & Mikes, 2012, lk 4–5, 9).

Infotehnoloogiafookusega suurorganisatsioonides on inimkapitali eristamine eriti oluline, sest tehniliste kompetentside strateegiline väärtus võib olla otseselt seotud organisatsiooni põhitegevuse ja strateegiliste võimekustega. Becker ja Huselid (2006) rõhutavad, et personaliarhitektuur peaks olema diferentseeritud vastavalt strateegilistele äriprotsessidele ja rollidele, mitte rakenduma kõigile töötajagruppidele ühetaoliselt (lk 903–906). Seda toetab ka personalisüsteemide kirjandus, mille järgi ei saa personalijuhtimise mõju mõista üksikute praktikate kaupa, vaid omavahel seotud süsteemina, mille toimivus sõltub praktikate koostoimest, süsteemi eesmärgist ja selgelt piiritletud praktikate kogumist (Boon et al., 2019, lk 2498–2502, 2517–2519). Sellest vaatenurgast tähistab personaliarhitektuur lisaks töötajagruppide eristamisele ka seda, kuidas erinevate rollide juhtimine seotakse organisatsiooni eesmärkide, protsesside ja kontrollikeskkonnaga ühtseks tervikuks.

1.2.2. Personaliarhitektuuri seos organisatsiooniarhitektuuriga

Organisatsiooniarhitektuur (*enterprise architecture*, EA) käsitleb organisatsiooni tervikliku süsteemina, milles strateegia, protsessid, organisatsioonistruktuur, rakendused, informatsioon ja tehnoloogiline taristu on omavahel seotud (Lankhorst et al., 2009, lk vi). Selle eesmärk on luua organiseeriv loogika, mille kaudu äriprotsessid ja tehnoloogiline taristu toetavad strateegiliste eesmärkide elluviimist ning organisatsiooni järjepidevat toimimist (Ross et al., 2006, lk 2–4, 8–9, 47).

Käesolevas töös on see oluline, sest personaliarhitektuuri ei käsitleta personalivaldkonna eraldiseisva sisekorraldusena, vaid organisatsiooniarhitektuuri ühe osana. Rollid, vastutused, kompetentsid, personaliprotsessid ja kasutatavad süsteemid peavad olema kooskõlas organisatsiooni laiemate protsesside ja juhtimispõhimõtetega. Seda seost aitab avada Ross et al. (2006, lk 26–28) operatsioonimudeli maatriks, mis on esitatud joonisel 2.



Joonis 2. Operatsioonimudeli maatriks (äriprotsesside integratsioon ja standardiseeritus) kui arhitektuurilise järjepidevuse lähtekoht
Allikas: autori koostatud Ross et al. (2006, lk 26–29) põhjal.

Operatsioonimudel kirjeldab, millisel määral vajab organisatsioon protsesside integratsiooni ja standardiseerimist, ning loob seeläbi aluse arhitektuurilisteks valikuteks (Ross et al., 2006, lk 26–28). Käesolevas töös aitab see avada, et personaliarhitektuur peab olema kooskõlas organisatsiooni laiemate integratsiooni- ja standardiseerimisvalikutega. Vastasel juhul võivad kujuneda killustunud töövood, ebaühtlased praktikad ja nõrgem kontrollikeskkond (Ross et al., 2006, lk 5–9, 47–51; Lepak & Snell, 1999, lk 33–37, 43–45).

1.2.3. Seosed infotehnoloogia ja infoturbe arhitektuuriga

Infotehnoloogiafookusega suurorganisatsioonides avaldub personaliarhitektuur selles, kuidas töötajate rollid, vastutused ja ligipääsud on seotud infosüsteemide, andmevoogude ja kontrollimehhanismidega. Personaliprotsessid toimivad üha enam digitaalses keskkonnas ning

töötajatega seotud otsused realiseeruvad praktikas süsteemsete õiguste, töövoogude ja kontrollide kaudu (Ross et al., 2006, lk 8–9; Lankhorst et al., 2009, lk vi).

Selles kokkupuutepunktis muutub personaliarhitektuur otseselt infoturbe ja riskijuhtimise küsimuseks. Personaliprotsessid hõlmavad töötajate ja kandidaatide isikuandmeid, rollipõhiseid ligipääse ning õiguste andmist, muutmist ja lõpetamist. Ebaselged seosed rollide, protsesside, süsteemide ja ligipääsude vahel võivad kaasa tuua vastutuse hajumise ja kontrollilüngad, mis suurendavad andmekaitse- ja infoturberiske. Eesti ettevõtete uuringud viitavad, et riskijuhtimist nõrgestavad keskse infoturberolli puudumine, teenuspartnerile vastutuse ekslik eeldamine ning vähene sõltumatu kontroll (McMenemy et al., 2017; KPMG Baltics OÜ, 2022, lk 2, 7–9).

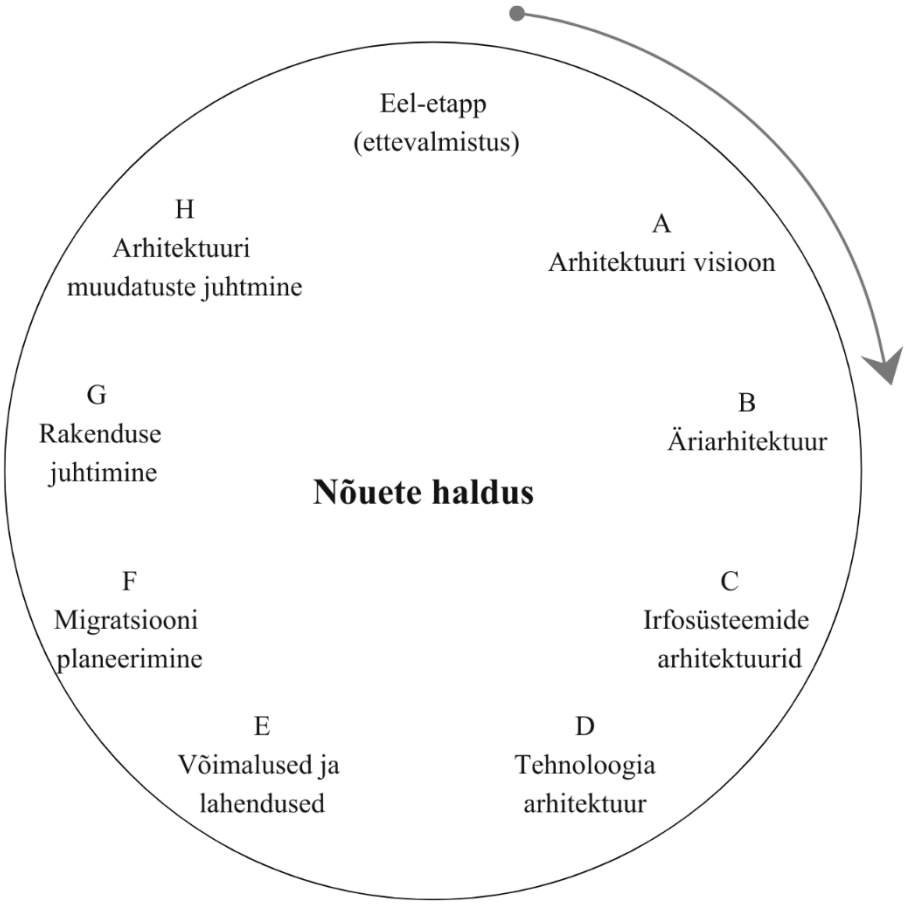
Personali-, IT- ja infoturbe arhitektuuri kooskõla on seetõttu oluline personaliarhitektuuri terviklikkuse eeldus. Riskide juhtimine eeldab, et rollide, protsesside, süsteemide ja ligipääsude tegelik toimimine on nähtav, juhitud ja kontrollidega kaetud. Eesti küberturvalisuse ülevaated kinnitavad, et riskid tulenevad sageli ka juhtimis- ja vastutusloogika ebaühtlusest (Riigi Infosüsteemi Amet, 2024, lk 19; KPMG Baltics OÜ, 2022, lk 7, 9). Käesoleva töö vaates tähendab see, et personaliarhitektuuri terviklikkus sõltub sellest, kui sidusalt on personaliprotsessid seotud IT-arhitektuuri, infoturbe kontrollide ja riskijuhtimise praktikatega.

1.2.4. Organisatsiooniarhitektuuri raamistikud ja nende kasutamine personalifunktsiooni kontekstis

Organisatsiooniarhitektuuri raamistikud aitavad kirjeldada ja juhtida seoseid, mis tekivad rollide, protsesside, andmete, süsteemide ja kontrollimehhanismide vahel. Personalifunktsiooni kontekstis seisneb nende väärtus selles, et need muudavad nähtavaks sõltuvused, mis tavapärases protsessikirjelduses võivad jääda varjatuks.

Näiteks kirjeldab TOGAF arhitektuuri arendamist strateegilistest eesmärkidest protsesside ja tehnoloogiliste lahendusteni, sidudes need iteratiivseks tervikuks. Selle keskne element on arhitektuuri arendusmeetod (ADM), mis toetab arhitektuuri kujundamist äriprotsesside, andmete, rakenduste ja tehnoloogia kihtides ning võimaldab neid seoseid käsitleda juhitud arendusprotsessina (The Open Group, 2018, lk 37–40).

TOGAFi arhitektuuri arendusprotsessi loogikat ja erinevate etappide seotust illustreerib joonis 3, mis näitab, kuidas organisatsiooni visioon, arhitektuurikihtide kujundamine ja muudatuste juhtimine on seotud ühtseks iteratiivseks protsessiks.



Joonis 3. TOGAFi arhitektuuri arendusmeetodi (ADM) tsükkel (lihtsustatud)
Allikas: autori koostatud The Open Group (2018, lk 39–40) põhjal.

TOGAFi täiendab ArchiMate modelleerimiskeel, mis võimaldab visualiseerida äriprotsesside, rollide, süsteemide ja tehnoloogilise taristu vahelisi seoseid. The Open Groupi white paper'i järgi on TOGAF ja ArchiMate teineteist täiendavad standardid: TOGAF toetab arhitektuuri arendusprotsessi ning ArchiMate pakub ettevõttearhitektuuri modelleerimiskeelt ja graafilist notatsiooni (The Open Group, 2017, lk 4–8). Personalifunktsiooni kontekstis aitab see mõista, kuidas rollid ja vastutused seostuvad rakenduste, andmete ja ligipääsuloogikaga ning kus võivad tekkida sõltuvused ja riskikohad.

Käesolevas töös kasutatakse neid raamistikke kontseptuaalse alusena personaliarhitektuuri terviklikkuse mõtestamisel. Nende peamine väärtus seisneb selles, et need muudavad

organisatsiooni erinevate kihtide vahelised seosed nähtavaks ning toetavad riskide tuvastamist ja mõistmist (Aven, 2016, lk 2–3; International Organization for Standardization, 2018, lk 4–7, 8–11).

1.2.5. Personaliarhitektuuri roll organisatsiooni strateegias

Personaliarhitektuuri strateegiline tähendus seisneb selles, et see seob personalivaldkonna lahendused organisatsiooni eesmärkide ja toimimisloogikaga. Becker ja Huselid (2006, lk 899–901, 903–906) rõhutavad, et personalisüsteemide strateegiline sobivus mõjutab organisatsiooni võimet strateegiat ellu viia. Kui personaliarhitektuur ei ole strateegiaga kooskõlas, võivad tekkida vastuolud juhtimise, tehnoloogiliste lahenduste ja igapäevase töökorralduse vahel, mis nõrgestavad organisatsiooni toimivust (Becker & Huselid, 2006, lk 899–906; Lepak & Snell, 1999, lk 33–37).

Strateegilises vaates tähendab personaliarhitektuur erinevate inimkapitali tüüpide ja personalipraktikate sobitamist organisatsiooni vajadustega. Lepak ja Snell (1999, lk 42–45) rõhutavad, et organisatsioonis ei pruugi olla üht parimat personalipraktikate kogumit kõigile töötajatele, vaid personalisüsteemid peaksid arvestama inimkapitali väärtuse, unikaalsuse ja muutumisega ajas. Käesolevas töös laiendatakse seda vaadet infotehnoloogiafookusega organisatsioonidele, kus rollide ja kompetentside eristamine peab kajastuma ka vastutustes, ligipääsudes ja kontrollides. Seda vaadet toetab ka uuem strateegilise personalijuhtimise kirjandus, mille järgi on personali roll viimase kahekümne aasta jooksul muutunud üha ristfunktsionaalsemaks ja andmepõhisemaks ning tehnoloogiline areng on sidunud personali funktsiooni varasemast tihedamalt organisatsiooni väärtusloome, kultuuri, vastavusnõuete järgimise ja laiemate juhtimisprotsessidega (Fenwick et al., 2024, lk 1–2). Fenwick et al. (2024, lk 2–3) rõhutavad ühtlasi, et tänapäevases organisatsioonis ei ole personaliosakond enam pelgalt administratiivne või kitsalt strateegiline tugifunktsioon, vaid osa laiemast organisatsioonilisest ja tehnoloogilisest süsteemist, mille kaudu mõjutatakse inimeste juhtimist, töökorraldust ja organisatsiooni kohanemisvõimet.

Infotehnoloogiafookusega organisatsioonides tuleb siduda töötajate kompetentsid, ligipääsuõigused ja vastutusalad nii äriliste eesmärkide kui ka riskijuhtimise põhimõtetega. Seetõttu ei toeta personaliarhitektuur ainult strateegia elluviimist, vaid mõjutab ka töövoogude usaldusväärsust, personaliandmete kaitset ja süsteemsete riskide ennetamist (Aven, 2016, lk 5–6; Kaplan & Mikes, 2012, lk 4–5, 9). Sellest tulenevalt võib personaliarhitektuuri terviklikkuse astet

käsitleda organisatsiooni suutlikkuse näitajana, mille nähtavaks muutumisel on oluline roll ka võtmeisikute teadlikkusel.

1.3. Personaliarhitektuuri terviklikkus

Eelnevas alapeatükis määratletud personaliarhitektuuri terviklikkust kasutatakse edasises analüüsis mõistena, mille abil hinnata rollide, protsesside, süsteemide, andmekasutuse ja kontrollimehhanismide sidusust. Personaliarhitektuuri terviklikkus väljendab organisatsioonilise tasandi omadust: kuivõrd kooskõlaliselt on personalivaldkonna lahendused seotud organisatsiooni toimimisloogika, IT, juhtimismehhanismide ja riskijuhtimisega (Lepak & Snell, 1999, lk 33; Becker & Huselid, 2006, lk 903–904; Ross et al., 2006, lk 8–9). Selle töö uurimisobjekti seisukohalt on oluline just see, kas personaliga seotud otsused, protsessid ja kontrollid moodustavad organisatsioonis juhitud terviku või jäävad funktsioonide, süsteemide ja vastutusalade vahel killustunuks.

Personaliarhitektuuri terviklikkus muutub organisatsioonis nähtavaks eri funktsioonide kaudu. Personalifunktsioon puutub kokku töötaja elukaare, rollide, arenduse ja töökorraldusega; IT-funktsioon näeb süsteeme, ligipääse, töövooge ja tehnoloogilisi sõltuvusi; riski- või õigusfunktsioon keskendub kontrollidele, haavatavustele, vastutusele ja nõuetele vastavusele. Need vaated kirjeldavad sama organisatsioonilist tervikut erinevatest kokkupuutepunktidest. Seetõttu ei hinnata empiirilises osas ainult seda, mida vastajad personaliarhitektuurist teavad, vaid seda, millise pildi annavad nende kirjeldused organisatsiooni personaliarhitektuuri tegelikust sidususest. Organisatsiooniarhitektuuri käsitlus toetab seda lähtekohta, sest organisatsiooni toimivus sõltub rollide, protsesside ja tehnoloogiliste lahenduste kooskõlast (Ross et al., 2006, lk 8–9). Ka uuem personalijuhtimise kirjandus rõhutab personalifunktsiooni ristfunktsionaalset, andmepõhist ja tehnoloogiaga seotud rolli organisatsiooni kohanemisvõime, vastavusnõuete ja juhtimispraktikate kujundamisel (Fenwick et al., 2024, lk 1–3).

Selles töös eristatakse personaliarhitektuuri terviklikkust ja personaliarhitektuuri teadlikkust analüütiliselt erinevate tasanditena. Terviklikkus viitab organisatsiooni ülesehituse ja juhtimisloogika sidususele, teadlikkus aga sellele, kuidas juhid ja võtmeisikud neid seoseid mõistavad, kirjeldavad ja otsustes arvesse võtavad. Teadlikkus on seega individuaalse või funktsioonipõhise tasandi nähtus, mille kaudu saab hinnata, kui nähtavaks personaliarhitektuuri

terviklikkus organisatsioonis muutub. Kui eri funktsioonide esindajad kirjeldavad rolle, protsesse, ligipääse ja riske omavahel seotult, viitab see tugevamale ühisele arusaamale. Kui kirjeldused jäävad funktsioonipõhiselt eraldi, võib see osutada tervikpildi lünkadele või nõrgemale koordineerimisele.

Riskijuhtimise seisukohalt on see eristus oluline, sest riskide tuvastamine ja hindamine eeldab arusaama süsteemsetest seostest. Aveni (2016, lk 2–3) käsitluses sõltub riskijuhtimise kvaliteet teadmiste tasemest ja teadmiste piirangute teadvustamisest, ISO 31000 raamistik seob riskijuhtimise juhtimisprotsesside, otsustamise ja seirega (International Organization for Standardization, 2018, lk 4–5, 8–9, 14–15). Digitaalse personalijuhtimise küpsust käsitlev kirjandus rõhutab samuti liikumist killustunud praktikatelt süsteemsema ja paremini juhitud toimimiseni (Shahiduzzaman, 2025, lk 1–2). GDPR-i ja andmekaitse käsitlused näitavad, et riskid tekivad sageli rollide ebaselguse, liigsete ligipääsude ja killustunud andmevoogude tõttu (McMenemy et al., 2017; Smirnova & Travieso-Morales, 2024, lk 333–338). Nende lähtekohtade põhjal kasutatakse personaliarhitektuuri terviklikkust selles töös analüütilise mõistena, mille abil hinnata, kui sidusalt on organisatsioonis seotud personal, protsessid, tehnoloogia ja riskijuhtimine.

1.3.1. Personaliarhitektuuri terviklikkus kui analüütiline mõiste

Analüütilise mõistena võimaldab personaliarhitektuuri terviklikkus eristada kahte tasandit: organisatsiooni tegelikku sidusust ja üksikisikute teadlikkust sellest sidususest (Lepak & Snell, 1999, lk 31–37; Ross et al., 2006, lk 8–9). Seetõttu ei väljendu personaliarhitektuuri terviklikkus üksnes selles, mida organisatsioonis teatakse, vaid eelkõige selles, kuidas personaliga seotud valikud on tegelikult seotud organisatsiooni eesmärkide, toimimisloogika ja strateegiliste võimekustega (Becker & Huselid, 2006, lk 903–906; Lepak & Snell, 1999, lk 33–37).

Selline käsitlus võimaldab eristada kahte tasandit. Individuaalsel tasandil võib personaliarhitektuuri teadlikkus olla funktsiooniti erinev, sest personali-, IT- ning riski- või õigusfunktsioonidel on erinev vastutus, vaatenurk ja ligipääs informatsioonile (Ross et al., 2006, lk 8–9; Fenwick et al., 2024, lk 2–3). Organisatsioonilisel tasandil huvitab käesolevat tööd aga see, kas need erinevad osad moodustavad sidusa terviku või jäävad killustunuks. Seetõttu on põhjendatud käsitleda personaliarhitektuuri terviklikkust organisatsioonilise analüüsi keskse mõistena, samas kui teadlikkus toimib selle terviklikkuse üks olulisi eeldusi ja nähtavuse allikaid. Käesolevas töös ei hinnata seega üksnes seda, kui hästi vastajad personaliarhitektuuri kirjeldada oskavad, vaid ka seda, millise pildi nende kirjeldused annavad organisatsiooni

personaliarhitektuuri terviklikkusest. Selline eristus on oluline, sest organisatsioonis võib esineda olukordi, kus üksikud võtmeisikud mõistavad seoseid hästi, kuid süsteem ise on endiselt killustunud. Samuti võib osa seoseid olla organisatsioonis formaalselt olemas, kuid erinevad funktsioonid ei pruugi neid samal määral tajuda ega mõtestada.

1.3.2. Personaliarhitektuuri terviklikkuse mõõtmed

Käesolevas töös käsitletakse personaliarhitektuuri terviklikkust organisatsioonilise küpsusena, mis väljendub protsesside, tehnoloogiate ja rollide omavahelises sidususes ning kooskõlastatud juhtimises (Ross et al., 2006, lk 8–9, 47–51). Terviklikkus ei ole binaarne nähtus, vaid kujuneb järk-järgult ning hõlmab eri tasandeid, mille kaudu personaliarhitektuur organisatsioonis avaldub. Empiiriliseks hindamiseks eristatakse antud töös kolme omavahel seotud mõõdet: **protsessiline terviklikkus, tehnoloogiline terviklikkus ja rolliline terviklikkus**. Protsessiline terviklikkus viitab sellele, kuivõrd selgelt on personaliprotsessid struktureeritud ja seotud organisatsiooni põhitegevuse ning strateegiliste äriprotsessidega. Becker ja Huselid (2006) rõhutavad, et personaliarhitektuuri väärtus sõltub selle sobivusest strateegiliste äriprotsesside ja strateegia elluviimisega (lk 903–904). Tehnoloogiline terviklikkus hõlmab seda, mil määral toetavad personaliprotsesse infosüsteemid, automatiseeritud töövood ja tehnoloogilised kontrollmehhanismid ning kui sidusalt on need seotud organisatsiooni riskiloogikaga (Ross et al., 2006, lk 47–51; Teixeira et al., 2021, lk 715–717). Rolliline terviklikkus tähendab seda, kuivõrd selgelt on organisatsioonis määratletud kriitilised rollid, vastutused ja ligipääsuõigused ning kui kooskõlastatult need toimivad personali- ja riskijuhtimise vaatest (Lepak & Snell, 1999, lk 33–37, 43–45).

