Johanna Huotari

Datan synkronointi identiteetinhallinnan ja toiminnanohjausjärjestelmän välillä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

5.3.2024

Tiivistelmä

Tekijä:	Johanna Huotari
Otsikko:	Datan synkronointi identiteetinhallinnan ja toiminnanohjausjärjestelmän välillä
Sivumäärä:	28 sivua
Aika:	5.3.2024
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Hyvinvointi- ja terveysteknologia
Ohjaajat:	Yliopettaja Mikael Soini Case-yritys, työpaikkaohjaaja, sisäisen valvonnan johtaja

---

Tämän insinöörityön aiheeksi valikoitui Case-yrityksen identiteetinhallinnan sekä toiminnanohjausjärjestelmän välisen tiedonkulun sekä siinä ilmenevien haasteiden havainnointi. Lisäksi olennaista oli tutustua identiteetin provisiointiprosessiin, SAP-järjestelmän erilaisiin roolikokonaisuuksiin sekä näihin vaikuttaviin erilaisiin tekijöihin. Työn pääasiallisena tavoitteena oli synkronoida tiedot järjestelmien välillä sekä selvittää, miksei tieto pysy ajantasaisena.

Työ toteutettiin aikavälillä syyskuu 2023 – maaliskuu 2024. Tietoa ongelmasta kerättiin yrityksen sisäisistä materiaaleista sekä dokumenttianalyysin ja avoimien haastatteluiden avulla. Työn vaiheet pitivät sisällään analysointityötä aktiivisten ja inaktiivisten käyttäjien rooleista, roolien poistoa inaktiivisilta käyttäjiltä sekä raportointia.

Olennaisena tuloksena havaittiin, että identiteetinhallinnan ja SAP-toiminnanohjausjärjestelmän välillä ilmeni eroavaisuuksia esimerkiksi käyttäjien sekä roolien lukumäärässä useammasta syystä. SAP-järjestelmän roolipaketteja haettiin sekä lisättiin käyttäjätunnuksille, joiden provisiointiprosessi ei ollut valmistunut täysin identiteetinhallinnassa. Tämä oli omiaan aiheuttamaan ongelmia. Myös yrityksen automatisoidussa deprovisiointiprosessin toiminnallisuudessa ilmeni puutteita. Lisäksi havaittiin, että rooleja oli lisätty käyttäjille tavoilla, joka eivät olleet nykyisen käytännön mukaisia.

Tuloksia hyödynnetään jatkokehityksessä, jossa ylimääräisten sekä väärinmyönnettyjen roolien poistoprosessia laajennetaan myös aktiivisten käyttäjien pariin.

Avainsanat: identiteetinhallinta, käyttöoikeudet, SAP, IDM, ERP

Abstract

Author:	Johanna Huotari
Title:	Data Synchronization between Identity Management and Enterprise Resource Platform
Number of Pages:	26 pages
Date:	5th of March 2024
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	Health Technology
Supervisor:	Mikael Soini, Principal Lecturer

The topic of the study was to observe the data flow between the identity management and the enterprise resource planning system SAP, alongside with the challenges that arise in it. In addition, it was essential to become familiar with the identity provisioning process, the various role entities within SAP and the various factors influencing these. The main goal was to synchronize the data between the two systems and to find out why data does not stay up to date.

The study was carried out between September 2023 and March 2024. A comprehensive picture of the extent of the problem was formed by collecting information from the Case company's internal materials, document analysis and open interviews. This included analyzing the roles of active and inactive users, removing roles from inactive users, and frequent reporting to relevant stakeholders.

As a significant result, it was found that differences between the identity management and the SAP were caused by several reasons. The role packages in SAP were requested for and added to user IDs whose provisioning process had not been fully completed in identity management, and this was apt to cause errors. The functionality of the Case company's automated deprovisioning process also showed deficiencies. Additionally, it was found that roles had been added to users in ways that did not conform to the current policy.

The results will be used in further development where the process of removing extra and wrongly assigned roles will also be extended to active users.

Keywords: Identity management, usage permissions, SAP, IDM, ERP

Sisällys

Lyhenteet ja käsitteet

AD: *Active Directory.* Microsoftin käyttäjätietokantapalvelu.

Autentikointi:
Käyttäjän identiteetin todentaminen.

CRM: *Customer Relationship Management.* Asiakkuudenhallinta.

Duplikaattirooli:
SAP-järjestelmän yksittäinen rooli, joka on lisätty käyttäjälle monta kertaa.

ERP: *Enterprise Resource Planning.* Toiminnanohjausjärjestelmä.

GUI: *Graphical User Interface*. Graafinen käyttöliittymä.

IAM: *Identity and Access Management.* Identiteetin- ja pääsynhallinta.

IDM: *Identity Management.* Identiteetinhallinta.

Komposiittirooli:
SAP-järjestelmässä käytetty roolikokonaisuus, joka sisältää useampia yksittäisiä rooleja.

Roolipaketti:
SAP-järjestelmässä käytetty roolikokonaisuus, joka voi sisältää sekä komposiittirooleja että yksittäisiä rooleja useampaan eri ympäristöön.

SAP: Case-yrityksessä käytetty toiminnanohjausjärjestelmä.