Need mõõtmed on valitud seetõttu, et just nende kaudu avalduvad personaliarhitektuuri terviklikkuse tugevused ja lüngad kõige selgemini. Protsesside killustatus võib tekitada kontrollilünki, tehnoloogiliste sõltuvuste nõrk juhtimine suurendab ligipääsu- ja andmekaitseriske ning rollide ebaselgus nõrgestab vastutuse ja kontrolli rakendumist (KPMG Baltics OÜ, 2022, lk 7, 9; Riigi Infosüsteemi Amet, 2024, lk 19). Seetõttu käsitletakse käesolevas töös terviklikkust mitte staatilise omadusena, vaid küpsusena, mis väljendub nende kolme mõõtme kooskõlastatud kujundamises ja juhtimises. Nende mõõtmete koostoime alusel on koostatud personaliarhitektuuri terviklikkuse küpsusloogika, mis on esitatud tabelis 1.

Tabel 1. Personaliarhitektuuri terviklikkuse küpsustasemed

Tase	Kirjeldus (protsessid – tehnoloogiad – rollid)
5. Optimeeriv	Pidev parendamine ja integreeritud juhtimine: seosed protsesside, süsteemide ja rollide vahel on nähtavad, mõõdetavad ja arendatavad; õppetunnid jõuavad standarditesse ja arhitektuuriotsustesse.
4. Juhtiv	Strateegiline ja süsteemne seoste haldamine: personaliarhitektuur on joondatud strateegiaga; riskid ja kontrollid on teadlikult kujundatud ning kooskõlastatud üle funktsioonide.
3. Korrastatud	Standardiseeritud protsessid ja kontrollid: põhiprotsessid on kirjeldatud, rollid ja vastutused on määratud; tehnoloogilised töövood toetavad järjepidevat toimimist.
2. Reaktiivne	Ad hoc lähenemine ja probleemidele reageerimine: seosed protsesside, tehnoloogiate ja rollide vahel on osaliselt kujunenud, kuid ebaühtlased; kontrollid tekivad sageli pärast intsidenti või auditileidu.
1. Algeline	Killustunud tegevused ja nõrk sidusus: protsesside, tehnoloogiate ja rollide seosed on ebaselged; toimimine sõltub suurel määral üksikisikutest; kontrollilüngad ja riskid jäävad varjatuks.

Allikas*:* autori koostatud Ross et al. (2006, lk 8–10, 47–51), Aven (2016, lk 2–3, 5–6) ning ISO 31000:2018 (lk 4–7, 8–14) põhjal.

Käesolevas töös loodud viietasemeline küpsusloogika võimaldab intervjuuandmeid klassifitseerida vastavalt sellele, kui sidusalt on organisatsioonis seotud protsessid, tehnoloogiad ja rollid ning kui kooskõlastatult neid juhitakse. Küpsustasemete eesmärk ei ole mõõta üksikute vastajate teadmisi, vaid hinnata personaliarhitektuuri terviklikkuse astet organisatsioonis (Ross et al., 2006, lk 47–51; Aven, 2016, lk 2–3, 6).

1.3.3. Personaliarhitektuuri terviklikkuse indikaatorid

Empiirilises analüüsis hinnatakse personaliarhitektuuri terviklikkust indikaatorite kaudu, mis aitavad tuvastada, kui sidusalt on organisatsioonis seotud personal, protsessid, tehnoloogia ja kontrollimehhanismid. Need indikaatorid ei kirjelda üksikuid personalipraktikaid, vaid organisatsiooni süsteemset võimekust kujundada ja juhtida personaliarhitektuuri osana laiemast toimimisloogikast.

Käesolevas töös kasutatakse viit peamist indikaatorit: strateegiline sidusus, rollide ja vastutuste selgus, protsesside läbipaistvus ja standardiseeritus, tehnoloogilise arhitektuuri sidusus ning riskide käsitlemise süsteemsus.

Strateegiline sidusus väljendub selles, mil määral on personaliprotsessid ja rollimudelid seotud organisatsiooni eesmärkide ja kriitiliste võimekustega (Becker & Huselid, 2006, lk 903–906; Lepak & Snell, 1999, lk 33–37). Rollide ja vastutuste selgus viitab sellele, kas organisatsioonis on üheselt arusaadav, kelle vastutada on rollid, infoturbe juhtimine, kontrollid ja otsused (KPMG Baltics OÜ, 2022, lk 7, 9; Riigi Infosüsteemi Amet, 2024, lk 19). Protsesside läbipaistvus ja standardiseeritus näitavad, kuivõrd personaliprotsessid on dokumenteeritud, järjepidevad ja organisatsiooniüleselt juhitavad (Smirnova & Travieso-Morales, 2024, lk 334, 337). Tehnoloogilise arhitektuuri sidusus hõlmab seda, mil määral on personaliprotsesse toetavad infosüsteemid, andmevood ja tehnoloogilised sõltuvused omavahel kooskõlas (Ross et al., 2006, lk 47–48; Teixeira et al., 2021, lk 715–717). Riskide käsitlemise süsteemsus peegeldab seda, kuivõrd järjepidevalt suudab organisatsioon märgata, põhjendada ja ennetada personaliga seotud riske, seostades need rollide, protsesside ja tehnoloogiaga (Aven, 2016, lk 2–3, 5–6; Kaplan & Mikes, 2012, lk 4–5, 9).

Individuaalse tasandi teadlikkus ilmneb seejuures selles, kuidas personali-, IT- ning riski- või õigusfunktsiooni esindajad neid seoseid kirjeldavad ja tõlgendavad. Empiirilises osas kasutatakse neid indikaatoreid selleks, et võrrelda, millise pildi annavad eri funktsioonide esindajad personaliarhitektuuri terviklikkusest ning millistes kohtades ilmnevad tugevused, lüngad ja funktsioonipõhised erinevused.

1.4. Personaliarhitektuuri terviklikkuse ja riskijuhtimise seosed

Personaliarhitektuuri terviklikkus mõjutab riskijuhtimise praktikate kujunemist, sest see määrab, kui sidusalt on organisatsioonis seotud rollid, vastutused, personaliprotsessid, ligipääsud, andmevood ja kontrollimehhanismid. Riskid ei tulene üksnes tehnoloogilistest lahendustest või väliskeskkonnast, vaid ka sellest, kuidas inimesed, protsessid ja tehnoloogia on omavahel kooskõlastatud (Aven, 2016, lk 2–3; Ross et al., 2006, lk 8–9).

Riskijuhtimise kvaliteet sõltub sellest, kas organisatsioonil on terviklik ülevaade kriitilistest rollidest, protsessidest ja süsteemsetest sõltuvustest. Kui need seosed on selged, on võimalik riskikohti märgata enne nende realiseerumist. Seetõttu toetab personaliarhitektuuri terviklikkus ennetavat riskijuhtimist, sidudes riskihinnangud tegelike rolli-, protsessi- ja süsteemiseostega.

Kui terviklikkus on nõrk, muutub riskijuhtimine reageerivaks ning probleemid avalduvad ligipääsuvigade, andmekaitserikkumiste ja protsessikatkestustena, mis viitavad arhitektuurilisele killustatusele (Ross et al., 2006, lk 5–8).

1.4.1. Personaliarhitektuuriga seotud riskid ja lüngad

Personaliarhitektuuriga seotud riskid tulenevad sellest, kuidas on kujundatud rollid, vastutused, ligipääsuõigused ja personaliprotsessid (Lepak & Snell, 1999, lk 33–37). Need riskid ei teki enamasti üksikute vigade tulemusel, vaid rollide, protsesside ja tehnoloogiliste sõltuvuste koosmõjus (Aven, 2016, lk 2–3).

Praktikas avalduvad need riskid ligipääsuhalduses, rollipõhises autoriseerimises ning personaliandmete töötlemises. Kui ligipääsud on liiga laiad, rollid ebaselged või protsessid killustunud, suureneb kontrollilünkade ja rikkumiste tõenäosus (Kaplan & Mikes, 2012, lk 5–6; Hjerppe et al., 2019, lk 3–4, 6).

Need riskid muutuvad eriti nähtavaks personali elukaare kriitilistes etappides, nagu värbamine, sisseelamine, rollimuutused ja töösuhte lõpetamine, kus ristuvad erinevad süsteemid ja vastutajad. Kui nendes punktides puudub terviklik koordineerimine, tekivad kontrollilüngad, mille kaudu võivad realiseeruda andmekaitse-, infoturbe- ja operatsioonilised riskid (McMenemy et al., 2017). Seetõttu võib rolli-, protsessi- ja tehnoloogialünki käsitleda personaliarhitektuuri terviklikkuse nõrgenemise ilmingutena, millel on otsene mõju riskijuhtimise süsteemsusele.

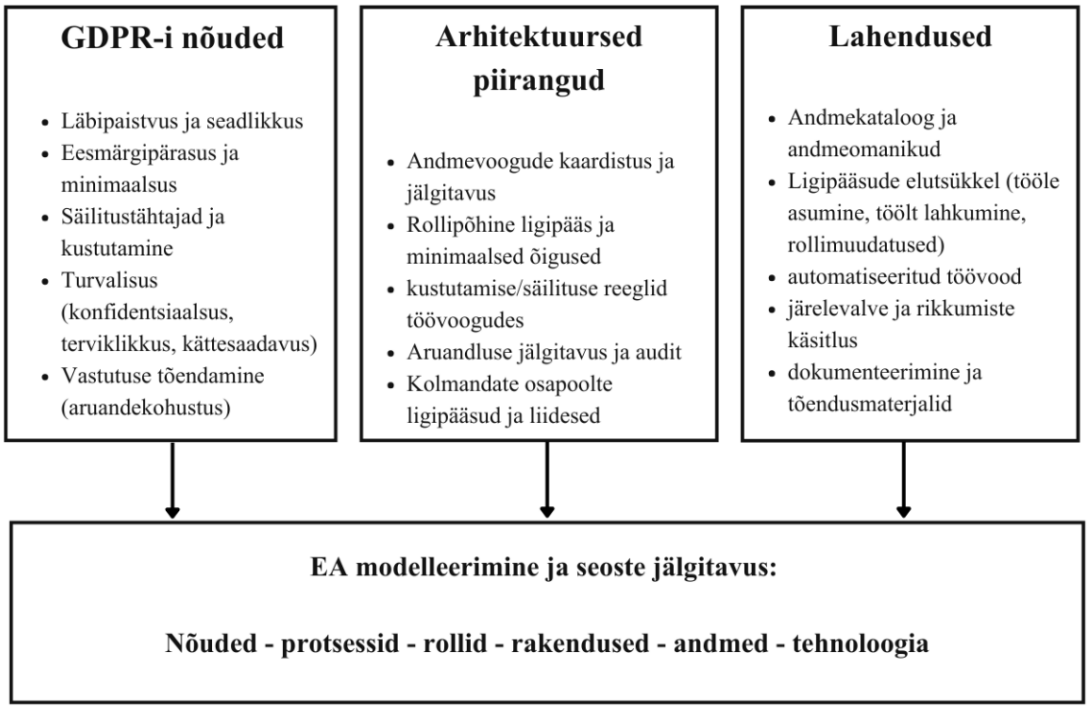
1.4.2. Infotehnoloogiline kontekst ja küberriskid

Infotehnoloogiast sõltuvates organisatsioonides on personaliprotsessid tihedalt seotud infosüsteemide, ligipääsuhalduse ja andmevoogudega (Ross et al., 2006, lk 8–9). Seetõttu mõjutab personaliarhitektuuri terviklikkus otseselt nii süsteemide toimimist kui ka turvalisust.

Küberriskid ei ole üksnes tehnilised, vaid tekivad tehnoloogia, andmete, protsesside ja inimkäitumise koosmõjus (Riigi Infosüsteemi Amet, 2024, lk 16, 23). Praktikas avalduvad probleemid sageli ligipääsuvigade, kontrollilünkade ja süsteemikatkestustena, mis mõjutavad samaaegselt nii töökorraldust kui ka andmekaitset (Riigi Infosüsteemi Amet, 2024, lk 18–20).

Eesti uuringud kinnitavad, et riskitaset tõstavad keskse infoturberolli puudumine, teenuspartnerile vastutuse ekslik eeldamine ning vähene sidus ülevaade riskidest (KPMG Baltics OÜ, 2022, lk 2, 7, 9). Seda seost tugevdab regulatiivne raamistik, nagu NIS2 ja E-ITS, mis rõhutavad rollide, vastutuste ja turvameetmete selgust organisatsiooni tasandil (Majandus- ja Kommunikatsiooniministeerium, 2024, lk 8–10, 16–17). Sellises keskkonnas muutub personaliarhitektuuri terviklikkus kriitiliseks, sest üks rolli- või ligipääsumuudatus võib mõjutada mitut süsteemi ja protsessi korraga. Mida sidusam on nende seoste juhtimine, seda tõenäolisem on, et riske märgatakse varakult ja juhtimine jääb ennetavaks.

Joonis 4 illustreerib, kuidas GDPR-i nõuded tõlgitakse organisatsioonis arhitektuurseteks piiranguteks ning edasi konkreetseteks lahendusteks ja kontrollideks.



Joonis 4. GDPR-i nõuete tõlkimine arhitektuurseteks piiranguteks ja kontrollideks
Allikas: autori koostatud Hjerppe et al. (2019, lk 3–6) ja Teixeira et al. (2021, lk 715–718, 720–723) põhjal.

Joonise väärtus seisneb selles, et see teeb nähtavaks seose õiguslike nõuete, rollide, protsesside, andmete ja süsteemide vahel, näidates, et andmekaitse sõltub nende elementide sidusast integreerimisest organisatsiooni arhitektuuri. GDPR-i nõuete rakendamine ei piirdu üksikute tehniliste kontrollidega, vaid eeldab regulatiivsete nõuete, kasutusjuhtude, andmevoogude, rollide

ja arhitektuursete lahenduste läbimõeldud seostamist (Hjerppe et al., 2019, lk 3–9; Teixeira et al., 2021, lk 715–718, 720–723; Lankhorst et al., 2009, lk vi).

1.5. Riskijuhtimise teoreetiline alus

Riskijuhtimine toetab organisatsiooni eesmärkide saavutamist olukorras, kus otsuseid tuleb teha ebakindluse ja võimalike tagajärgede tingimustes (International Organization for Standardization, 2018, lk v, 1–2). Selle kvaliteet sõltub sellest, kui hästi suudab organisatsioon siduda riskid oma eesmärkide, protsesside, vastutuste ja kontrollidega ning millisele teadmusbaasile riskihinnangud tuginevad (Aven, 2016, lk 2–3, 6; International Organization for Standardization, 2018, lk 5–7, 9, 11, 14–15).

Tehnoloogiakesksetes suurorganisatsioonides tekivad riskid sageli mitme sõltuvuse koosmõjus. Operatsioonid, personaliprotsessid, andmetöötlus ja ligipääsud on seotud IT-süsteemide ning rollipõhiste õigustega, mistõttu võib ühe protsessi või rolli muutus mõjutada korraga mitut töövoogu, süsteemi ja kontrolli (Ross et al., 2006, lk 5–9). Riskijuhtimise seisukohalt tähendab see vajadust näha riske organisatsiooni toimimisloogika osana.

Selle töö vaates seob riskijuhtimise teoreetiline alus omavahel kaks keskset küsimust: kuidas organisatsioon mõistab riske ebakindluse tingimustes ning kuidas need riskid on seotud rollide, protsesside, tehnoloogiate ja kontrollimehhanismidega. Siit tekib otsene seos personaliarhitektuuri terviklikkusega. Mida sidusamalt on personaliga seotud rollid, ligipääsud, töövood ja kontrollid organisatsioonis kujundatud, seda paremad eeldused on riskide varajaseks märkamiseks, hindamiseks ja juhtimiseks.

Riskide kategooriad aitavad seda seost täpsustada. Kaplan ja Mikes (2012, lk 4–9) eristavad välditavaid, strateegilisi ja väliseid riske, mis eeldavad erinevat juhtimisloogikat. Personaliarhitektuuri terviklikkuse vaates on see eristus oluline, sest personaliprotsessides võivad riskid avalduda nii sisemiste kontrollilünkadena, strateegiliste rolli- ja kompetentsivalikutena kui ka väliskeskkonnast tulenevate regulatiivsete või küberriskidena. Seetõttu kasutatakse riskijuhtimise teooriat selles töös raamistikuna, mille abil hinnata, kuidas personaliga seotud rolli, protsessi- ja tehnoloogiaseosed toetavad ennetavat ning süsteemset riskijuhtimist.

1.5.1. Riskijuhtimise definitsioon ja roll strateegilises juhtimises

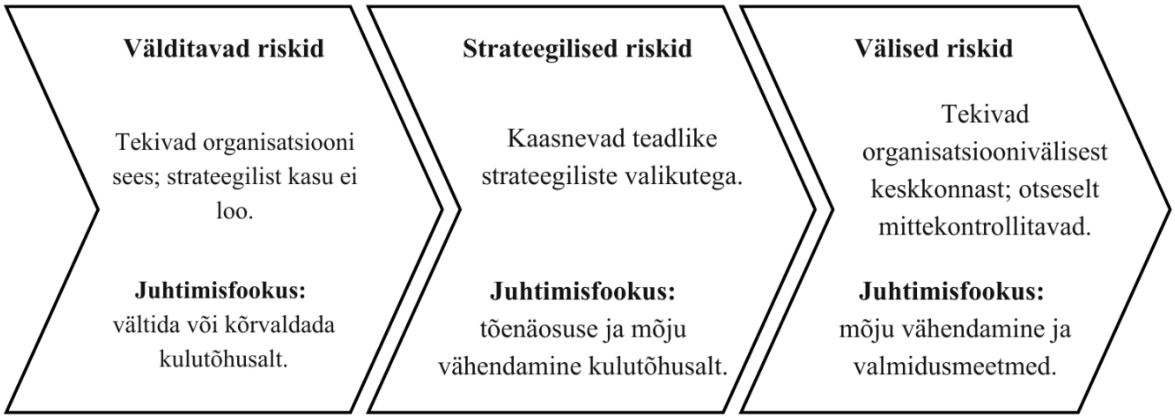
Varasemalt käsitleti riskijuhtimist peamiselt tehnilise ja kvantitatiivse tegevusena, mis keskendus tõenäosuste ja võimalike kahjude hindamisele. Kaasaegne käsitlus näeb riskijuhtimist otsustamist toetava tegevusena ebakindluse tingimustes, kus keskne on lisaks tagajärgede hindamisele ka teadmiste kvaliteedi ja piirangute arvestamine (Aven, 2016, lk 1–3).

ISO 31000 defineerib riskijuhtimise kui koordineeritud tegevuste kogumi, mille abil organisatsiooni riske suunatakse ja kontrollitakse. Standard rõhutab, et riskijuhtimine peab olema integreeritud organisatsiooni juhtimisse ja põhitegevustesse, mitte toimima eraldiseisva kontrollimehhanismina (International Organization for Standardization, 2018, lk 1, 4–7).

Strateegilisel tasandil tähendab see, et riskijuhtimine kujundab, milliseid ebakindlusi organisatsioon on valmis aktsepteerima ja kuidas neid juhitakse. Tehnoloogia- ja andmepõhises keskkonnas suurendavad killustunud protsessid, hajunud andmed ja ebaselged vastutusjaotused süsteemsete riskide tõenäosust (Ross et al., 2006, lk 5–9; Hjerppe et al., 2019, lk 3–6; Smirnova & Travieso-Morales, 2024, lk 337–338).

Riskide kolm kategooriat

Riskide süstemaatiline käsitlemine eeldab arusaama, et riskid erinevad nii tekkepõhjuse kui ka juhtimisvõimaluste poolest. Kaplan ja Mikes (2012, lk 4–9) eristavad kolme riskikategooriat: välditavad, strateegilised ja välised riskid. Riskide jaotus ning sellele vastavad juhtimisfookused on esitatud joonisel 5.



Joonis 5. Riskide kolm kategooriat ja juhtimisloogika

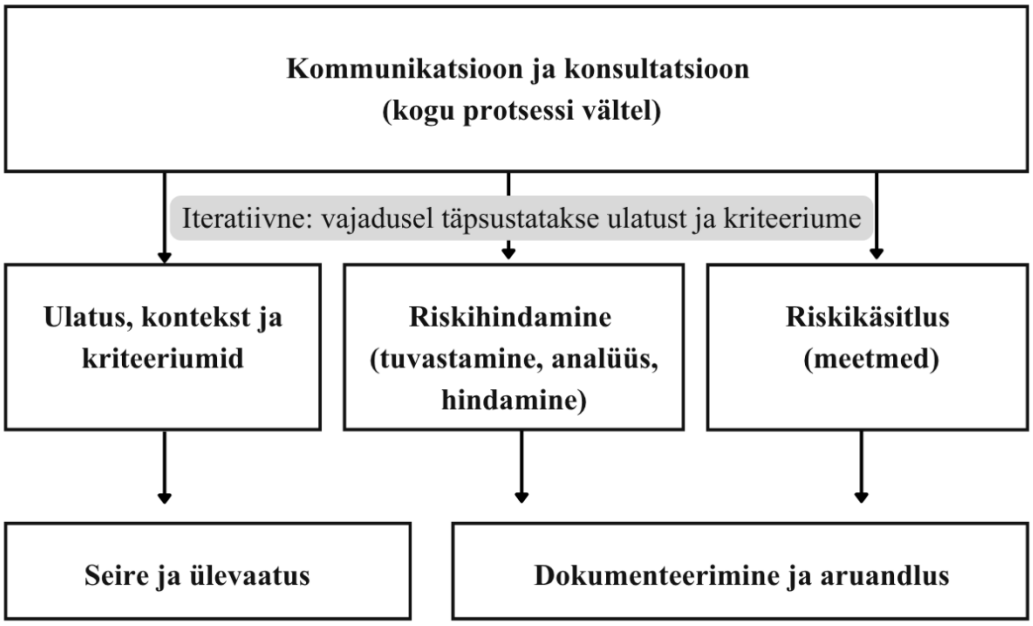
Allikas: autori koostatud Kaplan ja Mikes (2012, lk 4–5, 9) põhjal.

Välditavad riskid tekivad organisatsiooni sees ega loo strateegilist väärtust, olles seotud näiteks reeglite rikkumise või puuduliku kontrolliga. Personaliarhitektuuri kontekstis avalduvad need ebaselgete rollipiiride, valesti määratud ligipääsuõiguste ja kooskõlastamata töövoogudena.

Strateegilised riskid kaasnevad teadlike otsustega, nagu kasv, muutus ja innovatsioon, ning võivad väljenduda kompetentsivajaduse muutumises ja rollide ümberkujundamises. Välised riskid tulenevad organisatsioonivälisest keskkonnast, näiteks regulatiivsetest muutustest või küberohtudest, ning ei ole otseselt kontrollitavad (Kaplan & Mikes, 2012, lk 4–5, 9). Kõigi riskikategooriate käsitlemine eeldab arusaama rollide, protsesside ja tehnoloogiate vahelistest seostest, kuna riskid avalduvad nende koosmõjus.

1.5.2. Riskijuhtimise protsess ning riskide tuvastamine ja hindamine

Riskijuhtimine on iteratiivne protsess, mille käigus määratletakse kontekst, tuvastatakse ja hinnatakse riske, kavandatakse riskikäsitlusmeetmed ning tagatakse pidev seire ja kommunikatsioon (International Organization for Standardization, 2018, lk 8–14). Selle protsessi loogikat illustreerib joonis 6.



Joonis 6. Riskijuhtimise protsess (lihtsustatud) ISO 31000:2018 alusel
Allikas: autori koostatud ISO 31000:2018 (lk 8–14) põhjal.

Riskide tuvastamine ja hindamine on protsessi keskne osa, kuna need loovad aluse teadlike otsuste tegemiseks. Riskide hindamine ei piirdu ohtude loetlemisega, vaid eeldab arusaama organisatsioonist terviksüsteemina, kus riskid kujunevad protsesside, tehnoloogiate ja inimtegevuse koosmõjus (Aven, 2016, lk 2–3, 6).

Personalivaldkonnas tähendab see, et riskid tekivad sageli rollide, vastutuste, ligipääsuõiguste ja töövoogude ebakõlade tulemusena. Uuringud näitavad, et näiteks värbamise, andmetöötluse ja ligipääsude lõpetamisega seotud protsessides võivad riskid jääda varjatuks, kui andmevood ja vastutused ei ole piisavalt läbipaistvad (Hjerppe et al., 2019, lk 3–6; Teixeira et al., 2021, lk 715–717; Smirnova & Travieso-Morales, 2024, lk 334, 337).

1.5.3. Suurorganisatsioonide riskijuhtimise praktikad

Suurorganisatsioonides on riskijuhtimine üldjuhul formaliseeritud ning hõlmab riskipoliitikaid, registreid, kontrollimehhanisme ja regulaarseid hinnanguid (International Organization for Standardization, 2018, lk 8–15). Selline raamistik loob eeldused süstemaatiliseks käsitluseks, kuid ei taga iseenesest tõhusat juhtimist.

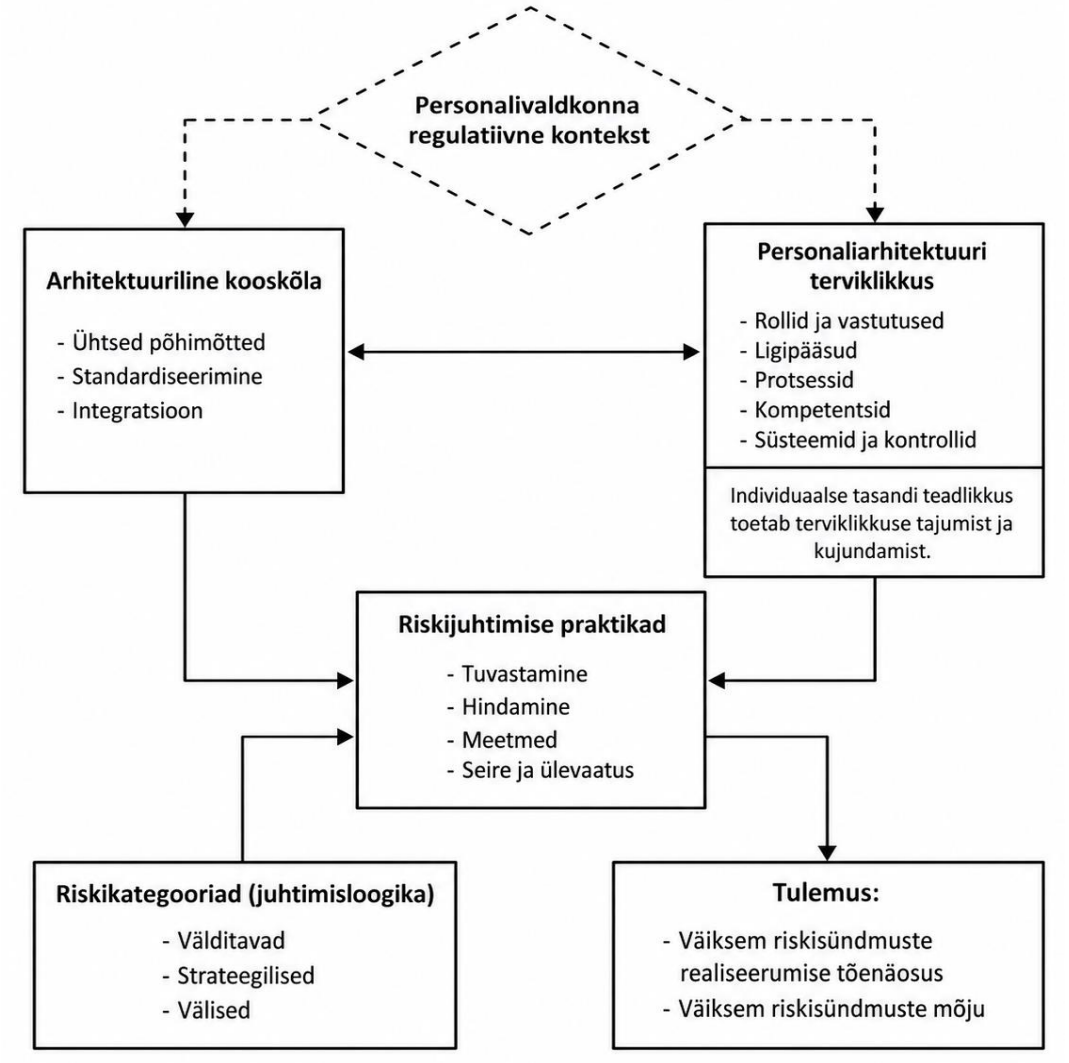
Praktikate kvaliteet sõltub sellest, kuivõrd hästi on riskijuhtimine seotud organisatsiooni tegelike protsesside, rollide ja vastutustega (Aven, 2016, lk 2–3, 6; Ross et al., 2006, lk 5–9). Personalivaldkonnas avalduvad riskid eeskätt olukordades, kus rollid, ligipääsuõigused ja tööprotsessid ei ole selgelt määratletud või omavahel kooskõlas.

Eesti kontekstis näitavad uuringud, et töötajate teadlikkus, keskse infoturberolli puudumine ja ebaselge vastutus on jätkuvalt olulised haavatavuse allikad (KPMG Baltics OÜ, 2022, lk 7–9; Riigi Infosüsteemi Amet, 2024, lk 19). See viitab, et riskijuhtimise süsteemsus sõltub otseselt organisatsiooni suutlikkusest siduda riskikaalutlused igapäevase toimimisega.

Käesoleva töö kontekstis tähendab see, et riskijuhtimise kvaliteet on seotud personaliarhitektuuri terviklikkusega: mida sidusamalt on seotud rollid, vastutused, protsessid ja tehnoloogilised lahendused, seda süsteemsemalt on võimalik riske märgata ja juhtida.

1.6. Teoreetiline süntees: personaliarhitektuuri terviklikkuse ja riskijuhtimise integratsioonimudel

Eelnevates alapeatükkides käsitletud teoreetilised lähtekohad koondatakse integratsioonimudeliks, mis seob personaliarhitektuuri terviklikkuse, arhitektuurilise kooskõla, riskikategooriad ja riskijuhtimise praktikad ühtseks analüütiliseks raamistikuks. Mudeli eesmärk on näidata, kuidas rollide, vastutuste, protsesside, ligipääsude ja tehnoloogiliste sõltuvuste sidus kujundamine mõjutab organisatsiooni võimet riske märgata, hinnata ja juhtida. Mudeli struktuur on esitatud joonisel 7.



Joonis 7. Personaliarhitektuuri terviklikkuse ja riskijuhtimise integratsioonimudel
Allikas: autori koostatud Lepak ja Snell (1999, lk 35–38), Becker ja Huselid (2006, lk 899–906), Boon et al. (2019, lk 2498–2502, 2517–2519), Ross et al. (2006, lk 8–10, 25–29, 47–51), Aven (2016, lk 2–3, 5–6), Kaplan ja Mikes (2012, lk 4–5, 9–10) ning ISO 31000:2018 (lk 4–7, 8–14) põhjal.

Mudelis tähistavad katkendjooned personalivaldkonna regulatiivse konteksti mõju, mis toimib taustatingimusena ning suunab nii arhitektuurilist kooskõla kui ka personaliarhitektuuri terviklikkuse kujunemist. Täisjooned tähistavad mudeli põhikomponentide otsesemaid seoseid. Individuaalse tasandi teadlikkus toimib mudelis toetava tegurina, mõjutades seda, kui hästi eri funktsioonide esindajad seoseid tajuvad, kirjeldavad ja juhtimisotsustesse tõlgivad.

Mudeli keskmes on personaliarhitektuuri terviklikkus ehk personaliga seotud rollide, vastutuste, ligipääsude, protsesside, kompetentside, süsteemide ja kontrollimehhanismide sidusus. Terviklikkus väljendub nende elementide koostoimes organisatsiooni toimimisloogika ja riskikeskkonnaga (Ross et al., 2006, lk 8–9; Becker & Huselid, 2006, lk 899–906). Personalisüsteemide kirjandus toetab sama loogikat: personalipraktikate mõju kujuneb nende koosmõjus ning personalisüsteemi mõtestamisel on oluline selgelt piiritleda, millised praktikad süsteemi kuuluvad ja kuidas need tervikuna toimivad (Boon et al., 2019, lk 2498–2502, 2517–2519).

Personaliarhitektuuri terviklikkus on seotud arhitektuurilise kooskõlaga, mis hõlmab organisatsiooniüleseid põhimõtteid, standardiseeritust ja integratsiooni. Arhitektuuriline kooskõla tähendab, et personaliga seotud otsused, protsessid ja tehnoloogilised lahendused lähtuvad ühisest toimimisloogikast, mitte üksikute üksuste eraldiseisvatest valikutest (Ross et al., 2006, lk 8–9, 26–28). Kooskõla muudab rolli-, ligipääsu- ja protsessiloogika selgemaks; terviklikkus aitab seda kooskõla hoida ja riskijuhtimisse siduda.

Riskijuhtimise praktikad hõlmavad mudelis riskide tuvastamist, hindamist, meetmete kavandamist, seiret ja ülevaatust (International Organization for Standardization, 2018, lk 8–14). Kui rollide, protsesside, ligipääsude ja andmevoogude seosed on nähtavad ja kooskõlastatud, on riskijuhtimine tõenäolisemalt süsteemne ja ennetav. Kui seosed on killustunud, kaldub riskijuhtimine muutuma reageerivaks ning keskendub pigem juba avaldunud probleemidele kui nende varajasele ennetamisele (Aven, 2016, lk 2–3; International Organization for Standardization, 2018, lk 3–5, 8–14).

Riskikategooriad aitavad mudelis eristada, millist juhtimisloogikat eri riskid vajavad. Kaplan ja Mikes (2012, lk 4–9) eristavad välditavaid, strateegilisi ja väliseid riske. Välditavad riskid eeldavad eelkõige kontrollide ja reeglite tugevdamist, strateegilised riskid teadlikku juhtimisotsust

ja riskivalmiduse määratlemist ning välised riskid suuremat kohanemis- ja reageerimisvõimet (Kaplan & Mikes, 2012, lk 5–9).

Regulatiivne kontekst mõjutab mudelis nii terviklikkust kui ka arhitektuurilist kooskõla. Andmekaitse-, infoturbe- ja küberturbenõuded suunavad organisatsioone selgemalt määratlema rolle, ligipääse, vastutusi, andmevooge ja kontrollimehhanisme (Rozehnal & Novák, 2018, lk 362–365; Hjerppe et al., 2019, lk 1–2). Seetõttu ei ole regulatiivne kontekst mudelis eraldi tulemusmuutuja, vaid taustatingimus, mis suurendab vajadust sidusa personaliarhitektuuri järele.

Integratsioonimudel väljendab järgmist põhjusloogikat: personaliarhitektuuri terviklikkus muudab süsteemsed seosed nähtavaks, arhitektuuriline kooskõla aitab neid organisatsiooniüleselt hoida ning riskikategooriad suunavad sobivate riskijuhtimise praktikate valikut. Nende tegurite koosmõjul kujunevad süsteemsemad riskijuhtimise praktikad, mis aitavad vähendada riskisündmuste realiseerumise tõenäosust ja mõju.

Mudeli teoreetiline väärtus seisneb selles, et see seob personaliarhitektuuri, organisatsiooniarhitektuuri, personalisüsteemide ja riskijuhtimise käsitlused üheks tervikuks. Personaliarhitektuuri terviklikkus ei tähenda üksnes personalivaldkonna korrastatust, vaid organisatsiooni suutlikkust juhtida inimeste, protsesside ja tehnoloogia koostoimet süsteemselt.

Empiirilises osas kasutatakse integratsioonimudelit selleks, et hinnata, kuidas personaliarhitektuuri terviklikkus, arhitektuuriline kooskõla, riskikategooriad ja riskijuhtimise praktikad eri funktsioonides avalduvad. Intervjuupõhist analüüsi käsitletakse seega mitte ainult teadlikkuse väljendusena, vaid ka personaliarhitektuuri terviklikkuse avaldumisena organisatsioonis.

2. EMPIIRILINE UURIMUS

Peatükk kirjeldab empiirilise uurimuse metoodilist ülesehitust: uurimisstrateegiat, valimit, andmekogumist, analüüsiviisi ning usaldusväärsuse ja eetika tagamist. Metoodika eesmärk on näidata, kuidas valitud lähenemine võimaldab vastata uurimisküsimustele läbipaistvalt ja jälgitavalt.

Uurimus keskendub personaliarhitektuuri terviklikkuse seostele riskijuhtimise praktikatega Eesti infotehnoloogiafookusega suurorganisatsioonides. Kuna nähtus on mitmetasandiline, kontekstist sõltuv ning seotud organisatsioonisiseste tõlgenduste ja praktikatega, kasutatakse kvalitatiivset lähenemist. Poolstruktureeritud intervjuud võimaldavad uurida, kuidas personali-, IT- ning riski- või õigusfunktsiooni esindajad kirjeldavad rollide, protsesside, süsteemide, andmete ja kontrollide seoseid ning nende mõju riskide ennetamisele ja juhtimisele.

Empiirilises osas ei hinnata üksnes vastajate teadlikkust, vaid kasutatakse nende kirjeldusi ja näiteid personaliarhitektuuri terviklikkuse analüüsimiseks. Seega toimib individuaalse tasandi teadlikkus uurimuses sissepääsuna organisatsioonilise tasandi nähtuse mõistmiseks.

2.1. Uuringu eesmärk ja uurimisküsimused

Empiirilise uuringu eesmärk on selgitada, kuidas personaliarhitektuuri terviklikkus seostub riskijuhtimise praktikatega Eesti infotehnoloogiafookusega suurorganisatsioonides. Täpsemalt uuritakse, kuidas inimeste, rollide, protsesside, andmete ja tehnoloogiate sidus käsitlemine toetab riskide märkamist, ennetamist ja juhtimist eri organisatsiooniliste funktsioonide vaatenurgast.

Magistritöö põhiküsimus on järgmine: **kuidas on personaliarhitektuuri terviklikkus seotud riskijuhtimise praktikatega Eesti infotehnoloogiafookusega suurorganisatsioonides?**

Sellest lähtuvad uurimisküsimused:

1. Kuidas avaldub personaliarhitektuuri terviklikkus uuritud organisatsioonides ning kuidas kirjeldavad juhid ja võtmeisikud selle rolli organisatsiooni toimimises?
2. Millised tegurid toetavad või takistavad personaliarhitektuuri terviklikkust erinevates organisatsioonilistes rollides ja funktsioonides?
3. Millisel viisil avaldub personaliarhitektuuri terviklikkus riskijuhtimise protsessides, otsustes ja praktikates?
4. Millised juhtumitevahelised mustrid viitavad personaliarhitektuuri terviklikkuse ja riskijuhtimise süsteemsuse seosele?

Kvalitatiivne uurimisstrateegia võimaldab keskenduda sellele, kuidas osalejad nähtust tõlgendavad ning milliste näidete ja kogemuste kaudu nad seoseid põhjendavad.

2.2. Uurimisstrateegia ja uurimisinstrument

Uurimus lähtub kvalitatiivsest uurimisstrateegiast, sest eesmärk on mõista, kuidas personaliarhitektuuri terviklikkus organisatsioonides avaldub ja kuidas see seostub riskijuhtimise praktikatega. Kvalitatiivne lähenemine sobib kontekstisõltuva nähtuse uurimiseks, kuna võimaldab analüüsida osalejate kogemusi, tõlgendusi ja praktilisi näiteid nende organisatsioonilises keskkonnas (Laherand, 2010; Õunapuu, 2014, lk 52–54).

Uurimus põhineb mitme juhtumiga juhtumiuuringul, kus iga organisatsiooni käsitletakse eraldi juhtumina. See võimaldab võrrelda sama nähtuse avaldumist eri organisatsioonilistes kontekstides ning tuvastada juhtumiteüleseid mustreid, erinevusi ja korduvaid riskikohti. Uuringu eesmärk ei ole statistiline üldistus, vaid analüütiline üldistus personaliarhitektuuri terviklikkuse ja riskijuhtimise seoste kohta.

Andmekogumise põhimeetodina kasutati poolstruktureeritud intervjuusid, mis võimaldasid koguda kontekstipõhiseid kirjeldusi ning säilitada samal ajal piisava ühtsuse organisatsioonide ja funktsioonide võrdlemiseks. Intervjuu teemad ja põhiküsimused olid ette valmistatud, kuid küsimuste sõnastust ja järjekorda kohandati vastaja rolli ja kogemuse järgi (Laherand, 2010; Õunapuu, 2014, lk 171–173). Kuna personaliarhitektuuri terviklikkus ei pruugi organisatsioonides

väljenduda ühtse sõnavara kaudu, ei defineeritud mõistet intervjuu alguses kitsalt, vaid vastajatel võimaldati avada teemat oma näidete ja praktikate kaudu.

Intervjuukava koostati teoreetilisest raamistikust tuletatud analüüsimaatriksi alusel. Selle lähtekohaks oli arusaam, et terviklikkus avaldub protsesside, tehnoloogiate ja rollide sidususes ning nende seostes riskijuhtimise praktikatega. Protsesside plokk keskendus personaliprotsesside ülesehitusele ja töötaja elukaarele, tehnoloogiate plokk infosüsteemidele, andmevoogudele, ligipääsudele ja integratsioonidele ning rollide plokk vastutustele, otsustusõigustele ja kontrollidele. Uurimuses kasutatud poolstruktureeritud intervjuu kava on esitatud lisas 1.

Kõik intervjuud transkribeeriti ja anonümiseeriti. Töös kasutatakse organisatsioonide ja vastajate eristamiseks üldistatud tähiseid, näiteks organisatsiooninumbrit ja funktsiooni nimetust. Intervjuude transkriptsioonid on autori valduses ning neid ei esitata töö lisana konfidentsiaalsuse tagamiseks.

2.3. Pilootuuring

Enne põhiuuringut viidi läbi pilootuuring, mille eesmärk oli hinnata intervjuukava arusaadavust, küsimuste järjestust ja sobivust uurimisküsimustele vastamiseks. Pilootuuring aitab kvalitatiivses uurimuses kontrollida, kas andmekogumisvahend võimaldab uuritavat nähtust avada piisava sügavusega ning koguda analüüsi jaoks sisukaid ja võrreldavaid vastuseid (Laherand, 2010, lk 192).

Pilootintervjuud viidi läbi kolme osalejaga, kes esindasid personali-, IT- ning riski- või õigusfunktsiooni. Tulemused näitasid, et intervjuukava üldine loogika toimis, kuid vastajad kaldusid ilma täpsustavate küsimusteta kirjeldama pigem üksikuid protsesse, süsteeme või rolle, mitte nendevahelisi seoseid. Samuti jäi riskijuhtimise käsitlus sageli kontrollide ja tagajärgede tasandile ega toonud esile ennetavat vaadet.

Pilootuuringu põhjal tehti intervjuukavasse neli täpsustust. Esiteks seoti küsimused selgemalt töötaja elukaare etappidega (nt *onboarding*, rollimuutused, *offboarding*). Teiseks lisati küsimusi, mis suunasid kirjeldama protsesside, süsteemide ja rollide seoseid. Kolmandaks tugevdati riskide ennetamise ja süsteemidevaheliste mõjude käsitlemist. Neljandaks lisati standardiseeritud

järelküsimused (nt konkreetsete näidete toomine), et suurendada vastuste võrreldavust (Õunapuu, 2014, lk 172–173).

Pilootuuringu kokkuvõte on esitatud lisas 4. Intervjuukava on toodud lisas 1, koodiraamat lisas 2 ning juhtumite võrdlusmaatriks lisas 3.

2.4. Uuringu läbiviimine, andmekogumine ja valim

Uuring viidi läbi etapiviisiliselt: esmalt koostati intervjuukava teoreetilise raamistiku alusel, seejärel viidi läbi pilootuuring ning selle põhjal täpsustati küsimusi. Seejärel valiti organisatsioonid ja osalejad ning viidi läbi intervjuud.