Yksittäinen rooli:

Käyttäjälle myönnettävä pääsyoikeus yhteen SAP-järjestelmän ympäristöön.

1 Johdanto

Kesällä 2021 Case-yrityksessä toteutettiin IT-projektin tietoteknisiä prosesseja koskeva auditointi. Auditointi tarkoittaa prosessien ja toimintojen objektiivista, riippumatonta (uudelleen)tarkastelua ja varmistusta, jonka tarkoituksena on parantaa organisaation toimintaa ja havainnoida mahdollisia olemassaolevia (tai potentiaalisia tulevia) riskejä. [1.]

Auditoinnin tuloksena tuli ilmi, että kahden oleellisen käytetyn järjestelmän välillä (identiteetinhallintajärjestelmä IDM:n sekä yrityksen toiminnanohjausjärjestelmä SAP:n) esiintyi ongelmia, jotka on korjattava. Identiteetinhallinnan pääsääntöinen tehtävä on muodostaa yrityksen työntekijöille käyttäjätunnus, eli identiteetti, ja välittää tietoa kohdejärjestelmiin (tässä tapauksessa SAP:n) siitä, kuka järjestelmään pyrkii kirjautumaan ja minkälaisilla valtuuksilla hänet on tarkoitus päästää käyttämään järjestelmän eri ominaisuuksia.

Ongelmien seurauksena SAP-järjestelmässä ilmenee eroavaisuuksia käyttäjien todellisissa käyttöoikeuksissa verrattuna IDM-järjestelmässä näkyviin hyväksyttyihin sekä asetettuihin käyttöoikeuksiin. Riskiksi muodostuu tällöin tilanne, joka ei noudata konsernin politiikkaa käyttöoikeuksiin liittyen *least privilege access approach* -periaatteeseen. Tämän periaatteen mukaan järjestelmän turvallisuusarkkitehtuuri on suunniteltava siten, että käyttäjälle myönnetään pienimmät ja vähimmäisimmät käyttövaltuudet järjestelmään, joita tarvitaan tehtävän täytäntöönpanemiseksi [2]. Liian laajat sekä tarpeettomat oikeudet mahdollistavat erilaiset väärinkäytökset – sekä tahalliset että tahattomat.

Tämä insinöörityö käsittelee pääasiassa erilaisia metodeja ja konkreettisia korjaustoimenpiteitä auditoinnin löydöksien suhteen ja perehtyy identiteetinhallinnan ja kohdejärjestelmä SAP:n välisiin ongelmiin sekä tietoteknisestä perspektiivistä että loppukäyttäjän kannalta. Toimeksiantajan

työntekijöiden tiukasta vaitiolovelvollisuudesta johtuen yritykseen viitataan työssä termillä *Case-yritys*. Konsernin sisäiset dokumentit ja muu runsaasti saatavilla ollut kirjallinen materiaali kuuluvat liiketoimintasalaisuuden piiriin.

2 Työn lähtökohdat

2.1 Identiteetinhallintajärjestelmä IDM

Identiteetinhallinnan hyödyntäminen Case-yrityksessä perustuu paikallisten lakien (mm. Sähköisen viestinnän tietosuojadirektiivi [3], EU:n tietosuoja-asetus GDPR [4] sekä GDPR:ää täsmentävä Helsingissä säädetty tietosuojalaki [5]) noudattamisen varmistamiseksi sekä Case-yrityksen sisäisten prosessien ja liiketoimintasalaisuuden toteutumisen turvaamiseksi.

Identiteetinhallintajärjestelmä IDM:n keskitetään tietoa yrityksen työntekijöistä ja tätä tietoa välitetään eri kohdejärjestelmiin. Identiteetinhallinnassa luodaan ja provisioidaan käyttäjälle identiteetti (käyttäjätunnus), jolla varmistetaan käyttäjän olevan aidosti yrityksen autorisoima työntekijä ja jonka avulla työntekijä kirjautuu yrityksen käyttämiin järjestelmiin ja palveluihin. Kaikki myönnetyt käyttöoikeudet perustuvat työntekijän, jolle muodostetaan identiteetti, sekä Case-yrityksen väliseen lailliseen sopimukseen (tyypillisesti työsopimus), jossa määritellään muodostettavan identiteetin pääsyoikeuksien tarve (työnimike tai eritellyt työtehtävät) [6].

Kun työntekijän työkuva muuttuu, vanhan työnkuvan mukaiset pääsyoikeudet on poistettava uuden työnkuvan mukaisten pääsyoikeuksien myöntämisen yhteydessä. Tällöin identiteetinhallinnasta lähetetään pyyntö kohdejärjestelmiin, joissa muutokset suoritetaan. Tämän jälkeen kohdejärjestelmä lähettää vahvistuksen onnistuneesta muutoksesta identiteetinhallintaan. Samaa toimenpidettä sovelletaan esimerkiksi työntekijän poistuessa yrityksen palveluksesta. Olemassaolevalle identiteetille suoritetaan deprovisiointi, eli käyttäjätunnuksen poistamisprosessi, jonka yhteydessä myös pyyntö käyttöoikeuksien poistamisesta ja käyttäjätietojen hävittämisestä välitetään

kohdejärjestelmiin, joka jälleen vahvistetaan identiteetinhallinnalle, kun pyydetyt toimenpiteet on suoritettu kohdejärjestelmässä.