Uuringus osales kuus Eesti infotehnoloogiafookusega suurorganisatsiooni ning kokku viidi läbi 15 intervjuud. Osalejad esindasid personali-, IT- ning riski- või õigusfunktsiooni. Kolmes organisatsioonis puudus eraldi riskifunktsioon, mistõttu käsitleti seda vaadet personali- või IT-funktsiooni kaudu. Kõik intervjuud viidi läbi eesti keeles, kestsid keskmiselt umbes 40 minutit, salvestati osalejate nõusolekul ning transkribeeriti täismahus.

Valim moodustati sihipäraselt organisatsioonidest, kus digitaliseeritus ja regulatiivne surve on kõrged. Valikukriteeriumid olid järgmised:

- organisatsiooni tegevus sõltub infosüsteemidest ja digitaalsest töökorraldusest;
- vähemalt 250 töötajat Eestis või 1000 Baltikumis;
- personaliprotsessid on seotud infosüsteemide, ligipääsuhalduse ja andmetöötlusega;
- olemas on vähemalt osaliselt formaliseeritud riskijuhtimise või vastavusfunktsiooni loogika;
- esineb HR-, IT- ja riski-/õigusfunktsiooni koostoime.

Valimi eesmärk ei olnud statistiline, vaid analüütiline üldistus. Iga organisatsiooni käsitleti eraldiseisva juhtumina, mida analüüsiti ühtse teoreetilise raamistiku alusel ning võrreldi teiste juhtumitega (Laherand, 2010, lk 74–77; Õunapuu, 2014, lk 84–85).

Selline ülesehitus võimaldas analüüsida personaliarhitektuuri terviklikkuse ja riskijuhtimise seoseid nii juhtumite sees kui ka nende vahel.

2.5. Eetilised kaalutlused ning uurimuse usaldusväärsus ja kvaliteet

Uurimus viidi läbi kooskõlas teaduseetika põhimõtetega. Kõigilt osalejatelt saadi teadlik nõusolek ning neile selgitati uuringu eesmärki, andmete kasutamist, salvestamist ja anonümiseerimist. Osalemine oli vabatahtlik ning vastajatel oli õigus intervjuu igal ajal katkestada.

Anonüümsuse tagamiseks ei avaldata töös osalejate ega organisatsioonide nimesid. Arvestades valimi väiksust, vähendati ka kaudse tuvastamise riski, esitades ainult analüüsi seisukohalt vajalikud tunnused. Kõiki andmeid käsitleti konfidentsiaalselt ja kasutati üksnes käesoleva uurimuse eesmärgil.

Uurimuse usaldusväärsust toetas funktsioonipõhine triangulatsioon, kuna kaasati erinevate valdkondade esindajad (personal, IT, risk/õigus). See võimaldas võrrelda sama organisatsiooni sees erinevaid vaateid ning hinnata nende kooskõla või erinevusi (Laherand, 2010, lk 348–349). Uurimuse kvaliteeti toetas analüüsiraamistiku läbipaistvus. Intervjuukava töötati välja teoreetilise analüüsimaatriksi alusel, seda täpsustati pilootuuringu käigus ning kõigis juhtumites kasutati sama loogikat. Intervjuud salvestati, transkribeeriti ja analüüsiti ühtse kodeerimisraamistiku alusel, mis tagas protsessi jälgitavuse (Laherand, 2010, lk 353–356).

Uurimuse piiranguna tuleb arvestada, et tegemist on kvalitatiivse mitme juhtumiga uuringuga, mille eesmärk ei ole tulemuste statistiline üldistamine kõikidele Eesti suurorganisatsioonidele. Tulemused kirjeldavad uuritud organisatsioonide ja intervjueeritud funktsioonide vaateid ning võimaldavad analüütilist üldistust personaliarhitektuuri terviklikkuse ja riskijuhtimise seoste mõistmiseks.

Uurija refleksiivsust toetas eelnevalt määratletud analüütiliste mõõtmete kasutamine ning funktsioonidevaheline võrdlus nii juhtumite sees kui ka nende vahel. See aitas vältida üksikute hinnangute ületõlgendamist ning siduda järeldused empiirilise materjaliga.

2.6. Andmete analüüsimeetod

Intervjuuandmeid analüüsiti temaatilise sisuanalüüsi abil, mida toetas teooriast tuletatud kodeerimisraamistik. See võimaldas süstematiseerida ja tõlgendada, kuidas eri funktsioonide esindajad kirjeldavad personaliarhitektuuri terviklikkust ning selle seoseid riskijuhtimise

praktikatega. Kvalitatiivses uurimuses hõlmab analüüs andmete liigendamist, kategoriseerimist ja tõlgendamist viisil, mis toob esile nähtuse sisemise loogika (Laherand, 2010, lk 289–293).

Analüüsi aluseks oli teoreetilisest osast tuletatud analüüsimaatriks, mis koondas personaliarhitektuuri terviklikkuse põhikomponendid ja riskijuhtimise indikaatorid. Selle põhjal koostati kodeerimisraamistik, mille abil seoti empiirilised andmed protsesside terviklikkuse, tehnoloogia terviklikkuse, rollide ja vastutuste terviklikkuse ning riskijuhtimise integratsiooni mõõtmetega. Lähenemine vastab suunatud kvalitatiivse sisuanalüüsi loogikale, kus esialgne kodeerimisskeem tugineb teooriale ning täpsustub analüüsi käigus (Laherand, 2010, lk 294).

Andmete analüüs toimus kolmes etapis. Esmalt kodeeriti intervjuuandmed temaatilise sisuanalüüsi abil. Seejärel koostati iga organisatsiooni kohta juhtumiprofiil, milles kirjeldati personaliarhitektuuri terviklikkuse avaldumist ja selle seoseid riskijuhtimise praktikatega. Iga juhtumi puhul analüüsiti protsesside terviklikkust, tehnoloogia terviklikkust ning rollide ja vastutuste terviklikkust ning toodi välja peamised tugevused, lüngad ja kriitilised riskikohad. Pärast esmast kodeerimist kujundati iga juhtumi kohta personaliarhitektuuri terviklikkuse koondhinnang, mis tugines lisas 2 esitatud koodiraamatule ja selle alusel sõnastatud hindamiskriteeriumidele (vt lisa 2, tabel L2.2). Koondhinnangu kujundamisel lähtuti seoste nähtavusest, vastuste süsteemsusest, näidete konkreetsusest, funktsioonidevahelisest kooskõlast ning sellest, kuidas protsesside, tehnoloogia ning rollide ja vastutuste terviklikkus seostus riskijuhtimise praktikatega. Viimases etapis võrreldi juhtumiprofiile omavahel, et tuvastada korduvaid mustreid, erinevusi ja võimalikke seletusmehhanisme.

Analüüsi fookus ei olnud kvantitatiivsel hindamisel, vaid vastuste süsteemsusel, seoste ulatusel ja näidete konkreetsusel. Intervjuuandmeid käsitleti organisatsiooni personaliarhitektuuri terviklikkuse avaldumisena eri funktsioonide vaates. Terviklikkuse taset hinnati selle põhjal, kas organisatsiooni kirjeldati üksikute tegevuste kogumina või omavahel seotud protsesside, rollide, vastutuste ja süsteemide tervikuna.

Juhtumitevaheline võrdlus võimaldas hinnata, millistes aspektides seostub suurem või väiksem terviklikkus riskijuhtimise praktikate süsteemsusega ning millised katkestused korduvad eri organisatsioonides. Analüüs on kooskõlas mitme juhtumiga juhtumiuuringu loogikaga, mille puhul käsitletakse iga juhtumit eraldi ning võrreldakse neid ühise teoreetilise raamistiku alusel (Laherand, 2010, lk 74–77; Õunapuu, 2014, lk 84–85). Tabelis 2 esitatud analüüsimaatriks toimis

nii kodeerimise kui ka tõlgenduse alusena. Selle põhjal koostatud koodiraamat on esitatud lisas 2 ning juhtumite võrdlusmaatriks lisas 3.

Tabel 2. Analüüsimaatriks intervjuuandmete kodeerimiseks ja tõlgendamiseks

Analüüsimõõde	**Analüüsi fookus**	**Mida intervjuudes otsitakse**	**Seos riskijuhtimise praktikatega**
Protsessiline terviklikkus	Personaliprotsesside ülesehituse ja seoste sidusus	Töötaja elukaare kirjeldused, protsesside järjepidevus, üleminekukohad, standardiseeritus, erandite käsitlemine	Riskide tuvastamine protsessilünkades, kontrollimeetmete kavandamine ja seire
Tehnoloogiline terviklikkus	Infosüsteemide, andmevoogude, ligipääsude ja integratsioonide sidusus	Süsteemide roll, töövood, ligipääsude määramine ja tagasivõtmine, tehnoloogilised sõltuvused	Riskide hindamine tehnoloogiliste sõltuvuste vaates, ligipääsukontrollid ja jälgitavus
Rolliline terviklikkus	Rollide, vastutuste ja õiguste jaotuse sidusus	Rollipiirid, vastutusjaotus, otsustusõigused, koostöö HR-i, IT ja riski- või õigusfunktsiooni vahel	Riskide omanikud, vastutuse selgus ja kontrollide rakendamine
Riskijuhtimise integratsioon	Arusaam sellest, kuidas personaliarhitektuuri terviklikkus seostub riskide ennetamise ja juhtimisega	Näited riskide tuvastamisest, hindamisest, ennetusest, seirest ja ülevaatusest	Näitab, kas riskijuhtimine on ennetav, reageeriv, killustunud või süsteemne
Terviklikkuse koondhinnang	Personaliarhitektuuri terviklikkuse üldine aste	Seoste kirjeldamise ulatus, vastuste süsteemsus, näidete konkreetsus, funktsioonidevaheline kooskõla	Võimaldab hinnata, kuidas personaliarhitektuuri terviklikkus toetab või piirab riskijuhtimise praktikaid

Allikas*:* autori koostatud teoreetilise analüüsimaatriksi põhjal.

Kokkuvõttes võimaldas valitud analüüsimeetod siduda intervjuuandmed töö teoreetilise raamistikuga ning liikuda üksikute kirjelduste tõlgendamisest juhtumisisese analüüsi kaudu juhtumitevaheliste mustrite sünteesini.

2.7. Juhtumite lühikirjeldus ja kontekst

Juhtumeid käsitletakse organisatsioonipõhiste tervikutena, kus personaliarhitektuuri terviklikkus avaldub protsesside, tehnoloogiliste lahenduste ja rollijaotuse koosmõjus. Kirjelduste eesmärk on anda analüüsiks vajalik minimaalne kontekst, mitte esitada detailset organisatsioonitutvustust. Anonüümsuse tagamiseks esitatakse juhtumid profiilidena, tuues välja ainult analüüsi seisukohalt olulised tunnused: valdkond, suurus, peamised funktsioonid ning tehnoloogia- ja andmekeskkonna üldine laad.

Kõik juhtumid pärinevad Eesti infotehnoloogiafookusega suurorganisatsioonidest, mille tegevus sõltub infosüsteemidest, digitaalselt vahendatud tööprotsessidest ja rollipõhisest ligipääsuhaldusest. Organisatsioonid esindavad telekommunikatsiooni ja IT-teenuste, tarkvara- ja digiteenuste ning finants- ja kindlustusvaldkonda. Personaliprotsessid toimuvad kõigis juhtumites vähemalt osaliselt digitaalses keskkonnas ning on seotud personaliinfosüsteemi (HRIS, *human resource information system*), ligipääsuhalduse, dokumendihalduse ja süsteemiintegratsioonidega. Juhtumid erinevad formaliseerituse, regulatiivse surve, arhitektuurilise kooskõla ja vastutusloogika selguse poolest. Osa organisatsioone iseloomustab standardi- ja auditipõhine lähenemine, teistes on suurem roll funktsioonidevahelisel koordineerimisel. Need erinevused loovad aluse järgmistes alapeatükkides esitatavate juhtumiprofiilide ja mustrite tõlgendamiseks. Juhtumite detailsem võrdlus on esitatud lisas 3.

2.8. Juhtumianalüüsid

Käesolevas peatükis esitatakse uuringus osalenud organisatsioonide juhtumipõhised analüüsid. Analüüsi eesmärk on näidata, kuidas personaliarhitektuuri terviklikkus avaldub eri organisatsioonides ning kuidas see seostub riskijuhtimise praktikatega konkreetsetes kontekstides. Iga organisatsiooni käsitletakse analüütilise tervikuna, mille puhul vaadeldakse protsesside terviklikkust, tehnoloogia terviklikkust ning rollide ja vastutuste terviklikkust ning nende seoseid riskide tuvastamise, hindamise, ennetamise ja seirega. Analüüs lähtub ühtsest teoreetilisest ja metodoloogilisest raamistikust, mis võimaldab juhtumeid omavahel võrrelda. Juhtumianalüüsides kasutatud koondhinnang tugines lisas 2 esitatud koodiraamatule ja selle põhjal sõnastatud hindamiskriteeriumidele (vt lisa 2, tabel L2.2).

Juhtumianalüüsides hinnatakse, kui süsteemselt on kirjeldatud rollide, protsesside, ligipääsude, andmevoogude ja tehnoloogiliste sõltuvuste vahelisi seoseid ning mil määral on need seotud riskijuhtimise praktikatega. Eraldi tähelepanu pööratakse sellele, kas riskijuhtimine avaldub pigem ennetava või reageeriva lähenemisena ning millised on peamised katkestused või tugevused personaliarhitektuuri terviklikkuse seisukohalt. Samuti võimaldavad vastajate kirjeldused hinnata funktsioonidevahelisi erinevusi sama organisatsiooni sees.

Kõik juhtumid on esitatud ühtse struktuuri alusel. Esmalt käsitletakse personaliarhitektuuri terviklikkuse põhimõõtmeid, seejärel nende seoseid riskijuhtimise praktikatega ning lõpuks esitatakse juhtumi koondprofiil ja peamised riskikohad. Selline ülesehitus loob aluse järgmises peatükis esitatavale juhtumitevahelisele võrdlevale analüüsile.

2.8.1. Organisatsioon 1

Organisatsioon 1 on infotehnoloogiafookusega suurorganisatsioon, kus personaliprotsessid on olulisel määral digitaalselt vahendatud ning seotud ligipääsuhalduse, süsteemiintegratsioonide ja töövoogude automatiseerimisega. Juhtumis olid esindatud personali-, IT- ja riskijuhtimise vaated (Organisatsioon 1: HR-funktsiooni esindaja, 18.02.2026; Organisatsioon 1: IT-funktsiooni esindaja, 20.02.2026; Organisatsioon 1: riskijuhtimise funktsiooni esindaja, 03.03.2026).

Protsesside terviklikkus

Protsesside terviklikkus oli keskmisel tasemel. Põhiloogika on struktureeritud, kuid töötaja elukaare üleminekukohad ei ole kõigis etappides võrdselt riskikindlad. Juhtumile iseloomulikult ei seostunud riskid mitte süsteemide tehnilise nõrkusega, vaid inimtegevusest sõltuvate sammudega, mida ilmestab personaliesindaja tähelepanek: „Seal, kus tuleb sisse inimene ehk siis süsteemid, IT-süsteemid on ikkagi suhteliselt riskikindlad, aga niipea, kui tuleb sisse inimese käsi, siis seal võib olla risk“ (Organisatsioon 1: HR-funktsiooni esindaja, 18.02.2026). IT- ja riskivaates tõusid peamiste katkestuskohtadena esile rollimuutused, *offboarding* ja ligipääsude ajakohastamine; protsesside arendamine on pigem reageeriv (Organisatsioon 1: IT-funktsiooni esindaja, 20.02.2026; Organisatsioon 1: riskijuhtimise funktsiooni esindaja, 03.03.2026).

Tehnoloogia terviklikkus

Tehnoloogia terviklikkus oli keskmisel tasemel, kuid funktsiooniti ebaühtlane. IT-funktsioonil oli süsteemsem ülevaade autentimisest, ühekordsest sisselogimisest (*single sign-on*, SSO) ja auditiloogikast, kuid rõhutati ka varjatud tööriistade ja väliskeskkondade riski (Organisatsioon 1:

IT-funktsiooni esindaja, 20.02.2026). Personalifunktsioon kirjeldas keskkonda killustununa (Organisatsioon 1: HR-funktsiooni esindaja, 18.02.2026), riskivaates lisandusid ligipääsude äravõtmise ebaühtlus ja puudulik nähtavus andmete paiknemise üle (Organisatsioon 1: riskijuhtimise funktsiooni esindaja, 03.03.2026).

Rollide ja vastutuste terviklikkus

Vajaduspõhine ligipääsuloogika on põhimõtteliselt olemas, kuid rollide kriitilisus, vastutuse piirid ja õiguste ajakohastamine ei ole täielikult formaliseeritud. IT-funktsioon tõi esile sõltuvuse õigeaegsest teavitamisest rollimuutuste korral (Organisatsioon 1: IT-funktsiooni esindaja, 20.02.2026), riskifunktsioon aga märkis, et kriitilisi rolle eristatakse praktikas, kuid mitte formaalselt (Organisatsioon 1: riskijuhtimise funktsiooni esindaja, 03.03.2026).

Riskijuhtimise integratsioon

Riskijuhtimise integratsioon oli osaline ja pigem reageeriv. IT-vaates seostus riskijuhtimine tehnoloogiliste kontrollidega (MFA, SSO, auditid), personalivaates protsesside järjepidevuse ja töökorralduslike katkestustega (Organisatsioon 1: IT-funktsiooni esindaja, 20.02.2026; Organisatsioon 1: HR-funktsiooni esindaja, 18.02.2026). Riskifunktsioon rõhutas, et protsesse täiustatakse sageli alles siis, kui risk on juba nähtavaks muutunud (Organisatsioon 1: riskijuhtimise funktsiooni esindaja, 03.03.2026).

Tabel 3. Organisatsioon 1 küpsusprofiil

Mõõde	**Hinnang**	**Lühiselgitus**
Protsesside terviklikkus	keskmine	Põhiprotsessid on struktureeritud, kuid üleminekukohad sõltuvad osaliselt inimestest ja reaktiivsest parandamisest.
Tehnoloogia terviklikkus	keskmine	Kontrollid ja töövood on olemas, kuid ligipääsude elukaar, andmete paiknemine ja tööriistade hajumine tekitavad lünki.
Rollide ja vastutuste terviklikkus	keskmine	Rollide ja õiguste põhimõtted on olemas, kuid kriitiliste rollide ja vastutuse loogika ei ole täielikult formaliseeritud.

Riskijuhtimise integratsioon	osaline, pigem reageeriv	Riskijuhtimine on nähtav kontrollides ja vastavuses, kuid vähem protsesside ennetavas kujundamises.

Allikas: autori koostatud Organisatsioon 1 intervjuude põhjal (Organisatsioon 1: HR-funktsiooni esindaja, 18.02.2026; Organisatsioon 1: IT-funktsiooni esindaja, 20.02.2026; Organisatsioon 1: riskijuhtimise funktsiooni esindaja, 03.03.2026).

Organisatsiooni 1 iseloomustab osaliselt süsteemne, kuid ebaühtlane personaliarhitektuuri terviklikkus. Tugevuseks on põhiprotsesside formaliseerimine ja tehnoloogiliste kontrollide olemasolu (Organisatsioon 1: IT- ja riskifunktsiooni esindajad, veebruar–märts 2026).

Nõrgemaks jääb rollide, ligipääsude, andmete ja protsesside sidusus töötaja elukaare lõikes. Peamised riskikohad on seotud *offboarding'u*, rollimuutuste, teadmuse kadumise ja andmete hajumisega. Riskijuhtimine on seetõttu pigem reageeriv kui ennetav.

2.8.2. Organisatsioon 2

Organisatsioon 2 on infotehnoloogiafookusega suurorganisatsioon, mille personaliprotsessid on seotud infosüsteemide, ligipääsuhalduse ja andmevoogudega. Töötaja elukaare etapid on vähemalt osaliselt kaardistatud, kuid tervikloogika ei ole veel täielikult ühtlustatud (Organisatsioon 2: HR-funktsiooni esindaja, 16.02.2026; Organisatsioon 2: IT ja riskijuhtimise funktsiooni esindaja, 16.02.2026). Juhtumi eripäraks on ühendatud IT- ja riskijuhtimise vaade, mistõttu tehnoloogiline ja riskiloogika olid tihedalt põimunud.

Protsesside terviklikkus

Töötaja elukaare etappe mõistetakse osaliselt omavahel seotud protsessina. IT- ja riskivaates rõhutati, et *onboarding*, rollimuutused ja *offboarding* moodustavad seotud protsessirea, mille toimimine sõltub struktureeritud lähteandmetest (Organisatsioon 2: IT ja riskijuhtimise funktsiooni esindaja, 16.02.2026). Personali vaates kirjeldati elukaart pigem alles ühtlustamisel olevate osadena (Organisatsioon 2: HR-funktsiooni esindaja, 16.02.2026).

Tehnoloogia terviklikkus

IT- ja riskivaade kirjeldas tehnoloogilist loogikat süsteemsemalt, rõhutades, et killustatus suurendab käsitöö mahtu ja andmekvaliteedi riske (Organisatsioon 2: IT ja riskijuhtimise funktsiooni esindaja, 16.02.2026). Personalifunktsioon tõi esile paralleelsed süsteemid ja

dubleeritud andmesisestuse ning ebaselguse selles, milline andmestik on õige (Organisatsioon 2: HR-funktsiooni esindaja, 16.02.2026).

Rollide ja vastutuste terviklikkus

Personalifunktsioon rõhutas, et kriitilised rollid eksisteerivad pigem juhitasandi teadmisena kui formaliseeritud süsteemina (Organisatsioon 2: HR-funktsiooni esindaja, 16.02.2026). IT- ja riskivaates seostusid rollid eelkõige ligipääsudega: teatud rollidele rakendatakse tugevamaid kontrolle, kuid vastutuspiirid ei ole alati üheselt selged (Organisatsioon 2: IT ja riskijuhtimise funktsiooni esindaja, 16.02.2026).

Riskijuhtimise integratsioon

ISO-põhine raamistik ja regulaarne riskide ülevaatamine on olemas, kuid riskianalüüsi kvaliteet sõltub suurel määral sellest, kes riske hindab (Organisatsioon 2: IT ja riskijuhtimise funktsiooni esindaja, 16.02.2026). Personalifunktsioon seostas riskid andmekaitse ja andmekvaliteedi ning elukaare üleminekukohtadega (Organisatsioon 2: HR-funktsiooni esindaja, 16.02.2026).