Ideaalitilanteessa työkuvan muutokset ja tähän liittyvät roolien ja oikeuksien muutokset toimisivat automatisoituna prosessina. Case-yrityksen tapauksessa nämä hoidetaan manuaalisesti linjaesihenkilön toimesta. Ilman keskitettyä identiteetin- ja pääsyoikeuksienhallintaa ja sen tarjoamaa automatiikkaa (niiltä osin, joissa Case-yrityksen prosessi ei ole manuaalinen) yrityksen tietohallinto-osasto joutuisi hallinnoimaan sekä tallentamaan dataa että myöntämään pääsyoikeuksia manuaalisesti, mikä tarkoittaisi entistä suurempaa työmäärää, korkeampaa todennäköisyyttä inhimillisille virheille sekä alentunutta toiminnan tehokkuutta. [7]

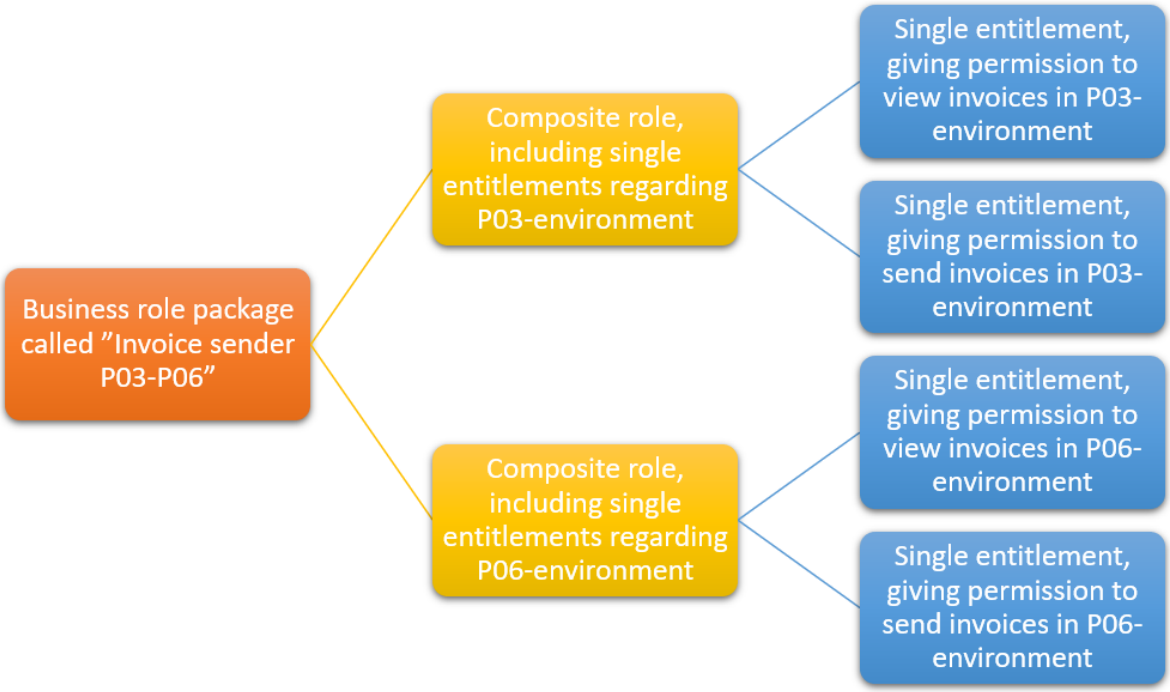
Automatiikka lisää kuitenkin myös potentiaalisia riskejä: tietovarkaudet sekä paikallisiin lakeihin ja autentikointiin eli identiteetin todentamiseen liittyvät riskit ovat omiaan kasvamaan sitä mukaa kuin identiteetinhallinnan automatisointia kasvatetaan organisaatiossa. [8]

2.2 ERP ja SAP

ERP (*Enterprice Resource Planning*) eli toiminnanohjausjärjestelmä on alusta, johon on keskitetty yrityksen eri osa-alueiden, esimerkiksi kirjanpidon, CRM:n eli asiakkuudenhallinnan, tuotannon tai tekoälyn, toimintoja useamman eri järjestelmän sijasta. Keskittämällä toimintoja saman järjestelmän alle voidaan minimoida monen eri järjestelmän tai sovelluksen ylläpitoon, henkilöstön kouluttamiseen sekä datan synkronointiin liittyviä kustannuksia. Oraclen mukaan [9] toiminnanohjausjärjestelmän käytön hyödyt näkyvät myös järjestelmien ja palvelujen skaalautuvuudessa, manuaalisen työn vähenemisessä sekä riskienhallinnassa. ERP:n käytössä ilmenee myös riskejä. Ongelmia on havaittu muuan muassa valitun järjestelmän vakauteen, datan eheyteen sekä sen käsittelyyn liittyen. [10.]

SAP on sekä yritys että Case-yrityksessä käytetty toiminnanohjausjärjestelmä: globaalisti SAP-järjestelmällä on yli 230 miljoonaa käyttäjää [11]. SAP-alkuperäisohjelmiston pohjalle on luotu myös globaali toiminnanohjausjärjestelmille suunnattu standardi [11, 12], joka määrittää vaatimukset sekä rakenteen yrityksille suunnatuille toiminnanohjausjärjestelmille. SAP:lla on lukuisia eri järjestelmäversioita [13], mutta tässä insinöörityössä keskitytään tarkastelemaan identiteetinhallinnan ohella SAP ERP:n graafiseen käyttöliittymään SAPgui:hin.

Jotta SAP:in käyttäjällä olisi mahdollisuus päästä käsiksi relevantteihin ympäristöihin, hänen käyttäjätunnukselleen tulee osoittaa yksi tai useampi roolipaketti (kokoelma komposiitti- sekä yksittäisiä rooleja, jotka myöntävät pääsyoikeudet eri ympäristöihin) identiteetinhallinnan kautta. Näitä on havainnollistettu kuvassa 1.



Kuva 1. Roolipakettien, komposiittiroolien sekä yksittäisten roolien sisältö ja suhde toisiinsa havainnollistettuna.

Kuvassa 1 näkyvä hypoteettinen roolipaketti ”Invoice sender P03-P06” tarjoaa käyttäjille, joilla tämä roolipaketti on myönnetty ja aktiivinen, pääsyn SAP-järjestelmän kahteen eri ympäristöön, P03:een sekä P06:een. Sen sisällä olevat komposiittiroolit sekä yksittäiset roolit myöntävät käyttäjälle luvan suorittaa erilaisia toimintoja, esimerkiksi laskujen tarkastelu (”*View invoices”)* sekä laskujen lähetys (”*Send invoices”*). Käyttäjä, jolla on laskujen tarkastelu- ja lähetysoikeus, ei voi samanaikaisesti toimia laskujen hyväksyjäroolissa. Case-yrityksen prosessi koskien SAP-oikeuksia ja rooleja pyrkii ehkäisemään näissä tilanteissa mahdollisia ristiriitaisten oikeuksien konfliktia sekä tahallisia että tahattomia väärinkäytöksiä.

2.3 Tietoturva

Identiteetinhallintajärjestelmän käyttöä sekä palvelujen keskittämistä yhden toiminnanohjausjärjestelmän, SAP:n, alle perustellaan tietoturvasyillä.

Tietoturva tarkoittaa yhtä metodia järjestelmän, datan, aineiston ja henkilöstön suojaamiseen. Tämä pitää sisällään erilaisia aktiviteetteja, joilla varmistua esimerkiksi tietosuojan (joka tietoturvasta poiketen taas merkitsee jokaisen perusoikeutta oikeudenmukaiseen henkilötietojen käsittelyyn ja niiden suojelemiseen) toteutumisesta sekä tähän liittyvien väärinkäytösten estämisestä. [14.]

Tietosuojan toteutumisen valvontaa ei olla jätetty ainoastaan yritysten toimintaan luottamisen vastuulle. Suomessa tietosuojan toteutumisen turvaamiseksi noudatetaan (jo *2.1 Identiteetinhallinta IAM* -luvussa esiteltyjä) erilaisia aihetta koskevia lakeja, kuten sähköisen viestinnän tietosuojadirektiiviä [3], EU:n tietosuoja-asetusta GDPR [4] sekä GDPR:ää täsmentävää Helsingissä säädettyä tietosuojalakia [5].

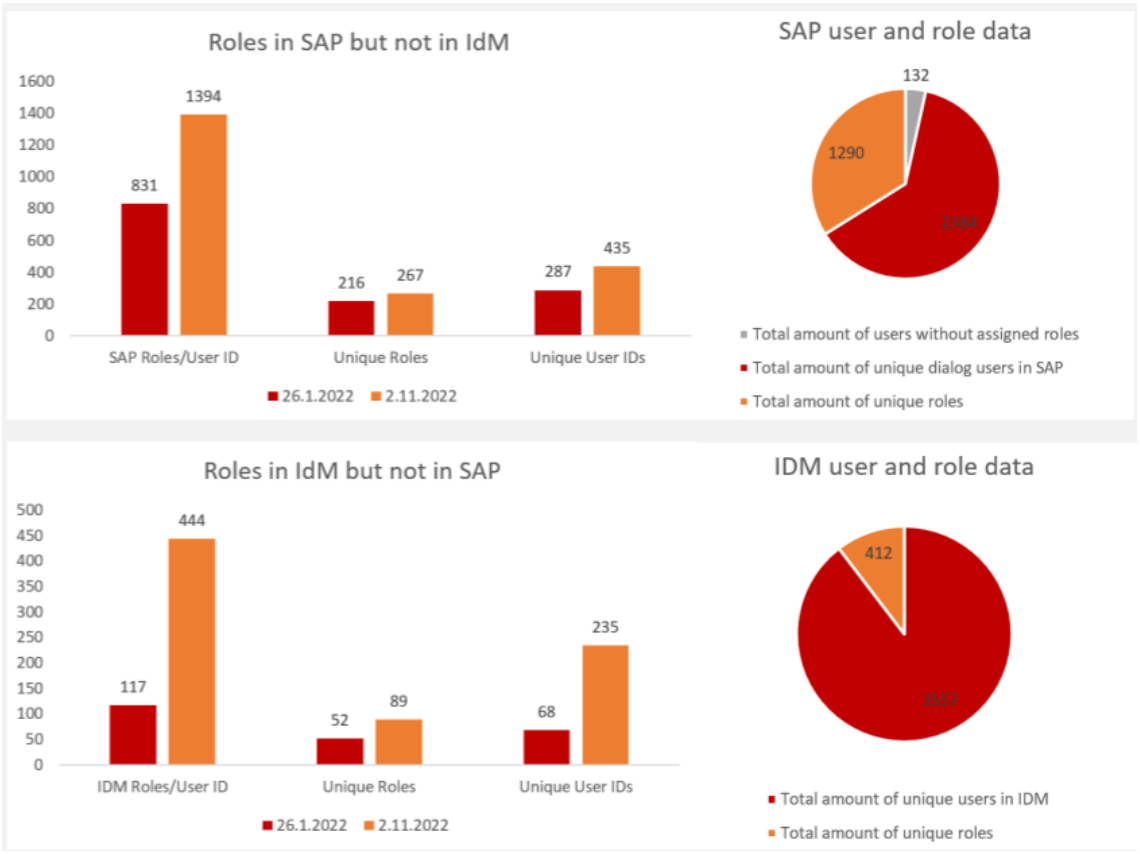
Tietoturvan kannalta on ratkaisevan tärkeää määritellä identiteettien vastuut sekä tunnistaa henkilö, joka haluaa tarkastella näitä tietoja. Tutkimuksen mukaan yrityksen on mahdollista pienentää merkittävästi identiteetinhallintaan liittyviä tietoturvariskejä valitsemalla ohjelmiston ja palveluntarjoajan