Tabel 4. Organisatsioon 2 küpsusprofiil

Mõõde	**Hinnang**	**Lühiselgitus**
Protsesside terviklikkus	keskmine	Põhiprotsessid on olemas ja osaliselt seotud, kuid töötaja elukaare tervik ei ole veel täielikult ühtlustatud.
Tehnoloogia terviklikkus	keskmine	Süsteemide ja riskide seoseid mõistetakse, kuid tehnoloogiline tervikpilt on funktsiooniti ebaühtlane.
Rollide ja vastutuste terviklikkus	keskmine	Kriitilised rollid on osaliselt teadvustatud, kuid vastutuse, asendatavuse ja kriitilisuse loogika ei ole täielikult formaliseeritud.
Riskijuhtimise integratsioon	keskmine	Riskid on nähtavad ja neid hinnatakse, kuid käsitlus sõltub endiselt kogemusest ega ole veel täielikult orgaaniline osa igapäevasest juhtimisest.

Allikas: autori koostatud Organisatsioon 2 intervjuude põhjal (Organisatsioon 2: HR-funktsiooni esindaja, 16.02.2026; Organisatsioon 2: IT ja riskijuhtimise funktsiooni esindaja, 16.02.2026).

Organisatsiooni 2 iseloomustab keskmine ja arenev personaliarhitektuuri terviklikkus. Tugevuseks on protsessiliste ja tehnoloogiliste riskikohtade hea nähtavus, eriti elukaare üleminekutes,

andmevoogudes ja ligipääsuhalduses (Organisatsioon 2: HR- ning IT- ja riskifunktsiooni esindajad, veebruar 2026).

Nõrgemaks jääb rollikriitilisuse, vastutuspiiride ja tehnoloogilise tervikpildi formaliseeritus. Riskijuhtimine on olemas, kuid selle seos personaliarhitektuuri tervikloogikaga on veel osaliselt killustunud.

2.8.3. Organisatsioon 3

Organisatsioon 3 on infotehnoloogiafookusega suurorganisatsioon, kus personaliprotsesside administratiivne baas on olemas, kuid protsesside, tehnoloogia ning rollide ja vastutuste tervikloogika ei ole veel täielikult ühtlustatud ega läbipaistvalt juhitud (Organisatsioon 3: HR-funktsiooni esindaja, 13.02.2026; Organisatsioon 3: IT ja riskijuhtimise funktsiooni esindaja, 12.02.2026). Juhtumi eripäraks on detsentraliseeritud riskivastutus – eraldi riskifunktsioon puudub.

Protsesside terviklikkus

Personali vaates kirjeldati personaliprotsesside administratiivset baasi toimivana: põhilised hügieeniprotsessid on olemas, kuid strateegilisem osa toimib *ad hoc* loogikaga (Organisatsioon 3: HR-funktsiooni esindaja, 13.02.2026). IT- ja riskivaade oli kriitilisem, rõhutades, et protsessid on pigem ajas kujunenud lahenduste kogum kui teadlikult kujundatud süsteem; eriti haavatavad on elukaare üleminekukohad (Organisatsioon 3: IT ja riskijuhtimise funktsiooni esindaja, 12.02.2026).

Tehnoloogia terviklikkus

Ligipääsude loogika on suures osas individuaalne, mitte rolli- ja riskipõhine; vananenud personaliinfosüsteem nõrgestab aruandlust ja suurendab valeandmete riski (Organisatsioon 3: HR-funktsiooni esindaja, 13.02.2026; Organisatsioon 3: IT ja riskijuhtimise funktsiooni esindaja, 12.02.2026).

Rollide ja vastutuste terviklikkus

Kriitilisi rolle tunnetatakse praktikas, kuid neid ei eristata ametlikult riskimõju alusel – kriitilisus seostub sageli konkreetse inimesega, mitte ametikohaga. Samuti ilmnes sõltuvus raskesti asendatavate inimeste teadmistest vanades süsteemides (Organisatsioon 3: HR-funktsiooni esindaja, 13.02.2026; Organisatsioon 3: IT ja riskijuhtimise funktsiooni esindaja, 12.02.2026).

Riskijuhtimise integratsioon

Iga valdkond vastutab oma riskide eest iseseisvalt; riskid muutuvad nähtavaks ESG aruandluse, finantsauditi leidude ja kaudsete indikaatorite kaudu, kuid personalifunktsioonil puuduvad selged mõõdikud oma riskiprofiili järjepidevaks jälgimiseks (Organisatsioon 3: HR-funktsiooni esindaja, 13.02.2026; Organisatsioon 3: IT ja riskijuhtimise funktsiooni esindaja, 12.02.2026).

Tabel 5. Organisatsioon 3 küpsusprofiil

Mõõde	**Hinnang**	**Lühiselgitus**
Protsesside terviklikkus	keskmine	Põhiprotsessid on olemas, kuid elukaare tervik ja üleminekukohad ei ole veel läbivalt standardiseeritud.
Tehnoloogia terviklikkus	keskmine	Süsteemide ja ligipääsude kriitilisust mõistetakse, kuid tehnoloogiline tervikpilt on killustunud ja ebaühtlaselt juhitud.
Rollide ja vastutuste terviklikkus	keskmine	Kriitilised rollid on tajutud, kuid nende strateegiline väärtus, vastutus ja asendatavus ei ole täielikult formaliseeritud.
Riskijuhtimise integratsioon	keskmine, hajutatud	Riskid on nähtavad, kuid nende juhtimine on funktsioonipõhine ega ole veel täielikult seotud personaliarhitektuuri ennetava kujundamisega.

Allikas: autori koostatud Organisatsioon 3 intervjuude põhjal (Organisatsioon 3: IT ja riskijuhtimise funktsiooni esindaja, 12.02.2026; Organisatsioon 3: HR-funktsiooni esindaja, 13.02.2026).

Organisatsiooni 3 iseloomustab keskmine, kuid ebaühtlaselt rakenduv personaliarhitektuuri terviklikkus. Tugevuseks on administratiivne baas ja riskide osaline teadvustamine, kuid protsesside, süsteemide ning rollide ja vastutuste seosed ei ole läbivalt seotud ega järjepidevalt juhitud (Organisatsioon 3: HR- ning IT- ja riskifunktsiooni esindajad, veebruar 2026).

Peamised riskikohad on seotud elukaare üleminekute, süsteemide killustatuse, võtmeisikupõhise toimeloogika ja hajutatud vastutusega. Riskijuhtimine on seetõttu pigem hajutatud kui ennetav.

2.8.4. Organisatsioon 4

Organisatsioon 4 on infotehnoloogiafookusega suurorganisatsioon, mille personaliprotsessid on tihedalt seotud ligipääsuhalduse, rollimuutuste ja mitmekesise süsteemimaastikuga. Organisatsioonis mõistetakse, et töötajate liikumine, rollid, õigused ja süsteemide ülesehitus mõjutavad otseselt riskide kujunemist, kuid see ei ole kõikjal kujunenud ennetavalt juhitud

praktikaks (Organisatsioon 4: HR-funktsiooni esindaja, 18.02.2026; Organisatsioon 4: IT ja riskijuhtimise funktsiooni esindaja, 09.03.2026).

Protsesside terviklikkus

Töötaja elukaare riskitundlikke hetki mõistetakse hästi, kuid protsesside olemasolu ei taga veel nende terviklikku toimimist. Eriti sisemiste rollimuutuste korral võivad vanad ligipääsud jääda alles ja uued lisanduda ilma süsteemse ülevaatuseta; aastane sisekontroll viitab pigem järelhindamisele kui ennetavale disainile (Organisatsioon 4: IT ja riskijuhtimise funktsiooni esindaja, 09.03.2026).

Tehnoloogia terviklikkus

Tehnoloogia terviklikkus kujunes selle juhtumi tugevaimaks mõõtmeks. IT- ja riskivaates mõistetakse selgelt, et *legacy*-lahendused ja ebaühtlane ligipääsuloogika ei ole pelgalt IT-korralduse küsimused, vaid mõjutavad otseselt personaliprotsessidest tulenevaid riske. Olukordi kirjeldas üks vastaja järgnevalt: „Kõik süsteemid ei ole SSO all, kõik õigused ei jookse läbi ühe keskse loogika ja osa ligipääse on ajalooliselt tekkinud üsna käsitööna. See tähendab, et sul võib põhimõtteliselt olla paberil üsna korralik protsess, aga praktikas on sul mitu erandit... ja siis sa avastad, et tegelik olukord on palju kirjum kui protsessijoonis näitab“ (Organisatsioon 4: IT ja riskijuhtimise funktsiooni esindaja, 09.03.2026). Sama vastaja rõhutas, et piiratud nähtavus muudab keeruliseks kontrollida, kas õiged inimesed omavad õigel ajal vajalikke õigusi ning kas mittevajalikud õigused on eemaldatud (Organisatsioon 4: IT ja riskijuhtimise funktsiooni esindaja, 09.03.2026).

Rollide ja vastutuste terviklikkus

Rollide ja vastutuste seost mõistetakse sisuliselt hästi. IT- ja riskivaates rõhutati, et peamine probleem ei seisne teadmiste puudumises, vaid rollide hägususes: vastutuspiirid peavad olema selged (Organisatsioon 4: IT ja riskijuhtimise funktsiooni esindaja, 09.03.2026). Personalifunktsiooni vaade kinnitas, et vastutusjaotus ei ole kõigis olukordades veel üheselt standardiseeritud (Organisatsioon 4: HR-funktsiooni esindaja, 18.02.2026).

Riskijuhtimise integratsioon

Riskid on nähtavad ja funktsioonidevaheline koostöö on olemas, kuid riskide ennetav sissekujundamine protsessidesse ja rollidesse ei ole veel küps. Üks vastaja sõnastas selle selgelt: „Me suudame päris hästi probleeme lahendada, aga me ei jõua alati piisavalt hästi neid ette

modelleerida... Reaktiivne organisatsioon ei pruugi olla halb organisatsioon, aga ta kulutab rohkem energiat tagajärgede korrigeerimisele kui algse disaini tugevdamisele“ (Organisatsioon 4: IT ja riskijuhtimise funktsiooni esindaja, 09.03.2026).

Tabel 6. Organisatsioon 4 küpsusprofiil

Mõõde	**Hinnang**	**Lühiselgitus**
Protsesside terviklikkus	keskmine	Elukaare kriitilisi protsesse mõistetakse, kuid muutusolukordades ei rakendu need veel ühtlaselt ja ennetavalt.
Tehnoloogia terviklikkus	kõrge	Süsteemide killustatust, *legacy*-lahendusi ja ligipääsude arhitektuurseid riske mõistetakse selgelt.
Rollide ja vastutuste terviklikkus	keskmine, kaldub pigem kõrge poole	Rollide ja vastutuste tähtsust mõistetakse hästi, kuid vastutuspiirid ei ole kõigis olukordades veel piisavalt selged.
Riskijuhtimise integratsioon	osaline	Riskid on nähtavad ja seotud kontrollimehhanismidega, kuid nende ennetav kujundamine protsessidesse ja rollidesse on veel ebaühtlane.

Allikas: autori koostatud Organisatsioon 4 intervjuude põhjal (Organisatsioon 4: HR-funktsiooni esindaja, 18.02.2026; Organisatsioon 4: IT ja riskijuhtimise funktsiooni esindaja, 09.03.2026).

Organisatsiooni 4 iseloomustab tugev tehnoloogiline terviklikkus ning mõõdukam protsesside ning rollide ja vastutuste sidusus, mis ei ole veel läbivalt ennetav. Tugevuseks on selge arusaam, et risk tekib inimese, protsessi ja tehnoloogia kokkupuutepunktis, eriti ligipääsude, *legacy*-süsteemide ja rollimuutuste puhul (Organisatsioon 4: HR-, IT- ja riskifunktsiooni esindajad, veebruar–märts 2026).

Peamised riskikohad on seotud rollimuutuste, SSO-väliste süsteemide, vastutuspiiride hägususe ja teadlikkuse ebaühtlusega. Arenguvajadus seisneb selle arusaama muutmises järjepidevaks ja ennetavaks juhtimispraktikaks.

2.8.5. Organisatsioon 5

Organisatsioon 5 on infotehnoloogiafookusega suurorganisatsioon, mille personaliprotsessid on tihedalt seotud infosüsteemide, ligipääsuhalduse, andmekaitse ning üleorganisatsioonilise riskijuhtimisega. Töötaja elukaare protsessid, kriitilised rollid ja nendega seotud riskid on

teadlikult kujundatud ning seotud nii kvaliteedijuhtimise kui ka juhtimistasandi vastutusega (Organisatsioon 5: HR-funktsiooni esindaja, 26.02.2026; Organisatsioon 5: IT-funktsiooni esindaja, 20.02.2026; Organisatsioon 5: riskijuhtimise funktsiooni esindaja, 16.02.2026). Kõigi kuue juhtumi võrdluses esindab Organisatsioon 5 kõrgeima küpsusega juhtumit.

Protsesside terviklikkus

Töötaja elukaart käsitletakse tervikuna alates värbamisest kuni lahkumiseni; protsessid on seotud äristrateegiaga ning toetatud regulaarse funktsioonivahelise infovahetusega (Organisatsioon 5: HR-funktsiooni esindaja, 26.02.2026). Riskivaates on suurimad riskid teadlikult kaardistatud ning paiknevad elukaare üleminekukohtades, kus ühe protsessi väljundist saab teise protsessi sisend – need on kontrollide all (Organisatsioon 5: riskijuhtimise funktsiooni esindaja, 16.02.2026).

Tehnoloogia terviklikkus

Personalifunktsioon kirjeldas tehnoloogiat tugeva toetava komponendina, tunnistades samas selle riske (Organisatsioon 5: HR-funktsiooni esindaja, 26.02.2026). IT-vaates rõhutati rollipõhiste õiguste tähtsust ning riske, mis tekivad vigasest andmesisestusest või partnerite ligipääsude ebapiisavast läbipaistvusest (Organisatsioon 5: IT-funktsiooni esindaja, 20.02.2026). Riskivaates seostus tehnoloogia terviklikkus protsesside läbipaistvuse ning liikumisega tabelipõhisest haldusest süsteemsema lahenduse suunas (Organisatsioon 5: riskijuhtimise funktsiooni esindaja, 16.02.2026).

Rollide ja vastutuste terviklikkus

Kriitilisi ametikohti, rolle ja tegevusi hinnatakse regulaarselt; ligipääsud lähtuvad rollist, mitte isikust (Organisatsioon 5: HR-funktsiooni esindaja, 26.02.2026). Võtmeisikud on eraldi kategoriseeritud, sealhulgas elutähtsa teenuse vaates, ning indiviidisõltuvuse vähendamisega tegeldakse teadlikult (Organisatsioon 5: riskijuhtimise funktsiooni esindaja, 16.02.2026). Kõrgema riskiga rollidele rakendatakse rangemaid kontrolle (Organisatsioon 5: IT-funktsiooni esindaja, 20.02.2026).

Riskijuhtimise integratsioon

Organisatsioonis on üleettevõtteline protsessijuhtimise vaade, ISO 9001 sertifikaat ning regulaarne riskide ülevaatamine, kus kõrgema taseme riskid on seotud juhatuse vastutusega (Organisatsioon 5: riskijuhtimise funktsiooni esindaja, 16.02.2026). Personaliarhitektuur on osa äristrateegiast ning riskide ennetamine toimub protsesside, kommunikatsiooni, rollihindamise ja tehnoloogiliste

muudatuste kaudu (Organisatsioon 5: HR-funktsiooni esindaja, 26.02.2026). IT-funktsiooni hinnang, et riskiteadlikkus võiks personalipoolel mõnes küsimuses tugevam olla, viitab pigem küpsele enesehindamisele kui süsteemi nõrkusele (Organisatsioon 5: IT-funktsiooni esindaja, 20.02.2026).

Tabel 7. Organisatsioon 5 küpsusprofiil

Mõõde	**Hinnang**	**Lühiselgitus**
Protsesside terviklikkus	kõrge	Töötaja elukaart käsitletakse tervikuna ning protsesside üleminekukohad on teadlikult jälgitavad.
Tehnoloogia terviklikkus	keskmisest kõrgem kuni kõrge	Tehnoloogia rolli ja selle riskiseoseid mõistetakse hästi, eriti automatiseerituse, andmekaitse ja partneririskide vaates.
Rollide ja vastutuste terviklikkus	kõrge	Kriitilised rollid, ligipääsud, asendatavus ja vastutused on regulaarse hindamise objekt.
Riskijuhtimise integratsioon	kõrge	Riskid on seotud protsesside, rollide, kvaliteedijuhtimise ja juhtimistasandi vastutusega ning neid käsitletakse suurel määral ennetavalt.

Allikas: autori koostatud Organisatsioon 5 intervjuude põhjal (Organisatsioon 5: riskijuhtimise funktsiooni esindaja, 16.02.2026; Organisatsioon 5: IT-funktsiooni esindaja, 20.02.2026; Organisatsioon 5: HR-funktsiooni esindaja, 26.02.2026).

Organisatsiooni 5 iseloomustab kõrge personaliarhitektuuri terviklikkus ning tugev seos riskijuhtimise praktikatega. Tugevusteks on töötaja elukaare tervikvaade, kriitiliste rollide regulaarne hindamine, rollipõhine ligipääsuhaldus ning riskide sidumine protsessi- ja juhtimisloogikaga (Organisatsioon 5: HR-, IT- ja riskifunktsiooni esindajad, veebruar 2026).

Peamised riskikohad tulenevad keerukamatest sõltuvustest, nagu protsessiüleminekud, käsitsi tegevused, automatiseeritud õigused, partneririskid ja funktsioonidevahelise teadlikkuse ebaühtlus. Seetõttu on tegemist kõrge küpsusega juhtumiga, kus arengufookus on keerukamate riskide ja sõltuvuste juhtimisel.

2.8.6. Organisatsioon 6

Organisatsioon 6 on infotehnoloogiafookusega suurorganisatsioon, kus personaliprotsessid on tihedalt seotud süsteemide, ligipääsude, partnerite ja töövoogude koostoimega. Organisatsioonis

on olemas arusaam töötaja elukaarest, rollidest ja tehnoloogilistest sõltuvustest, kuid personaliarhitektuuri tervik ei ole veel kõigis mõõtmetes ühtlaselt välja kujunenud (Organisatsioon 6: HR-funktsiooni esindaja, 17.03.2026; Organisatsioon 6: IT-funktsiooni esindaja, 18.03.2026; Organisatsioon 6: riskijuhtimise funktsiooni esindaja, 18.03.2026). Juhtumile on iseloomulik tugev riskikohtade äratundmisvõime, mis ei ole veel kujunenud süsteemseks ennetavaks juhtimiseks.

Protsesside terviklikkus

Protsesside terviklikkus oli keskmine, kaldudes keskmisest kõrgema poole. Personalifunktsiooni vaates kirjeldati töötaja elukaart tervikuna, kuid protsessid ei ole alati töötajatele ja juhtidele piisavalt selgelt koondatud ning dokumentatsioon on hajus (Organisatsioon 6: HR-funktsiooni esindaja, 17.03.2026). IT-vaates sõnastas üks esindaja protsesside kriitilised nõuded selgelt: „Just need kohad on kriitilised, sest seal ei piisa sellest, et iga funktsioon teeb oma osa. Seal on vaja, et info liiguks õigeaegselt, piisava detailsusega ja et keegi vaataks tervikut“ – viidates *onboarding'u*, rollivahetuste, ajutiste asenduste ja *offboarding'u* üleminekukohtadele (Organisatsioon 6: IT-funktsiooni esindaja, 18.03.2026). Riskivaates kinnitati, et risk tekib eelkõige siis, kui personaliosakond, IT, juhid ja riskifunktsioon käsitlevad sama olukorda erineva loogika alusel (Organisatsioon 6: riskijuhtimise funktsiooni esindaja, 18.03.2026).

Tehnoloogia terviklikkus

Kõik kolm funktsiooni nägid selgelt süsteemide ja andmevoogude rolli riskide kujunemisel, kuid samal ajal ilmnes märkimisväärne killustatus. Personalifunktsioon kirjeldas mitut süsteemi ja vahekihti, mis ei ole omavahel täielikult ühendatud (Organisatsioon 6: HR-funktsiooni esindaja, 17.03.2026). IT-vaates on suurimad riskid seotud hägusate ligipääsuloogikatega ja partnerite kaudu hallatavate õigustega (Organisatsioon 6: IT-funktsiooni esindaja, 18.03.2026). Riskifunktsioon tõi esile ohu, et kontrollikeskkonda peetakse tugevamaks, kui see tegelikult on (Organisatsioon 6: riskijuhtimise funktsiooni esindaja, 18.03.2026).

Rollide ja vastutuste terviklikkus

Sisuline arusaam rollide, otsustusõiguse, asendatavuse ja sõltuvuste koosmõjust on tugev kõigis kolmes funktsioonis (Organisatsioon 6: HR-funktsiooni esindaja, 17.03.2026; Organisatsioon 6: IT-funktsiooni esindaja, 18.03.2026; Organisatsioon 6: riskijuhtimise funktsiooni esindaja, 18.03.2026). IT-funktsioon tõi esile olukorra, kus kriitiline teadmine ja praktilised kontrolliõigused

võivad koonduda liiga kitsalt ühe inimese kätte. Formaliseeritus ja laiapõhjaline rakendumine ei ole veel kõikjal küpsed.

Riskijuhtimise integratsioon

Riskifunktsiooni vaates käsitletakse riskiteemat kõige tõsisemalt siis, kui midagi on juba juhtunud (Organisatsioon 6: riskijuhtimise funktsiooni esindaja, 18.03.2026). IT-vaates muutuvad riskid nähtavaks eelkõige auditite, ümberkorralduste ja võtmerollidest lahkumiste käigus (Organisatsioon 6: IT-funktsiooni esindaja, 18.03.2026). Personalifunktsioon seostas riskid andmekaitse ja teadlikkuse ebaühtlusega, märkides, et probleemid jõuavad personaliosakonda sageli alles pärast nende avaldumist (Organisatsioon 6: HR-funktsiooni esindaja, 17.03.2026).