huolellisesti, kouluttamalla henkilöstönsä (sekä yrityksen sisäiset, että konsulttityöntekijät) perusteellisesti ja arvioimalla koko organisaation kypsyyttä sitoutua ja mukautua IAM-periaatteisiin ennen palvelun piiriin siirtymistä. [15]

2.4 Lähtötilanne

Auditoinnissa ilmitulleet ongelmalliset löydökset koskivat identiteetinhallinnan ja toiminnanohjausjärjestelmän välisiä ongelmia. Näitä olivat muun muassa roolien myöntämis- ja peruutusprosessien haasteet, duplikaattiroolien (tilanne, jossa käyttäjälle on myönnetty yksittäinen rooli, ja tämän lisäksi myös roolipaketti joka sisältää jo valmiiksi kyseisen yksittäisen roolin) ilmeneminen sekä tiedon ja datan kulun häiriöitä kahden kyseenomaisen järjestelmän välillä oheishaittoineen. Konkreettiseksi oheishaitaksi mainittakoon esimerkiksi yrityksen tuottavuuteen tai käyttäjien tietosuojaan liittyvät negatiiviset vaikutukset ja riskit. Myös leaver-prosessissa, eli käyttäjien deprovisioinnissa, on epäilty olevan edelleen haasteita, mutta tälle epäilylle ei saatu ennen työn aloittamista vielä varmistusta.

Kuvassa 2 havainnollistetaan sitä, kuinka tiedot käyttäjistä sekä rooleista eivät käytännössä ole ajan tasalla.



Kuva 2. Roolien lukumäärät sekä niiden eroavaisuudet kahdessa eri järjestelmässä.

Kuvasta 2 konkretisoituu, kuinka järjestelmien data ei ole synkronoitu. Erot kahden järjestelmän näkymissä olivat merkittäviä. IDM:n perspektiivistä rooleja oli olemassa marraskuussa 444 kappaletta, mutta SAP:ssa näkyviä rooleja oli samaan aikaan 1394 kappaletta. Tämän perusteella identiteetinhallinnassa siis ei näkynyt 950 roolia, mikä tarkoittaa merkittävää määrää vääristynyttä tietoa.

Tällä voi olla myös suuri kustannusvaikutus. Mikäli tämän vääristyneen tiedon perusteella tehtäisiin päätöksiä, esimerkiksi Case-yrityksen ostaessa lisenssipalveluita (joiden hinta määräytyy laajuuden perusteella), Case-yritys voisi maksaa turhan monesta laajemmasta lisenssistä. Merkittävässä määrässä tapauksista kevyempi ja halvempi lisenssi olisi riittävä käyttäjälle. Kevyemmän lisenssin sopivuus selviäisi ainoastaan poistamalla turhia olemassaolevia rooleja, ja tarkastelemalla, onko kaikille näille rooleille aidosti tarvetta.

Kuvasta on havaittavissa myös roolien ja identiteettien määrässä selvää kasvua vuoden 2022 aikana – erilaisille pääsyoikeuksille ilmeni jatkuvasti kasvavaa tarvetta, joka tarkoittaa myös kasvavia tiedonhallinnan haasteita, mikäli jo olemassaolevia haasteellisia löydöksiä ei saada hallintaan.