Tabel 8. Organisatsioon 6 küpsusprofiil

Mõõde	**Hinnang**	**Lühiselgitus**
Protsesside terviklikkus	keskmine, kaldub pigem keskmisest kõrgema poole	Töötaja elukaare põhiprotsessid on olemas ja üleminekukohad on teadvustatud, kuid dokumentatsioon ja rakendumine on veel ebaühtlased.
Tehnoloogia terviklikkus	keskmine	Süsteemide, ligipääsude ja andmevoogude riskiseoseid mõistetakse, kuid tehnoloogiline tervikpilt on killustunud ja osaliselt partnerisõltuv.
Rollide ja vastutuste terviklikkus	keskmine	Rollide, vastutuste ja kriitilise teadmuse tähendus on sisuliselt hästi mõistetud, kuid formaliseeritus ja asendatavus ei ole veel kõikjal piisavalt küpsed.
Riskijuhtimise integratsioon	keskmine	Riskid on nähtavad ja ennetuse vajadust mõistetakse, kuid käsitlus sõltub endiselt palju funktsioonide koostööst ja üksikute inimeste tähelepanelikkusest.

Allikas: autori koostatud Organisatsioon 6 intervjuude põhjal (Organisatsioon 6: HR-funktsiooni esindaja, 17.03.2026; Organisatsioon 6: IT-funktsiooni esindaja, 18.03.2026; Organisatsioon 6: riskijuhtimise funktsiooni esindaja, 18.03.2026).

Organisatsiooni 6 iseloomustab keskmine personaliarhitektuuri terviklikkus: põhielemendid on olemas ja teadvustatud, kuid nende seotus ei ole veel läbivalt standardiseeritud ega juhitud. Tugevusena oskavad HR-, IT- ja riskifunktsioon selgelt kirjeldada riskikohti, mis koonduvad eelkõige üleminekukohtadesse, ligipääsudesse, süsteemide ja partnerite sõltuvustesse ning

võtmeisikute teadmuse koondumisse (Organisatsioon 6: HR-, IT- ja riskifunktsiooni esindajad, märts 2026).

Peamised lüngad on seotud protsesside killustatuse, süsteemimaastiku keerukuse, partnerisõltuvuse ning vastutuse hajumisega muutusolukordades. Arenguvajadus seisneb olemasoleva arusaama muutmises ühtlasemaks ja ennetavamaks ning selle sidumises igapäevase juhtimispraktikaga.

2.9. Juhtumite võrdlev analüüs

Pärast juhtumipõhist analüüsi viidi läbi juhtumitevaheline võrdlus, et tuvastada korduvaid mustreid ja erinevusi kuue organisatsiooni lõikes. Võrdlus tugines samale analüüsiraamistikule nagu üksikjuhtumite analüüs: protsesside terviklikkus, tehnoloogia terviklikkus, rollide ja vastutuste terviklikkus ning riskijuhtimise integratsioon. Koondhinnangu loogika on esitatud lisas 2 tabelis L2.2 ning juhtumite võrdlusmaatriks lisas 3.

Võrdlus näitas, et personaliarhitektuuri terviklikkus ja riskijuhtimise praktikad on kõigis juhtumites seotud, kuid seose tugevus varieerub. Kõige süsteemsemalt avaldus see Organisatsioonis 5, kus protsessid, rollid, tehnoloogia ja riskijuhtimine moodustasid ühtse juhtimisloogika. Teistes organisatsioonides olid põhielemendid olemas ja osaliselt seotud, kuid nende seotus ei olnud veel läbivalt standardiseeritud ega juhitud.

Juhtumite võrdlusest joonistus välja kolm korduvat mustrit. Esiteks koonduvad riskid töötaja elukaare üleminekukohtadesse, nagu onboarding, rollimuutused ja offboarding. Teiseks seostub riskijuhtimise süsteemsus eelkõige sellega, kui sidusalt on seotud protsessid, rollid ja tehnoloogia, mitte üksikute kontrollimeetmete olemasoluga. Kolmandaks eristab organisatsioone rollide ja vastutuste selgus, eriti kriitiliste rollide ja ligipääsude formaliseeritus. Juhtumite koondprofiil on esitatud tabelis 9.

Tabel 9. Juhtumite koondprofiil

Organisatsioon	**Terviklikkus**	**Tugevus**	**Peamine risk**	**Riskijuhtimise tüüp**
1	madal–keskmine	protsessid	elukaare katkestused	reageeriv
2	keskmine	riskinähtavus	rolli/tehnoloogia sidusus	osaliselt integreeritud
3	keskmine (ebaühtlane)	baas olemas	killustatus	hajutatud
4	tehnoloogiliselt tugev	riskimõistmine	rolli/protsessi lüngad	osaliselt ennetav
5	kõrge	tervikloogika	keerukad sõltuvused	ennetav
6	keskmine	riskide sõnastamine	juhtimisloogika puudujäägid	arenev

Allikas: autori koostatud juhtumianalüüside ja juhtumite võrdluse põhjal.

Tabel 9 näitab kokkuvõtlikult, et juhtumid erinevad eelkõige selle poolest, kui terviklikult on protsessid, rollid ja tehnoloogia seotud riskijuhtimise praktikatega. Detailsem mustrite tõlgendus ja nende seos teoreetilise raamistikuga on esitatud järgmises peatükis.

3. JUHTUMITE ARUTELU JA JÄRELDUSED

Empiiriline analüüs näitas, et personaliarhitektuuri terviklikkus ja riskijuhtimise praktikad on Eesti infotehnoloogiafookusega suurorganisatsioonides selgelt seotud, kuid seose tugevus ja süsteemsus erinevad juhtumiti. Määravaks ei osutunud üksikute kontrollimeetmete olemasolu, vaid see, kui sidusalt on omavahel seotud protsessid, tehnoloogia ning rollid ja vastutused. Erinevus ei seisne niivõrd riskide märkamises, vaid selles, kas riskikaalutlused on osa ühtsest toimimisloogikast või jäävad funktsiooniti killustunuks.

See tulemus on kooskõlas strateegilise personalijuhtimise käsitlustega, mille järgi personaliarhitektuur ei ole üksikute praktikate kogum, vaid loogika, mille kaudu kujundatakse rollid ja töösuhted kooskõlas organisatsiooni põhitegevusega (Lepak & Snell, 1999, lk 31–42; Becker & Huselid, 2006, lk 903–905). Empiiriline analüüs näitas, et seal, kus rollid, ligipääsud ja vastutused olid selgelt diferentseeritud ja formaliseeritud, oli ka riskijuhtimine süsteemsem. Kõige selgemalt avaldus see Organisatsioonis 5, kus personaliarhitektuuri terviklikkus oli seotud protsessi-, kvaliteedi- ja juhtimisloogikaga. Juhtumites, kus see loogika jäi tunnetuslikuks, sõltus riskijuhtimine rohkem üksikisikute kogemusest.

Tulemused kinnitavad ka organisatsiooniarhitektuuri vaadet, mille järgi organisatsiooni toimimise usaldusväärsus sõltub protsesside, rollide ja tehnoloogia sidususest (Ross et al., 2006, lk 8–9, 26–28). Suurema terviklikkusega juhtumites ei olnud riskijuhtimine eraldiseisev kontrollikiht, vaid osa samast toimimisloogikast. Madalama terviklikkusega juhtumites ilmnesid riskid eelkõige protsesside üleminekukohtades, näiteks rollimuutuste ja *offboarding'u* ajal.

Samuti toetavad tulemused Aveni (2016, lk 2–3, 6) ja ISO 31000 käsitlust, mille järgi riskijuhtimise kvaliteet sõltub teadmiste seotusest ja kasutamisest. Empiiriline analüüs näitas, et riskikohad olid sageli teada, kuid teadmised olid jaotunud funktsiooniti: Personaliosakond keskendus protsessidele, IT süsteemidele ja ligipääsudele ning riskifunktsioon kontrollidele. Kui need vaated ei koondunud ühtsesse loogikasse, jäi ka riskijuhtimine killustunuks. Seetõttu võib

personaliarhitektuuri terviklikkust käsitleda organisatsioonilise küpsuse näitajana, mitte üksnes personalifunktsiooni omadusena.

3.1. Kolme mõõtme koosmõju riskijuhtimise süsteemsusele

Juhtumite võrdlus näitas, et riskijuhtimise süsteemsus ei tulene ühest mõõtmest eraldi, vaid nende koostoimest. Ühe mõõtme tugevus ei kompenseeri teise nõrkust.

Protsesside terviklikkus mõjutas riskijuhtimist eelkõige töötaja elukaare loogika kaudu. Organisatsioonides, kus *onboarding*, rollimuutused ja *offboarding* olid käsitletud tervikliku protsessina, oli riskide märkamise võimekus suurem. Samas ilmnes, et peamised riskikohad tekkisid protsesside üleminekutes, eriti siis, kui vastutus liikus funktsioonide vahel. Seega oli määrav protsessi järjepidev rakendamine.

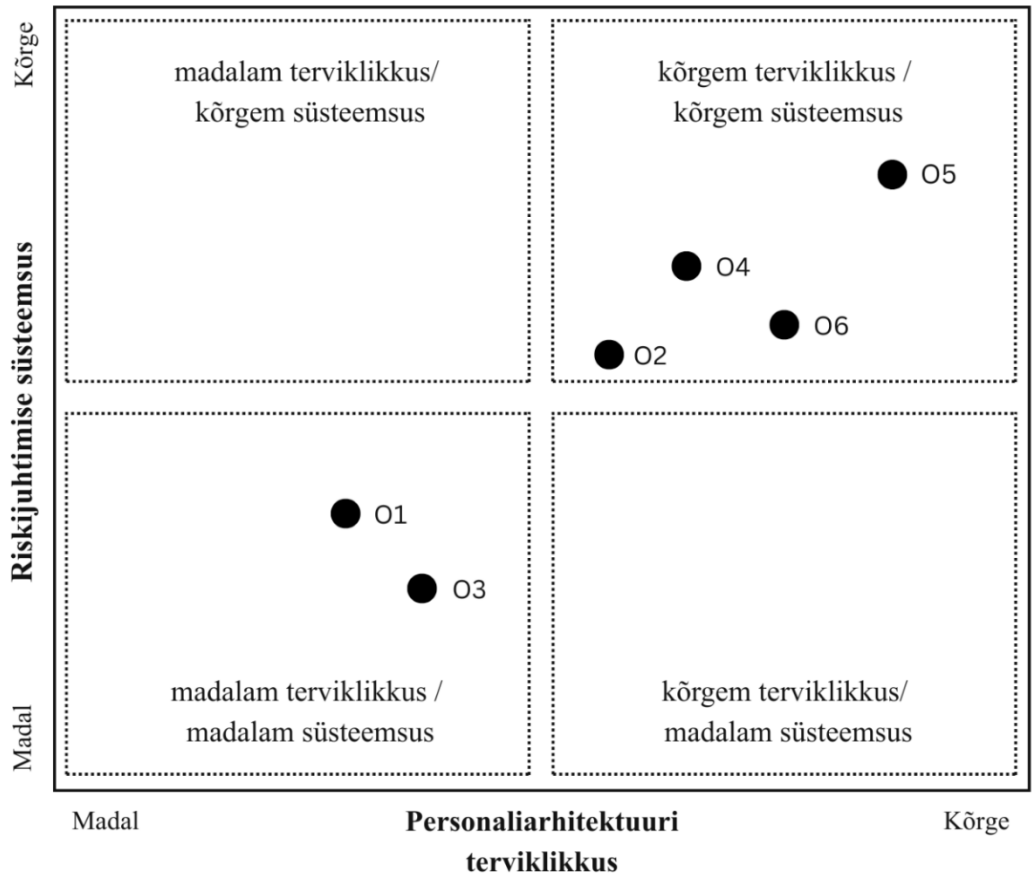
Tehnoloogia terviklikkus oli kõige nähtavam mõõde, kuid ei taganud iseseisvalt riskijuhtimise süsteemsust. Organisatsioonid teadvustasid hästi süsteemide killustatusest, *legacy*-lahendustest ja ligipääsuhaldusest tulenevaid riske, kuid ilma selge protsessi- ja vastutusloogikata jäi riskijuhtimine osaliselt reageerivaks. Organisatsioon 4 illustreeris seda näidates, et tehnoloogia terviklikkus oli tugev, kuid protsessi- ja vastutusloogika ebaühtlus piiras terviklikku juhtimist.

Rollide ja vastutuste terviklikkus eristas kõige selgemini küpsemaid ja vähem küpseid organisatsioone. Kriitilisi rolle tunnetati üldiselt hästi, kuid sageli jäi see teadmine juhitasandi või üksikisikute kogemuse tasandile. Ainult suurema terviklikkusega juhtumites oli see formaliseeritud ja süsteemselt juhitud. Seal, kus kriitilisus ei olnud nähtav ega juhitav, sõltus riskijuhtimine rohkem võtmeisikutest kui süsteemist.

Juhtumite põhjal võib järeldada, et riskijuhtimise praktikad muutuvad süsteemseks ainult siis, kui protsessid, tehnoloogia ning rollid ja vastutused toimivad kooskõlas. Kui üks neist katkeb, kandub risk edasi nende kokkupuutepunktidesse. Seetõttu sõltub riskijuhtimise kvaliteet eeskätt nende mõõtmete koostoime tugevusest, mitte üksikute elementide arendatuse tasemest.

3.2. Riskijuhtimise praktikate süsteemsus

Empiiriline analüüs näitas, et uuritud organisatsioonides erines riskijuhtimine selle poolest, kui sidus, ennetav ja igapäevase juhtimisloogikaga seotud see oli. Juhtumite võrdlusest joonistus välja kolm peamist lähenemist: reaktiivne ja killustunud käsitlus, osaliselt integreeritud käsitlus ning süsteemselt juhitud ja valdavalt ennetav käsitlus. Juhtumitevahelise sünteesi visualiseerimiseks on joonisel 8 esitatud organisatsioonide paiknemine personaliarhitektuuri terviklikkuse ja riskijuhtimise süsteemsuse telgedel.



Joonis 8. Uuritud organisatsioonide paiknemine personaliarhitektuuri terviklikkuse ja riskijuhtimise süsteemsuse telgedel
Allikas: autori koostatud juhtumianalüüside ja juhtumite võrdluse põhjal.

Joonis 8 näitab selget mustrit: suurem personaliarhitektuuri terviklikkus on seotud süsteemsema riskijuhtimisega. Paremas ülanurgas paiknev organisatsioon 5 esindab kõrgeimat küpsustaset, kus protsessid, rollid, tehnoloogia ja riskijuhtimine moodustavad ühtse juhtimisloogika. Riskide käsitlus on selles juhtumis valdavalt ennetav ning seotud igapäevase juhtimise, kvaliteediloogika ja kriitiliste rollide süsteemse hindamisega.

Samas kvadrandis, kuid mõnevõrra madalamal tasemel, paiknevad organisatsioonid 2, 4 ja 6. Nende puhul on personaliarhitektuuri terviklikkus küll suhteliselt kõrge, kuid riskijuhtimise süsteemsus on ebaühtlasem. Näiteks organisatsioon 4 paistab silma tugeva tehnoloogilise terviklikkusega, kuid protsesside ja rollide sidusus ei ole samal määral ennetavalt juhitud. Organisatsioon 6 puhul on seosed olemas, kuid rakenduses esineb katkestusi. Organisatsioon 2 paikneb selles rühmas kõige madalamal, viidates, et kuigi terviklikkuse eeldused on olemas, ei ole need veel täielikult riskijuhtimise praktikatesse integreeritud.

Alumises vasakus kvadrandis paiknevad organisatsioonid 1 ja 3, mida iseloomustab nii madalam personaliarhitektuuri terviklikkus kui ka madalam riskijuhtimise süsteemsus. Nendes juhtumites ei ole protsesside, rollide ja tehnoloogia vahelised seosed piisavalt formaliseeritud ega funktsioonideüleselt koordineeritud. Riskid muutuvad nähtavaks eeskätt katkestuste, ligipääsuprobleemide või üksikisikute kogemuste kaudu, mistõttu on juhtimine valdavalt reageeriv.

Oluline on märkida, et joonise paremas alumises kvadrandis (kõrge terviklikkus, madal süsteemsus) ei paikne ükski juhtum. See viitab, et suurem personaliarhitektuuri terviklikkus loob eeldused riskijuhtimise süsteemsuse kujunemiseks ning nende kahe nähtuse vahel esineb selge juhtumitevaheline koosmuster.

Seega ei eristanud organisatsioone mitte riskijuhtimise olemasolu, vaid selle lõimitus organisatsiooni toimimisloogikasse. Süsteemsemates juhtumites oli riskijuhtimine osa protsessi- ja rolliloogikast ning toetas ennetavat juhtimist. Vähem küpsetes juhtumites toimis see pigem järelkontrolli mehhanismina.

Need leiud on kooskõlas ISO 31000 käsitlusega, mille kohaselt peab riskijuhtimine olema integreeritud organisatsiooni juhtimisse ja otsustusprotsessidesse (International Organization for Standardization, 2018, lk 4–7, 8–14). Samuti toetavad need Aveni (2016, lk 2–3) käsitlust, mille järgi sõltub riskijuhtimise kvaliteet teadmiste sidususest ja kasutamisest. Kui protsessid, rollid ja tehnoloogia on ühendatud ühtse juhtimisloogikaga, muutuvad riskid paremini nähtavaks enne nende realiseerumist; killustunud seoste korral jääb riskijuhtimine pigem reageerivaks.

Joonis on kvalitatiivse juhtumivõrdluse visualiseering, mitte statistiline mõõtmistulemus. Punktide paiknemine tugineb juhtumiprofiilidele, koodiraamatu koondhinnangu alustele ja juhtumite võrdlevale tõlgendusele.

3.3. Funktsioonidevahelised erinevused

Üks olulisemaid järeldusi oli, et funktsioonidevahelised erinevused ei ole kõrvalnähtus, vaid personaliarhitektuuri toimimise osa. HR-, IT- ja riski- või õigusfunktsioon kirjeldasid sama nähtust erinevatest vaatenurkadest, mis ei olnud vastuolulised, vaid täiendavad.

Seda illustreerib järgmine tsitaat:
„HR näeb inimese staatust, ametikohta ja töösuhte muutust. IT näeb kontosid, ligipääse, süsteemseid sõltuvusi ja kontrolli. Juht näeb töövõimet, kiirust ja äri vajadust. Riskifunktsioon näeb võimalikku nõrka kohta“ (Organisatsioon 6: riskijuhtimise funktsiooni esindaja, 18.03.2026).

See näitab, et personaliarhitektuuri terviklikkus muutub organisatsioonis nähtavaks funktsiooniti jaotunud teadlikkuse kaudu. Personalifunktsioon tõi esile protsesside toimimise ja töötajakogemuse, IT süsteemid ja ligipääsud ning riskifunktsioon haavatavuse ja kontrolli piirid. Tegemist ei ole erinevate nähtustega, vaid sama süsteemi erinevate vaadetega.

Teoreetiliselt kinnitab see organisatsiooniarhitektuuri käsitlust, mille järgi eri funktsioonide teadmised tuleb siduda ühtseks toimimisloogikaks (Ross et al., 2006, lk 8–9, 47–51). Empiiriline analüüs näitas, et seal, kus see tõlkimine ei toimu, jääb riskijuhtimine killustunuks.

Kõrgema terviklikkusega juhtumites olid funktsioonide vaated paremini kooskõlas ja toetasid üksteist. Keskmise terviklikkusega juhtumites tekkis nende vahele lünk, kus riskid tegelikult realiseerusid. See funktsioonidevaheline vaheala on üks töö keskseid järeldusi.

Seega ei tähenda personaliarhitektuuri terviklikkus ainult paremat dokumentatsiooni või kontrolli, vaid eeldab funktsioonidevahelise ühise arusaama kujundamist. Individuaalne teadlikkus toimib siin organisatsiooni koordineerimisvõime näitajana: mida paremini suudetakse eri vaated siduda, seda väiksem on tõenäosus, et riskid jäävad märkamata.

3.4. Järeldused uurimisküsimuste lõikes

Esimesele uurimisküsimusele, kuidas avaldub personaliarhitektuuri terviklikkus uuritud organisatsioonides ning kuidas kirjeldavad juhid ja võtmeisikud selle rolli organisatsiooni toimimises, näitas analüüs, et kuigi mõiste ei olnud kõigile terminina tuttav, mõisteti selle sisu sisuliselt. Personaliarhitektuuri kirjeldati praktilise tervikuna, kus rollid, protsessid, õigused, süsteemid ja vastutus peavad olema omavahel kooskõlas. Eri funktsioonid kasutasid erinevat sõnavara, kuid kirjeldasid sama loogikat. See kinnitab, et personaliarhitektuur ei avaldu mõiste kasutuses, vaid organisatsiooni suutlikkuses siduda personaliga seotud valikud toimimisloogika ja strateegiliste võimekustega (Lepak & Snell, 1999, lk 33–42; Becker & Huselid, 2006, lk 899, 903–905). Praktiliselt tähendab see, et sisuline arusaam võib olla olemas ka ilma ühtse terminita, kuid süsteemne arendamine eeldab ühist käsitlust.

Teisele uurimisküsimusele, millised tegurid kujundavad personaliarhitektuuri terviklikkust, näitas analüüs, et määravaks on funktsionaalne vaade, ligipääs tervikpildile ja organisatsiooni formaliseerituse aste. Personal keskendus protsessidele ja töötajakogemusele, IT süsteemidele ja ligipääsudele ning riskifunktsioon kontrollile ja haavatavustele. See näitab, et teadlikkus tervikust on organisatsioonis jaotunud ning sõltub funktsiooni vaatenurgast. Seetõttu ei saa terviklikkust kujundada ühe funktsiooni sees, vaid see eeldab erinevate vaadete sidumist ühisesse loogikasse.