Syitä sille, miksi vuoden 2021 auditoinnissa havaittuja problemaattisia löydöksiä työstetään konkreettisesti vasta vuosien 2023-2024 vaihteessa, on useita. Case-yritys oli varannut työn edistämiselle henkilöstöresursseja konsulttiyrityksistä, jotka kuitenkin asian alkutaipaleelle saattamisen jälkeen joko vaihtoivat työtehtäviä tai koko työpaikkaa. Osalla ongelman korjaamiselle osoitetuista henkilöstöresursseista osoittautui olevan alempi taitotaso kuin osa korjaustoimenpiteistä olisi vaatinut. Henkilöstön vaihtuessa jo tehtyjä toimenpiteitä ei dokumentoitu ennen henkilön poistumista tarpeeksi kattavasti, jotta seuraavan henkilön tarttuessa tehtävään sujuvasta tiedonkulusta olisi voitu varmistua. Myös auditoinnin kohteena olleen projektin henkilöstö, vaiheet, vaatimukset, aikataulu ja resurssit muuttuivat niin oleellisesti, että näihin tarpeisiin vastaamista oli priorisoitava korkeammalle kuin auditoinnin löydöksien korjaamista.

Case-yrityksen toiminnan tehokkuuden varmistamiseksi molempien järjestelmien datan tulisi olla (sekä pysyä) synkronoituna, toisiaan vastaavien roolipakettien ja toimintojen oltava näkyvillä molemmissa järjestelmissä sekä tiedonkulun toimittava pitkälti automaattisesti. Myös käyttöoikeuspyyntöjen hyväksymisen sekä hylkäämisen tulisi toimia perustellusti suunnitellun prosessin mukaisesti.

Tiedon synkronoiminen kahden järjestelmän välillä on tärkeää monesta syystä. Jotta järjestelmien toimintaa ja käyttäjien lukumäärää voisi tarkastella (ja tarvittaessa kehittää), tarvitaan ajantasaista ja paikkaansapitävää tietoa. Tiedon läpinäkyvyys molemmista järjestelmistä käsin nopeuttaa muuta ongelmanratkaisua. Kun voidaan luottaa siihen, että molempien järjestelmien tiedot ovat ajan tasalla, niiden parissa työskenteleviä resursseja voidaan suoraan kohdistaa käsillä olevaan ongelmaan, synkronointiongelmien priorisoimisen sijasta. Myös turvallisuus on merkittävä tekijä synkronoinnissa.

Kansainvälinen dataintegraation parissa työskentelevä Talend kertoo [16], että datan epäonnistuneen synkronoinnin lopputuloksena yritys voi kohdata esimerkiksi viranomaismääräyksiin tai tietovuotoihin liittyviä ongelmia.

Käyttöoikeuksien myöntäminen tapahtui pitkään IDM-järjestelmän päädystä osin myös väärin perustein, eli vanhan prosessin mukaisesti. Tämän seurauksena kaikki SAP-järjestelmän roolit eivät olleet osittain tai lainkaan näkyvissä identiteetinhallinnassa. Tällaisia rooleja olivat yksittäiset roolit eli *single entitlementit*, usean yksittäisen roolin samaan toimintaympäristöön yhdellä kertaa myöntävät komposiittiroolit sekä business- ja IT-roolipaketit, jotka sisältävät pääsy- ja toimintaoikeuksia useaan eri ympäristöön.

2.5 Tutkimustavoitteet ja aiheen rajaaminen

Insinöörityön tutkimuskysymykset ovat seuraavat:

1. Miksi IDM- ja SAP-järjestelmien data ei pysy synkronoituna?
2. Kuinka saada käyttäjille myönnetyksi vain asianmukaisia roolipaketteja, sekä välttää tarpeettomien roolien myöntämistä?
3. Mistä duplikaattiroolit johtuvat?

Tavoitteina oli saada molemmat järjestelmät manuaalisesti ja perusteellisesti siivottua, kehittää toimintaprosessia yhtenäisten roolien manuaalisesta ja säännöllisestä tarkastamisesta, selvittää ongelmia hyväksyntäprosessissa, kehittää hyväksyntäprosessin ohjeistusta ja selvittää pyyntöjen hyväksyjien ongelmakohteita sekä tarpeita liittyen tilanteen parantamiseksi. Vaikkakin nämä tavoitteet ovat oleellisessa osassa insinöörityössä, työn pääfokus keskittyy tutkimuskysymysten ratkaisuun ja muut tavoitteet säilyvät sekondäärisellä prioriteetillä.

Aiheen keskittyessä IDM- sekä SAP-järjestelmien väliseen datan kulkuun ja synkronointiin, aiheesta rajattiin ulkopuolelle edellämainittujen järjestelmien parissa tiiviisti työskentelevän henkilöstön strukturoidut haastattelut. Vaikka käyttäjien näkemyksiä ja toiveita on tärkeää kuulla ja ottaa huomioon,

varsinaisten henkilökohtaisten haastattelusessioiden järjestäminen sekä niiden vastineiden analysointi veisi resursseja pois ongelman tekniseltä ratkaisulta. Juuri tämä tekninen ratkaisu on asia, mitä Case-yritys odotti insinöörityöltä, aiemman auditoinnin näkökulmasta.

Dataa siirtyi myös muihin Case-yrityksessä käytettyihin järjestelmiin IDM-järjestelmästä. Esimerkiksi hankinnan järjestelmä Coupa tai Microsoftin yhteistyöalusta SharePoint hyödynsivät käyttöoikeusprosessissaan identiteetinhallinnasta saatua dataa. Kuitenkin myös nämä kohdejärjestelmät rajattiin insinöörityön fokuksesta ulos, ja ensisijaisesti keskityttiin identiteetinhallinnan ja SAP:n yhteyteen sekä toimintaan. Tämä johtuu aikatauluhaasteesta sekä siitä, että auditoinnin löydökset ovat keskittyneet pääasiassa IDM-SAP-väliseen yhteyteen muiden kohdejärjestelmien sijasta.

Työn aikana jatkokehitykseen muita siirrettyjä osioita on käsitelty tarkemmin luvussa *6.2 Jatkokehitys*.

3 Menetelmät

Insinöörityön toteutus piti sisällään erilaisia tiedonkeruumenetelmiä: esimerkiksi palavereiden muistiinpanoja, sähköpostiketjuja eri sidosryhmien välillä, Case-yrityksen sisäisiä auditointia koskevia materiaaleja ja muuta jo olemassaolevaa aineistoa, avoimia haastatteluja yrityksen henkilöstölle. Myös dokumenttianalyysia hyödynnettiin muodostamaan monipuolinen ja kattava kuva tilanteesta sekä sen ratkaisuvaihtoehdoista.

Konkreettisen työn eri vaiheita havainnollistettu taulukossa 1.

Taulukko 1. Insinöörityön konkreettisen työn vaiheet

Vaihe 1: Suunnittelu	Vaihe 2: Analysointi	Vaihe 3: Korjaustoimet	Vaihe 4: Tulosten esittely	Vaihe 5: Jatkokehitys

Tausta-kartoitus, Dokumentti-analyysi, Aikataulu, etenemisen suunnittelu	Kategorisointi, avoimet haastattelut	Aktiviteettien delegointi tiimeille, turhien roolien poisto	Dokumentaatio auditoijille, ohjeistus loppukäyttäjille	Ylläpitotoimet, prosessien ja ohjeistuksen kehitys, monitorointi

Ensimmäisessä taulukossa näkyvässä kolmannessa vaiheessa mainitut aktiviteetit pitivät sisällään tikettien käsittelyä, problemaattisten käyttäjien tilanteen selvittelyä, identifioitujen syiden raportointia sekä turhien roolien poistoprosessin monitorointia. Taulukon kolmas vaihe oli konkreettisen työn aikaavievin osuus: sen päätökseen saattaminen oli pitkälti riippuvaista toisten tiimien toiminnasta ja aikataulusta. Identiteetinhallinnasta vastaavan tiimin kanssa työskentelyssä ilmeni hitautta sekä haasteita. Koko insinöörityön aikataulu jäi suunnitellusta jälkeen, ja jatkokehityksen piiriin oli siirrettävä huomattavan paljon enemmän tehtäviä, kuin vaiheessa 1 suunniteltu aikataulu piti sisällään. Näitä haasteita on kuvailtu tarkemmin luvussa 4.3 *Viestintä tiimien välillä*.

Ennen varsinaisen työskentelyn aloittamista oleellisena toimenpiteenä oli Case-yrityksen sisäiseen, ongelmaa käsittelevään, jo olemassaolevaan aineistoon tutustuminen. Tämän aineiston sisältöä on käsitelty laajemmin ongelman taustaan perehtyvässä alaluvussa *2.4 Lähtötilanne*.

Yhtenä oleellisena tapana varmistaa kattavan kuvan muodostaminen ongelman laajuudesta sekä erilaisista ratkaisuvaihtoehdoista oli saada perusteellinen koulutus SAP-järjestelmän oleellisiin tuotantoympäristöin, joihin tiedonkulun häiriöt pääasiassa keskittyivät. Koulutuksen, oheismateriaalit sekä tarvittavan käytön tuen järjesti Case-yrityksen IT-kehityksen ja arkkitehtuurin johtaja sekä hänen nimeämänsä yksittäinen aiheen parissa jo työskentelevä resurssi (tässä tapauksessa Authorizations-tiimin Service Manager).