Kolmandale uurimisküsimusele, kuidas personaliarhitektuuri terviklikkus avaldub riskijuhtimises, ilmnes neli korduvat mustrit. Esiteks avaldub see suutlikkuses märgata töötaja elukaare kriitilisi üleminekukohti (nt tööle asumine, rollimuutus, ajutine asendus ja töösuhte lõppemine). Teiseks sõltub see sellest, kui hästi on ligipääsud seotud tegelike rollide ja tööülesannetega. Kolmandaks väljendub see kriitiliste rollide ja asendatavuse riskide teadvustamises. Neljandaks avaldub see võimes tõlkida tehnoloogilised riskid juhtimisotsusteks, mitte jätta neid ainult IT tasandile. See on kooskõlas Aveni ja ISO 31000 käsitlusega, mille järgi riskijuhtimise kvaliteet sõltub teadmusest ja süsteemsest otsustusloogikast. Praktiliselt tähendab see, et personaliarhitektuuri terviklikkus on riskijuhtimise eeltingimus, mitte kõrvalteema.

Neljandale uurimisküsimusele, millised mustrid seostavad terviklikkust ja riskijuhtimise süsteemsust, näitas võrdlev analüüs selget seost. Juhtumites, kus protsessid, rollid ja tehnoloogilised lahendused olid omavahel seotud, oli riskijuhtimine süsteemsem ja ennetavam. Vastutused olid selgemad ning riskid nähtavamad enne nende realiseerumist. Juhtumites, kus neid

seoseid käsitleti eraldi, oli riskijuhtimine killustunum ja reageerivam. Seega näitab analüüs, et suurem personaliarhitektuuri terviklikkus on seotud suurema riskijuhtimise süsteemsusega. See tulemus on kooskõlas organisatsiooniarhitektuuri käsitlusega, mille järgi organisatsiooni toimivus sõltub integratsiooni ja standardiseerituse tasemest (Ross et al., 2006, lk 8–9, 26–28, 47–51).

3.5. Lõppjäreldus

Käesoleva töö keskne järeldus on, et personaliarhitektuuri terviklikkus on Eesti infotehnoloogiafookusega suurorganisatsioonides oluline organisatsioonilise küpsuse näitaja, sest see peegeldab organisatsiooni suutlikkust siduda inimesed, rollid, protsessid, ligipääsud ja tehnoloogiad ühtseks toimimisloogikaks. Empiiriline analüüs näitas, et riskijuhtimise praktikate tugevust ei mõjuta üksnes kontrollimeetmete olemasolu, vaid eelkõige see, kas organisatsioon suudab nende elementide omavahelisi seoseid terviklikult kujundada ja juhtida.

Töö peamine sisuline panus seisneb järelduses, et personaliarhitektuuri terviklikkus ei ole pelgalt personalifunktsiooni sisemine omadus, vaid organisatsiooniülene võimekus, mis mõjutab otseselt riskide ennetamist, juhtimist ja kontrollitavust. Juhtumites, kus protsesside terviklikkus, tehnoloogia terviklikkus ning rollide ja vastutuste terviklikkus olid omavahel kooskõlas, avaldus riskijuhtimine süsteemsemalt ja ennetavamalt ning oli vähem sõltuv üksikute inimeste kogemusest. Juhtumites, kus need mõõtmed jäid üksteisest eraldatuks või arenesid ebaühtlaselt, muutus riskijuhtimine hajusamaks, reageerivamaks ja tugevamalt funktsioonipõhiseks.

Teoreetiliselt toetavad tulemused arusaama, et personaliarhitektuuri on põhjendatud käsitleda organisatsiooniarhitektuuri funktsionaalse osana, mitte üksnes personalijuhtimise kitsama valdkonnana. Tulemused on kooskõlas Lepaki ja Snelli ning Beckeri ja Huselidi käsitlustega, mille järgi personalivalikud peegeldavad organisatsiooni strateegilisi prioriteete, samuti Ross et al. vaatega, mille järgi organisatsiooni toimivus sõltub protsesside, rollide ja tehnoloogilise taristu kooskõlast (Lepak & Snell, 1999, lk 31–37; Becker & Huselid, 2006, lk 899, 903–904; Ross et al., 2006, lk 8–9, 26–28, 47–51). Samuti haakuvad tulemused Aveni ning ISO 31000 käsitlustega, mille järgi riskijuhtimise praktikate kvaliteet sõltub sellest, kui hästi organisatsioon suudab ühendada teadmised, ebakindluse ja otsustusprotsessi ühtseks juhtimisraamiks (Aven, 2016, lk 2–3, 5–6; International Organization for Standardization, 2018, lk 1, 4–7, 8–14). Käesoleva töö tulemused täpsustavad seda arusaama, näidates, et personaliarhitektuuri terviklikkus on üks

mehhanism, mille kaudu see ühendamine praktikas kas toimib või katkeb, samal ajal kui eri funktsioonide teadlikkus sellest tervikust mõjutab, kui hästi need seosed organisatsioonis nähtavaks muutuvad.

Kokkuvõttes näitab käesolev töö, et personaliarhitektuuri terviklikkus on ühtaegu organisatsioonilise küpsuse näitaja ja praktiline lähtekoht riskijuhtimise süsteemsuse hindamiseks. Selle kaudu on võimalik mõista, miks mõnes organisatsioonis toetavad personaliprotsessid, rollid ja tehnoloogiad riskide ennetamist süsteemselt, samas kui teistes jäävad samad seosed killustunuks ja reageerivaks. Selles seisneb töö peamine järeldus ja panus.

3.5.1. Praktilised ettepanekud organisatsioonidele

Töö tulemuste põhjal saab esitada mitu praktilist ettepanekut organisatsioonidele, kes soovivad tugevdada personaliarhitektuuri terviklikkust ja selle kaudu ka riskijuhtimise süsteemsust.

Esiteks on oluline käsitleda personaliprotsesse, rollistruktuuri, ligipääsuhaldust ja tehnoloogilisi lahendusi omavahel seotud juhtimisvaldkondadena, mitte eraldiseisvate funktsioonidena. See tähendab, et personali-, IT- ja riskijuhtimise vaated tuleb siduda ühtseks arusaamaks sellest, kuidas töötajate rollid, õigused, vastutused ja protsessid organisatsioonis tegelikult toimivad.

Teiseks tuleks organisatsioonides selgemalt määratleda rollide ja protsesside kokkupuutekohad, eriti nendes töötaja elukaare etappides, kus riskid on suuremad, näiteks värbamisel, rollimuutuste korral ja töösuhte lõpetamisel. Just nendes punktides avalduvad kõige selgemini võimalikud katkestused vastutustes, andmevoogudes ja ligipääsude halduses.

Kolmandaks on soovitatav hinnata regulaarselt, kuivõrd ühtlaselt mõistavad erinevad funktsioonid personaliarhitektuuri tervikut. Töö tulemused näitasid, et riskijuhtimise praktikate tugevust mõjutab otseselt see, kas personali-, IT- ja riskivaldkonna esindajatel on ühine arusaam protsessidest, tehnoloogilistest sõltuvustest ja vastutusjaotusest.

Neljandaks ei peaks organisatsioonid piirduma üksnes uute kontrollimeetmete lisamisega, vaid pöörama tähelepanu ka sellele, kas olemasolevad kontrollid on seotud tegelike tööprotsesside ja rolliloogikaga. Kui kontrollid eksisteerivad formaalselt, kuid ei toetu toimivale protsessi- ja vastutusselgusele, jääb riskijuhtimine paratamatult killustunuks.

Viiendaks võib personaliarhitektuuri terviklikkust kasutada ühe analüütilise vaatenurgana organisatsiooni riskijuhtimise küpsuse hindamisel. See aitab nähtavaks teha, kas riskide käsitlemine toetub süsteemsele toimimisloogikale või sõltub peamiselt üksikute inimeste kogemusest ja funktsioonipõhisest praktikast.

KOKKUVÕTE

Magistritöö eesmärk oli selgitada, kuidas personaliarhitektuuri terviklikkus avaldub Eesti infotehnoloogiafookusega suurorganisatsioonides ning kuidas see on seotud riskijuhtimise praktikate süsteemsuse ja ennetavusega. Fookuses oli rollide, protsesside, andmete, ligipääsude ja tehnoloogiate seoste sidusus ning selle mõju organisatsiooni võimele riske märgata ja juhtida.

Teoreetiline käsitlus tõi esile, et personaliarhitektuur kirjeldab organisatsiooni toimimisloogikat personalivaldkonna vaates, sidudes rollid, vastutused, protsessid ja tehnoloogiad tervikuks. Organisatsiooniarhitektuuri vaade rõhutab nende elementide kooskõla tähtsust organisatsiooni toimimises, samas kui riskijuhtimise käsitlused (Aven; ISO 31000) seovad riskide juhtimise ebakindluse mõtestamise ja süsteemsete seoste mõistmisega. Nende lähtekohtade põhjal koostati integratsioonimudel, mis seob personaliarhitektuuri terviklikkuse, arhitektuurilise kooskõla ja riskijuhtimise praktikad ühtseks analüütiliseks raamistikuks.

Empiiriline uurimus viidi läbi kvalitatiivse mitme juhtumiga juhtumiuuringuna. Uuringus osales kuus Eesti infotehnoloogiafookusega suurorganisatsiooni ning viidi läbi 15 poolstruktureeritud intervjuud personali-, IT- ning riski- või õigusfunktsiooni esindajatega. Andmeid analüüsiti temaatilise sisuanalüüsi abil, kasutades teooriast tuletatud kodeerimisraamistikku. Analüüsi keskmes olid protsesside, tehnoloogia ning rollide ja vastutuste terviklikkus ning nende seosed riskijuhtimise praktikatega.

Tulemused näitasid, et personaliarhitektuuri terviklikkus ja riskijuhtimise praktikate süsteemsus on omavahel seotud, kuid selle seose tugevus erines juhtumiti. Riskijuhtimise praktikate kvaliteet oli seotud sellega, kui sidusalt olid organisatsioonis seotud protsessid, tehnoloogia ning rollid ja vastutused. Juhtumites, kus need moodustasid ühtse toimimisloogika, olid riskid paremini nähtavad ning riskijuhtimine süsteemsem ja ennetavam. Juhtumites, kus sama nähtust käsitleti funktsiooniti eraldi, jäi riskijuhtimine hajusamaks ja sõltus rohkem üksikisikute kogemusest.

Juhtumite võrdlus tõi esile kolm korduvat mustrit. Esiteks koondusid riskid töötaja elukaare üleminekukohtadesse, nagu tööle asumine, rollimuutused ja töösuhte lõppemine. Teiseks ilmnes, et tehnoloogia terviklikkus oli mitmes organisatsioonis arenenum kui protsesside ning rollide ja vastutuste terviklikkus. Kolmandaks sõltus rollide ja vastutuste küpsus sellest, kas kriitilised rollid, vastutus ja ligipääsud olid selgelt määratletud ja formaliseeritud või jäid praktilise kogemuse tasandile.

Analüüs näitas ka, et funktsioonidevahelised erinevused on personaliarhitektuuri terviklikkuse loomulik osa. HR-, IT- ja riskifunktsioon kirjeldasid sama nähtust erinevatest vaatenurkadest, keskendudes vastavalt protsessidele, süsteemidele ja kontrollikeskkonnale. Kui need vaated ei koondunud ühisesse arusaama, jäi ka riskijuhtimine killustunumaks.

Töö teoreetiline panus seisneb personaliarhitektuuri terviklikkuse käsitlemises organisatsiooniülese võimekusena ja organisatsioonilise küpsuse näitajana. Praktiline panus seisneb riskikohtade nähtavaks tegemises personaliprotsessides ning rõhutamises, et riskijuhtimise süsteemsus sõltub eelkõige funktsioonidevahelisest kooskõlast.

Uurimuse piirangud tulenevad kvalitatiivsest lähenemisest ja valimi suurusest. Edasised uuringud võiksid laiendada valimit, võrrelda eri riikide praktikaid ning analüüsida kvantitatiivselt seoseid personaliarhitektuuri terviklikkuse ja konkreetsete riskinäitajate vahel. Kokkuvõttes näitab töö, et personaliarhitektuuri terviklikkus on oluline organisatsioonilise küpsuse näitaja ning toetab riskijuhtimise süsteemsemat ja ennetavamat toimimist.

SUMMARY

THE RELATIONSHIP BETWEEN HR ARCHITECTURE INTEGRITY AND RISK MANAGEMENT PRACTICES IN ESTONIAN LARGE IT-ORIENTED ORGANISATIONS

Liis Hulkko

This master's thesis examines the relationship between human resources architecture integrity and risk management practices in large IT-oriented organisations in Estonia. The topic is relevant in the context of increasing digitalisation, growing data volumes, and rising cyber risks, which extend beyond IT and affect organisational functioning as a whole. Despite this, the HR function is often not fully integrated into enterprise architecture and risk management, which may limit an organisation's ability to understand and manage critical interdependencies.

The research problem lies in the limited knowledge of how HR architecture integrity manifests itself in Estonian large IT-oriented organisations and how it is related to risk management practices. The aim of the thesis was to clarify this relationship in order to better understand how the coherent management of people, roles, processes, data, and technologies supports risk prevention and risk management.

The main research question was: How is HR architecture integrity related to risk management practices in large IT-oriented organisations in Estonia? Based on this, four research questions were formulated, focusing on how HR architecture integrity manifests itself in the studied organisations, which factors support or hinder it across organisational functions, how it is reflected in risk management practices, and which cross-case patterns indicate a relationship between HR architecture integrity and the systematic nature of risk management.

The theoretical framework draws on HR architecture, enterprise architecture, and risk management literature. These perspectives are integrated through three analytical dimensions central to the study: processes, roles, and technologies.

The empirical part of the thesis followed a qualitative multiple-case study design. Data were collected through semi-structured interviews with representatives of HR, IT, and risk or legal functions from six large IT-oriented organisations in Estonia. In total, 15 interviews were conducted. The data were analysed using thematic analysis and cross-case comparison.

The results showed that HR architecture integrity and risk management practices are closely related, although the strength of this relationship varies across organisations. Where processes, roles, technological solutions, and control mechanisms were more coherently aligned, risk management was more systematic and preventive. Where these elements were less integrated, risk management appeared more fragmented, reactive, and more dependent on individual knowledge and experience. The findings also showed that awareness of HR architecture differed across organisational functions, which influenced how clearly risk points became visible and manageable.

The thesis concludes that HR architecture integrity is an organisational capability that supports governance, resilience, and risk control in digitally dependent environments. Its practical value lies in demonstrating how a more coherent HR architecture can strengthen risk management practices, improve cross-functional alignment, and support more sustainable organisational functioning.

KASUTATUD ALLIKATE LOETELU

Arthur, J. B., & Boyles, T. (2007). Validating the human resource system structure: A levels-based strategic HRM approach. *Human Resource Management Review, 17*(1), 77–92. https://doi.org/10.1016/j.hrmr.2007.02.001

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Becker, B. E., & Huselid, M. A. (2006). Strategic human resources management: Where do we go from here? *Journal of Management, 32*(6), 898–925. https://doi.org/10.1177/0149206306293668

Boon, C., Den Hartog, D. N., & Lepak, D. P. (2019). A systematic review of human resource management systems and their measurement. *Journal of Management, 45*(6), 2498–2537. https://doi.org/10.1177/0149206318818718

Fenwick, A., Molnar, G., & Frangos, P. (2024). Revisiting the role of HR in the age of AI: Bringing humans and machines closer together in the workplace. *Frontiers in Artificial Intelligence, 6*, Article 1272823. https://doi.org/10.3389/frai.2023.1272823

Hansen, N. K., Güttel, W. H., & Swart, J. (2019). HRM in dynamic environments: Exploitative, exploratory, and ambidextrous HR architectures. *The International Journal of Human Resource Management, 30*(4), 648–679. https://doi.org/10.1080/09585192.2016.1270985

Hjerppe, K., Ruohonen, J., & Leppänen, V. (2019). *The general data protection regulation: Requirements, architectures, and constraints* [Preprint]. arXiv. https://arxiv.org/abs/1907.07498

Intervjuud. (2026). 15 poolstruktureeritud intervjuud kuue Eesti infotehnoloogiafookusega suurorganisatsiooni HR-, IT- ning riski- või õigusfunktsiooni esindajatega [Anonümiseeritud transkriptsioonid]. Autori valduses.

International Organization for Standardization. (2018). *ISO 31000:2018 risk management—Guidelines*. ISO.

Kaplan, R. S., & Mikes, A. (2012, June). Managing risks: A new framework. *Harvard Business Review, 90*(6), 48–60.

KPMG Baltics OÜ. (2022). *Eesti ettevõtete küberturvalisuse uuring 2022*.

Laherand, M.-L. (2010). *Kvalitatiivne uurimisviis* (2. tr). OÜ Sulesepp.

Lankhorst, M. M., et al. (2009). *Enterprise architecture at work: Modelling, communication and analysis* (2nd ed.). Springer. https://doi.org/10.1007/978-3-642-01310-2

Lepak, D. P., & Snell, S. A. (1999). The human resource architecture: Toward a theory of human capital allocation and development. *Academy of Management Review, 24*(1), 31–48. https://doi.org/10.5465/amr.1999.1580439

Lorenz, B. (2024). *Cybersecurity skills needs analysis report: Estonia*. CyberHubs.

Majandus- ja Kommunikatsiooniministeerium. (2024). *Cybersecurity strategy 2024–2030: Cyber-conscious Estonia*. Republic of Estonia.

McMenemy, S. J., Vanderzanden, D., & Riga, S. A. (2017, December 4). *The highest risk area for GDPR compliance: Processing HR data*. Ogletree Deakins. https://ogletree.com/insights-resources/blog-posts/the-highest-risk-area-for-gdpr-compliance-processing-hr-data/

Riigi Infosüsteemi Amet. (2024). *Cyber security in Estonia 2024*. Riigi Infosüsteemi Amet.

Ross, J. W., Weill, P., & Robertson, D. C. (2006). *Enterprise architecture as strategy: Creating a foundation for business execution*. Harvard Business School Press.

Rozehnal, P., & Novák, V. (2018). The core of enterprise architecture as a management tool: GDPR implementation case study. In *IDIMT-2018: Strategic modeling in management, economy and society: 26th Interdisciplinary Information Management Talks* (pp. 359–366).

Shahiduzzaman, M. (2025). Digital maturity in transforming human resource management in the post-COVID era: A thematic analysis. *Administrative Sciences, 15*(2), Article 51. https://doi.org/10.3390/admsci15020051

Smirnova, Y., & Travieso-Morales, V. (2024). Understanding challenges of GDPR implementation in business enterprises: A systematic literature review. *International Journal of Law and Management, 66*(3), 326–344. https://doi.org/10.1108/IJLMA-08-2023-0170

Teixeira, C., Vasconcelos, A., Sousa, P., & Marques, M. J. (2021). Enterprise architecture patterns for GDPR compliance. In *Proceedings of the 23rd International Conference on Enterprise Information Systems (ICEIS 2021)* (Vol. 2, pp. 715–725). SCITEPRESS. https://doi.org/10.5220/0010441307150725

The Open Group. (2017). *How to use the TOGAF® 9.1 framework with the ArchiMate® 3.0 modeling language* (White Paper W171). The Open Group.

The Open Group. (2018). *The TOGAF® standard, version 9.2* (C182). The Open Group.

Ussher-Eke, D. (2025). HR and GDPR: Partnering to protect employee data. *World Journal of Advanced Research and Reviews, 27*(2), 717–730. https://doi.org/10.30574/wjarr.2025.27.2.2902

Vrhovec, S., & Markelj, B. (2024). We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers. *PLOS ONE, 19*(10), Article e0312266. https://doi.org/10.1371/journal.pone.0312266

Õunapuu, L. (2014). *Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes*. Tartu Ülikool.

LISAD

Lisa 1. Poolstruktureeritud intervjuukava

Üldpõhimõtted

Intervjueerija palub iga olulisema väite või teema kohta vähemalt ühe konkreetse näite. Kui vastus jääb üldiseks, kasutatakse täpsustavaid küsimusi, näiteks „Kas saate tuua ühe konkreetse näite?“, „Mis täpselt juhtus?“ ja „Kes otsustas ning mille põhjal?“.

Teemasid käsitletakse rollispetsiifiliselt HR-, IT- ja riski-/õigusvaates, kuid põhiteemad ja võrdlusloogika on kõigil osalejatel samad. Intervjuu alguses ei anta mõistele „personaliarhitektuur“ kitsast definitsiooni, et hinnata osaleja tegelikku arusaama.

Intervjuu sissejuhatus

Uuring käsitleb, kuidas organisatsioonides mõistetakse ja juhitakse personaliarhitektuuri tervikuna ning kuidas see on seotud riskide ennetamise ja juhtimisega digitaalses, sealhulgas küberriskide kontekstis. Tähelepanu keskmes on osaleja praktiline kogemus oma rollist lähtuvalt, eriti olukorrad, kus personaliprotsessid, tehnoloogia, otsused ja riskid omavahel kokku puutuvad või vajavad paremat kooskõla.

Enne intervjuu algust kinnitatakse anonüümsus ja andmete kasutamise põhimõtted, küsitakse nõusolekut salvestamiseks ning selgitatakse intervjuu eeldatav kestus, umbes 35 kuni 45 minutit.

Taustainfo

1. Palun kirjeldage lühidalt oma praegust rolli ja peamisi vastutusvaldkondi.
2. Kui kaua olete olnud selles rollis ja kui kaua kokku selles organisatsioonis?
3. Millistes personaliga seotud protsessides või otsustes olete ise otseselt osalenud või nende mõju kogenud?
4. Kellega te tavaliselt koostööd teete personaliprotsesside ja riskiteemade puhul?

1. Personaliarhitektuuri mõistmine ja tervikloogika

5. Kui te mõtlete oma organisatsiooni peale, siis mida tähendab teie jaoks personaliarhitektuur?

6. Millised osad on teie hinnangul selles kõige olulisemad, näiteks rollid, protsessid, tehnoloogia, reeglid või vastutused? Miks?

7. Kas personaliarhitektuur on teie organisatsioonis pigem teadlikult kujundatud tervik või ajas kujunenud lahenduste ja kompromisside kogum?

8. Millal muutub personaliarhitektuur teie jaoks eriti nähtavaks, näiteks auditi, intsidendi, kiire kasvu, koondamise, ühinemise või ligipääsuprobleemide korral?

Rollispetsiifilised täpsustused

HR: Millised osad on teadlikult kujundatud ja millised pigem ajalooliselt kujunenud?

IT: Kas tegemist on integreeritud terviku või eraldiseisvate lahendustega?

Risk/õigus: Millal muutub see teema riskiks või vastavusküsimuseks?

2. Protsesside terviklikkus

9. Palun kirjeldage, kuidas on personaliga seotud protsessid teie organisatsioonis seotud, kui vaadata töötaja elukaart tervikuna alates värbamisest kuni lahkumiseni.

10. Kus protsessid omavahel kokku puutuvad ja kuidas info nende vahel liigub?

11. Kus tekib katkestusi, dubleerimist või ebaselgust?

12. Millised töötaja elukaare üleminekukohad on teie hinnangul kõige riskitundlikumad ja miks?

Rollispetsiifilised täpsustused

HR: Kuidas tagatakse protsesside järjepidevus võtmeisikute vahetumisel?

IT: Millal tekitab protsesside killustatus tehnilisi või turberiske?

Risk/õigus: Kas protsessiriske käsitletakse ennetavalt või peamiselt tagantjärele?

3. Tehnoloogia terviklikkus

13. Millised süsteemid ja töövood toetavad teie organisatsioonis personaliprotsesse ja ligipääsude haldust?

14. Kui läbipaistev on teie jaoks seos rollide, vastutuste, ligipääsude ja süsteemide vahel?

15. Kas praegused tehnoloogilised lahendused pigem vähendavad riske või võivad neid teatud olukordades suurendada?

16. Millistes valdkondades puudub teie hinnangul organisatsioonil täielik ülevaade sellest, kellel on millele ligipääs ja miks?

Rollispetsiifilised täpsustused

HR: Kuidas mõjutab tehnoloogia protsesside kvaliteeti ja vigade riski?

IT: Kas ligipääsude loogika on rolli- ja riskipõhine või ajalooliselt kujunenud?

Risk/õigus: Kuidas hinnatakse tehnoloogiliste kontrollide piisavust?

4. Rollide ja vastutuste terviklikkus

17. Kuidas eristatakse teie organisatsioonis rolle nende strateegilise tähtsuse ja riskimõju alusel?

18. Kas teatud rollid on teadlikult määratletud kriitilisematena? Kuidas see kajastub ligipääsudes, kontrollides ja asendatavuses?

19. Milline roll või rollide rühm tekitaks suurima riski, kui see kaob ootamatult, muutub ajutiselt kättesaamatuks või teeb olulise vea?

Rollispetsiifilised täpsustused

HR: Kuidas hinnatakse kriitiliste rollide asendatavust ja teadmuse ülekandmist?

IT: Kas ligipääsude kriitilisus vastab rollide tegelikule riskile?

Risk/õigus: Kas rollide ebaselgus on põhjustanud intsidente või vastavusprobleeme?

5. Terviklikkuse ja riskijuhtimise seosed

20. Kuidas mõjutab teie hinnangul personaliarhitektuuri terviklikkus või selle puudumine riskide ennetamist ja juhtimist organisatsioonis?

21. Palun tooge üks konkreetne näide olukorrast, kus personaliarhitektuuri puudujääk või ebaselgus suurendas riski, tekitas vea või raskendas riski juhtimist.

22. Kas olete kogenud olukordi, kus riskijuhtimise kvaliteet sõltus rohkem konkreetsetest inimestest kui protsessidest ja süsteemist?

23. Millistes aspektides näete suurimat arenguvajadust, et personaliarhitektuur toetaks riskijuhtimist tõhusamalt?

24. Kas on mõni personaliprotsesside või riskijuhtimisega seotud teema, mis jääb organisatsioonides liiga sageli tähelepanuta või alahinnatud?

Lisa 2. Koodiraamat

Käesolev koodiraamat koondab intervjuuandmete analüüsis kasutatud põhikoodid ja alamkoodid. Koodiraamat tugineb töö teoreetilisele analüüsimaatriksile ning seda kasutati intervjuuandmete temaatilisel kodeerimisel, juhtumiprofiilide koostamisel ja juhtumite võrdlevas analüüsis. Koodide eesmärk oli teha nähtavaks, kuidas vastajad kirjeldavad personaliarhitektuuri terviklikkust protsesside, tehnoloogia ning rollide ja vastutuste vaates ning kuidas need seostuvad riskijuhtimise praktikatega. Koodiraamatu alusel kujundatud küpsuse koondhinnangu kriteeriumid on esitatud eraldi tabelis L2.2.

Tabel L2.1. Intervjuuandmete koodiraamat

Põhikood	**Alamkood**	**Koodi kirjeldus**	**Mida otsitakse vastustest**
Personaliarhitektuuri tervikloogika	Tervikvaade	Vastaja kirjeldab rolle, protsesse, tehnoloogiaid ja riske omavahel seotud süsteemina	Seoste sõnastamine, põhjus-tagajärg loogika, arhitektuurne tervikpilt
	Killustunud käsitlus	Vastaja kirjeldab üksikuid tegevusi või tööriistu, kuid mitte nendevahelisi seoseid	Fragmentaarsed vastused, üksikute probleemide loetelu
Protsesside terviklikkus	Töötaja elukaare tervik	Arusaam töötaja elukaarest kui seotud protsesside ahelast	Onboarding, rollimuutus, offboarding, ajutised õigused, erandid

	Üleminekukohad	Tähelepanu riskikohtadele protsesside vahekohtades	Rollivahetus, õiguste muutus, töölt lahkumine, ajutised rollid
	Standardiseeritus	Protsesside ühtlus, dokumenteeritus ja korduv rakendamine	Kas protsessid on kirjeldatud, kas neid järgitakse süsteemselt
	Erandite juhtimine	Kuidas käsitletakse erandeid ja kõrvalekaldeid	Ajutised õigused, käsitsi lahendused, erandotsused
Tehnoloogia terviklikkus	Süsteemide nähtavus	Arusaam sellest, millised süsteemid toetavad personaliprotsesse	HRIS, dokumendihaldus, IAM, töövood, integratsioonid
	Andmevood	Arusaam sellest, kuidas andmed liiguvad süsteemide ja protsesside vahel	Sisestamine, edastus, säilitamine, kustutamine, andmete dubleerimine
	Ligipääsuloogika	Arusaam õiguste andmise, muutmise ja tagasivõtmise loogikast	Rollipõhisus, õiguste lisamine, õiguste eemaldamine, ülevaatused
	Tehnoloogilised sõltuvused	Arusaam süsteemidevahelistest mõjudest ja riskidest	Integratsioonid, käsitsi sillad, tehnilised piirangud, süsteemivead
Rollide ja vastutuste terviklikkus	Rolliselgus	Arusaam sellest, kes mille eest vastutab	Rollikirjeldused, otsustusõigus, vastutuspiirid
	Kriitilised rollid	Arusaam sellest, millised rollid on organisatsiooni toimimise või turvalisuse seisukohalt kriitilised	Võtmerollid, raskesti asendatavad rollid, privileegitud rollid
	Vastutuse ja ligipääsu seos	Seos rolli, õiguste ja kontrolli vahel	Kellel on ligipääs, miks, kes kinnitab, kes kontrollib

	Funktsioonidevaheline koostöö	HR-i, IT ja riski-/õigusfunktsiooni omavaheline suhestumine	Koostöö kirjeldus, üleandmised, vastutuse hägustumine
Riskijuhtimise praktikad	Riskide tuvastamine	Kuidas märgatakse ja sõnastatakse personaliga seotud riske	Riskikohtade kirjeldused, probleemide märkamine, riskinäited
	Riskide hindamine	Kuidas hinnatakse riski olulisust ja mõju	Mõju, tõenäosus, teadmatus, ebakindlus, haavatavused
	Meetmete kavandamine	Kuidas valitakse ja rakendatakse ennetus- või kontrollimeetmeid	Kontrollid, koolitused, automatiseerimine, rollimuudatused
	Seire ja ülevaatus	Kuidas jälgitakse, kas protsessid ja kontrollid toimivad	Ligipääsude ülevaatus, auditid, logid, monitooring
Riskikäsitluse loogika	Ennetav loogika	Riskide käsitlus enne probleemi realiseerumist	Ennetus, disain, etteplaneerimine, riskikohtade varajane märkamine
	Reageeriv loogika	Riskide käsitlus pärast probleemi ilmnemist	Intsident, auditileid, rikkumine, tagajärgedepõhine käsitlus
	Vastavuspõhine käsitlus	Riskijuhtimist kirjeldatakse peamiselt nõuete täitmise kaudu	Vastavuskontroll, audit, regulatsioon, kontrollinõuded
	Ebakindluse teadvustamine	Riskide käsitlemine teadmatusest ja hallaladest lähtudes	Mida ei teata, süsteemidevahelised mõjud, nähtamatused

Allikas: autori koostatud töö teoreetilise analüüsimaatriksi põhjal.

Koodiraamatut kasutati kolmel tasandil:

1. esmasel kodeerimisel, et seostada intervjuuvastused teoreetiliste mõõtmetega;
2. juhtumiprofiilide koostamisel, et hinnata iga organisatsiooni terviklikkuse mustreid;
3. juhtumite võrdlevas analüüsis, et võrrelda funktsioonide ja organisatsioonide vahelisi sarnasusi, erinevusi ja katkestusi.

Koode käsitletakse analüütilise raamistikuna, mille abil hinnata seoste olemasolu, puudumist või killustatust intervjuuandmetes.

Tabel L2.2. Personaliarhitektuuri terviklikkuse koondhinnangu alused

Hindamistelg	**Madal küpsus**	**Keskmine küpsus**	**Kõrge küpsus**
Seoste nähtavus	Vastustes seosed rollide, protsesside, tehnoloogia ja riskide vahel on nõrgad või katkendlikud	Osa seoseid on nähtav, kuid kirjeldused on ebaühtlased	Seosed rollide, protsesside, tehnoloogia ja riskide vahel on selgelt sõnastatud
Vastuste süsteemsus	Vastused keskenduvad üksikutele probleemidele või tegevustele	Vastustes ilmneb osaline tervikvaade	Vastustes ilmneb läbiv tervikvaade ja sidus toimeloogika
Näidete konkreetsus	Näited on vähesed, juhuslikud või üldsõnalised	Näited on olemas, kuid mitte kõigis mõõtmetes võrdselt tugevad	Näited on konkreetsed, korduvad ja seotud eri mõõtmetega
Funktsioonidevaheline kooskõla	HR-i, IT ja riski-/õigusvaated on selgelt lahus või vastuolulised	Vaated kattuvad osaliselt, kuid lüngad on nähtavad	Vaated on suures osas kooskõlalised ja täiendavad üksteist
Protsesside terviklikkus	Elukaare protsessid on killustunud või sõltuvad üksikisikutest	Põhiprotsessid on olemas, kuid üleminekukohad on ebaühtlased	Protsessid on sidusad, kirjeldatud ja järjepidevalt juhitud

Tehnoloogia terviklikkus	Süsteemid ja ligipääsud on hajusad, seosed ebaselged	Põhiloogika on nähtav, kuid killustatus püsib	Süsteemid, andmevood ja ligipääsud on seostatud ja hästi mõistetavad
Rollide ja vastutuste terviklikkus	Vastutuspiirid on hägusad, kriitilised rollid vähe eristatud	Rollid ja vastutused on osaliselt selged	Rollid, vastutused ja kriitilisus on selgelt määratletud
Riskijuhtimise integratsioon	Riskijuhtimine on pigem reageeriv ja episoodiline	Riskid on nähtavad, kuid käsitlus on osaliselt killustunud	Riskijuhtimine on süsteemne, ennetav ja seotud protsesside, rollide ning tehnoloogiaga

Allikas: autori koostatud töö teoreetilise analüüsimaatriksi, koodiraamatu ja intervjuuandmete analüüsi põhjal.

Tabel L2.2 loodi töö teoreetilise analüüsimaatriksi ja koodiraamatu alusel, et põhjendada, mille järgi kujundati juhtumite personaliarhitektuuri terviklikkuse koondhinnang (Ross et al., 2006, lk 8–9, 47–51; Aven, 2016, lk 2–3, 6). Seda kasutati intervjuuandmete tõlgendamisel orientiirina, et võrrelda protsesside, tehnoloogia ning rollide ja vastutuste terviklikkuse avaldumist ning nende seoseid riskijuhtimise praktikatega. Koondhinnang kujunes nende tunnuste terviktõlgenduse põhjal.

Lisa 3. Võrdlusmaatriks

Käesolev võrdlusmaatriks koondab juhtumipõhise analüüsi põhijäreldused ühtsesse võrdlusraami. Maatriksi eesmärk on toetada juhtumitevahelist analüüsi, võimaldades võrrelda organisatsioonide vahel personaliarhitektuuri terviklikkuse mõõtmeid, riskijuhtimise praktikate iseloomu ning peamisi katkestusi ja tugevusi. Maatriks ei asenda juhtumianalüüse, vaid toimib nende sünteesiva kokkuvõttena.

Tabel L3.1. Juhtumite võrdlusmaatriks

Võrdlusdimensioon	**Organisatsioon 1**	**Organisatsioon 2**	**Organisatsioon 3**
Sektorigrupp	IT- ja digitaalse töökorraldusega suurorganisatsioon	IT-fookusega suurorganisatsioon	IT-fookusega suurorganisatsioon
Suurusklass	suurorganisatsioon	suurorganisatsioon	suurorganisatsioon
IT-sõltuvuse laad	mitme süsteemi, ligipääsuhalduse ja integratsioonide koosmõju	süsteemide, liidestuste ja andmevoogude sõltuvus	killustunud süsteemimaastik ja osaliselt vananenud lahendused
Regulatiivse surve tase	keskmine kuni kõrge	keskmine kuni kõrge	keskmine
Riskijuhtimise formaliseeritus	osaline	osaline	hajutatud
HR-, IT- ja riski-/õigusfunktsiooni eristatavus	eristatavad, kuid seosed ebaühtlased	HR eraldi, IT ja risk ühendatud	HR eraldi, IT ja risk ühendatud
Protsesside terviklikkus	keskmine	keskmine	keskmine
Tehnoloogia terviklikkus	keskmine	keskmine	keskmine
Rollide ja vastutuste terviklikkus	keskmine	keskmine	keskmine

Riskijuhtimise praktikate iseloom	kontrolli- ja vastavuspõhine	osaliselt ennetav, osaliselt kogemusest õppiv	hajutatud ja probleemipõhine
Valdav riskikäsitluse loogika	pigem reageeriv	keskmine, osaliselt ennetav	pigem reageeriv ja hajutatud
Peamised riskikohad	offboarding, rollimuutused, shadow IT, andmete hajumine	elukaare üleminekud, paralleelsed andmeallikad, vastutuse hägusus	teadmuse sõltuvus inimestest, killustunud süsteemid, ligipääsude läbipaistmatus
Peamised tugevused	tehnoloogiliste baasriskide teadvustamine, protsesside nähtavus	üleminekukohtade ja andmevoogude riskide teadvustamine	toimiv administratiivne baas, võtmeriskide tunnetamine
Funktsioonidevahelised vastuolud või katkestused	HR ja IT/risk näevad protsesse eri detailsusega	HR rõhutab andmekvaliteeti, IT/risk arhitektuuri ja õigusi	HR näeb toimivat hügieeni, IT/risk killustatust
Juhtumi koondhinnang	osaliselt süsteemne, kuid ebaühtlane	arenev, kuid osaliselt killustunud	administratiivselt toimiv, kuid strateegiliselt ebaühtlane

Allikas: autori koostatud juhtumianalüüside põhjal.

Lisa 4. Pilootuuringu analüüsi kokkuvõte

Käesolev lisa koondab pilootuuringu peamised tähelepanekud, nende tõlgenduse analüüsimaatriksi alusel ning pilootuuringu põhjal intervjuukavasse tehtud muudatused. Lisa eesmärk on näidata, kuidas pilootuuringut kasutati uurimisinstrumendi sisuliseks valideerimiseks ning põhiuuringu küsimuste täpsustamiseks.

Tabel L4.1. Pilootuuringu analüüsi kokkuvõte analüüsimaatriksi alusel

Analüüsimõõde	**Pilootuuringu põhitähelepanek**	**Esialgne tõlgendus küpsusloogika alusel**	**Pilootuuringu põhjal tehtud muudatus intervjuukavas**
Personaliarhitektuuri tervikloogika	Vastajad nimetasid rolle, protsesse ja süsteeme, kuid nendevahelised põhjus-tagajärg seosed ei olnud alati selgelt sõnastatud.	Keskmine tase. Põhielemendid on olemas, kuid terviklik arhitektuuriline loogika ei ole järjepidevalt nähtav.	Lisati rohkem küsimusi, mis suunavad vastajat kirjeldama seoseid, mitte ainult üksikuid tegevusi või vastutusi.
Protsesside terviklikkus	Onboarding ja offboarding olid üldjuhul kirjeldatavad, kuid töötaja elukaare tervik ning eriti üleminekukohad, näiteks rollimuutus ja ajutised õigused, jäid ebaühtlaselt nähtavaks.	Keskmine tase. Põhiprotsessid on olemas, kuid protsessi kui terviksüsteemi käsitlus on piiratud.	Küsimused seoti tugevamalt töötaja elukaare võtmeetappidega ning lisati täpsustused rollimuutuste, erandite ja õiguste muutmise kohta.
Tehnoloogia terviklikkus	IT-funktsioon kirjeldas süsteeme ja riske detailsemalt kui HR. HR-vaates käsitleti süsteeme pigem töövahenditena kui riskiloogika osana.	Ebaühtlane keskmine tase. Tehnoloogiline toimimine on osaliselt nähtav, kuid süsteemide, ligipääsude ja riskide seos ei ole kõigile funktsioonidele võrdselt selge.	Lisati küsimusi süsteemidevaheliste seoste, andmevoogude, ligipääsuõiguste muutmise ja tehnoloogiliste erandite kohta.

Rollide ja vastutuste terviklikkus	Kriitilisi rolle tunnetati pigem intuitiivselt kui süsteemselt. Otsustusõiguse, ligipääsu ja vastutuse seosed ei olnud alati läbipaistvad.	Madal kuni keskmine tase. Rollid on olemas, kuid rollipõhine juhtimis- ja kontrolliloogika ei ole ühtlaselt formaliseeritud.	Täiendati küsimusi kriitiliste rollide, vastutuse, otsustusõiguse ja ligipääsude seoste kohta.
Riskijuhtimise käsitlus	Riske kirjeldati peamiselt tagajärgede, auditileidude või vastavusnõuete kaudu. Teadmatusi ja ebakindlust käsitleti pigem paratamatusena kui juhitava riskina.	Keskmine tase. Riskidest räägitakse, kuid riskijuhtimise seos teadmatusest tulenevate haavatavustega ei ole süstemaatiliselt läbi mõtestatud.	Lisati küsimused ebakindluse, hallide alade, süsteemidevaheliste mõjude ja ennetusmeetmete otsustusloogika kohta.
Näidete ja tõenduslikkuse tase	Vastused jäid kohati üldiseks ning konkreetsed juhtumid ei kerkinud alati spontaanselt esile.	Analüütilise tõlgenduse jaoks ebapiisav detailsus ilma järelküsimusteta.	Lisati standardiseeritud täpsustavad järelküsimused, näiteks „Kas saate tuua konkreetse näite?” ja „Kuidas see praktikas toimib?”
Funktsioonide vaheline võrreldavus	Eri rollid käsitlesid samu teemasid erineva detailsuse ja rõhuasetusega, mistõttu ilma täiendava suunamiseta oli võrdlus ebaühtlane.	Võrdluspotentsiaal on olemas, kuid vajab suuremat struktuurset ühtlustamist.	Täpsustati küsimuste järjekorda ja lõppu lisati kontrollplokk, mis seob töötaja elukaare, rollid ja tehnoloogilised sõltuvused.

Allikas: autori koostatud pilootuuringu tulemuste ning töö teoreetilisest raamistikust tuletatud analüüsimaatriksi põhjal.

Pilootuuring näitas, et personaliarhitektuuri terviklikkuse kolm põhimõõdet, protsessid, tehnoloogia ning rollid ja vastutused, on empiiriliselt eristatavad, kuid vastajate kirjeldustes kipuvad need ilma täpsustava suunamiseta omavahel segunema. See tähendas, et intervjuukava tuli põhiuuringu jaoks siduda tugevamalt konkreetsete otsustuskohtade ja töötaja elukaare võtmeetappidega.

Pilootuuring kinnitas ka seda, et riskijuhtimise käsitlus kipub jääma vastavuse ja tagajärgede tasandile. Selleks et hinnata nähtust laiemalt, täiendati intervjuukava küsimustega, mis avavad teadmatusi ja ebakindluse kohti, süsteemidevahelisi mõjusid ning ennetusmeetmete valiku otsustusloogikat. Lisaks näitas piloot, et ilma standardiseeritud järelküsimusteta jäid vastused kohati liiga üldiseks. Seetõttu suurendati põhiuuringu intervjuukavas tõenduspõhiste näidete küsimise osakaalu.

Pilootuuringu tulemusel tehti intervjuukavasse neli peamist muudatust:

1. küsimused seoti tugevamalt töötaja elukaare etappidega, et vastused oleksid konkreetsemad ja võrreldavamad;
2. lisati küsimused ebakindluse ja teadmatusest tulenevate riskide kohta, et avada riskijuhtimist laiemalt kui ainult vastavus- ja kontrolliloogika kaudu;
3. täiendati tehnoloogilise mõõtme küsimusi, et tuua selgemalt välja süsteemide, andmevoogude ja ligipääsude seosed;
4. lisati standardiseeritud järelküsimused, mis aitavad esile kutsuda konkreetseid praktilisi näiteid.

Lisa 5. Lihtlitsents

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina Liis Hulkko

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose **Personaliarhitektuuri terviklikkuse seos riskijuhtimise praktikatega eesti infotehnoloogiafookusega suurorganisatsioonides**

mille juhendaja on Maarit Vabrit-Raadla, MA

1.1 reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2 üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.

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

02.05.2026

[1] *Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. jq 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.*