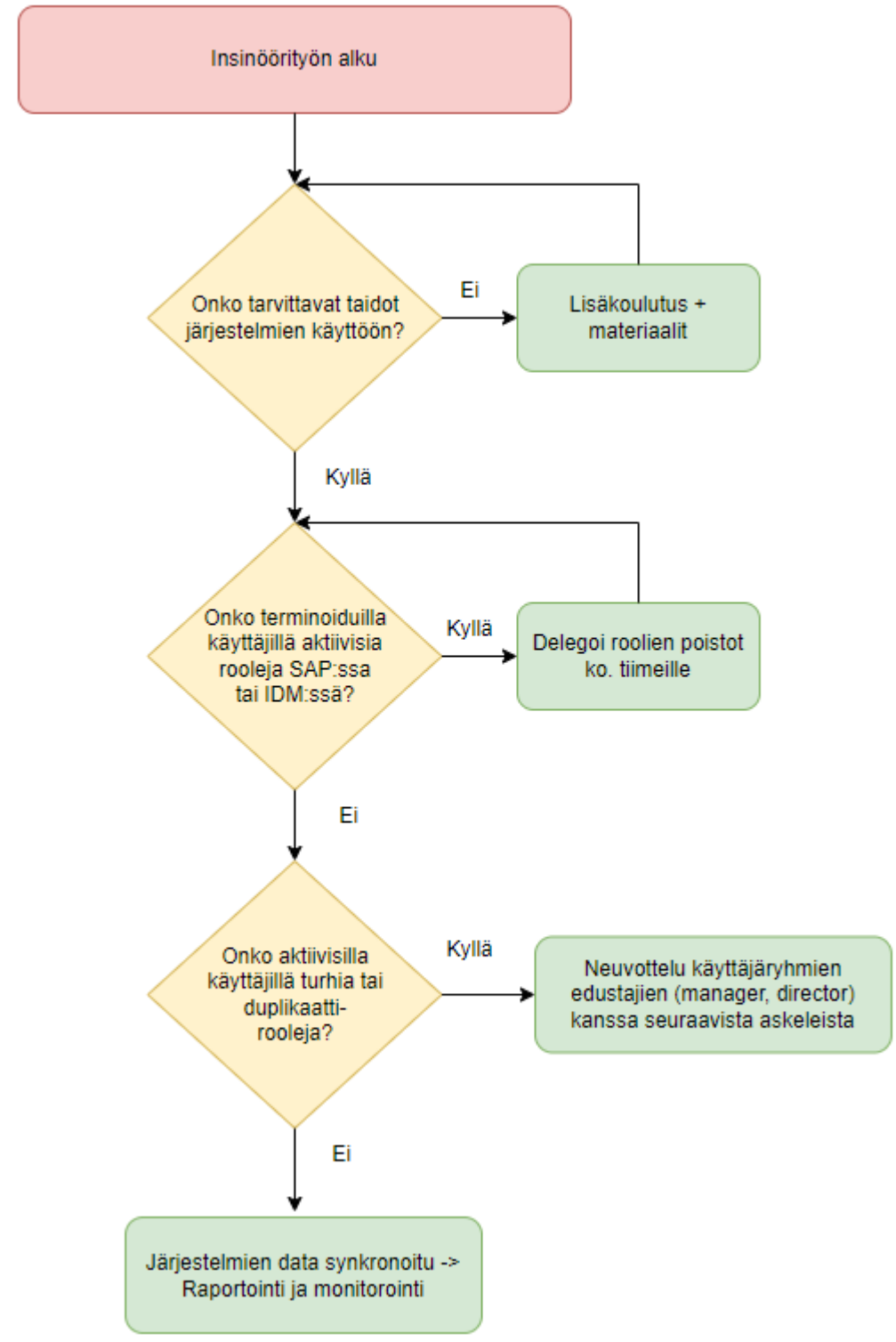
SAP-järjestelmää koskeva koulutus järjestettiin paikan päällä Case-yrityksen tiloissa autorisoinnin Service Managerin toimesta. Ennen koulutusta

varmistettiin tarvittavat pääsyoikeudet, jotka myönnettiin nopealla aikataululla. Koulutus piti sisällään SAP-järjestelmän eri toiminnallisuuksiin ja datan kulun prosessiin tutustumista, yleisimpiä virhetilanteita käyttäjien ja entitlementtien osalta sekä raportointia. Käytännön kokemusta IDM-järjestelmän tuotantoympäristöstä oli olemassa jo ennalta riittävästi ja tarvittavaa lisätietoa oli saatavilla Case-yrityksen sisäisistä ohjedokumenteista, joten erillistä varsinaista koulutusta identiteetinhallintaan liittyen ei katsottu tarpeelliseksi.

Konkreettisen työn edistymistä seurattiin viikottaisilla, pienemmän osallistujamäärän seurantapalavereilla. Näiden tarkoituksena oli nimensä mukaisesti seurata tarkasti lyhyen aikavälin edistysaskeleita. Kuukausittaisissa palavereissa taas keskiössä oli tarkastelussa pitkän aikavälin eteneminen, joissa taas raportoitiin etenemisestä auditoinnin parissa työskentelevälle sisäisen valvonnan johtajalle. Menetelmistä ja etenemisen järjestyksestä oli hiukan erilaisia näkökulmia ja toiveita IT:n sekä auditoinnin perspektiiveistä, joita käsitellään tarkemmin osiossa 4.3 *Viestintä tiimien välillä.*

Muihin tehtäviin ja menetelmiin tutkimuskysymyksiin vastaamisen edistämiseksi kuuluivat myös manuaaliset korjaustoimenpiteet puuttuvien yksittäisten roolien sekä roolipakettien osalta sekä SAP- että IDM-järjestelmässä, eritasoisia testaustoimenpiteitä (mukaanlukien aktiivisten sekä jo poistuneiden käyttäjien tunnuksien ja oikeuksien terminointi sekä näiden manuaalisten muutoksien vaikutusten havainnointi), mahdollisten uusien löydösten dokumentointi ja havaintojen säännöllinen raportointi.

Kuvassa 3 on perehdytty entistä tiiviimmin käytännön työn edistymiseen.



Kuva 3. Vuokaavio konkreettisen työn etenemisaskeleista.

4 Datan synkronointi

4.1 Analysointityö

Analysointityön, eli taulukossa 1 näkyvässä toisessa vaiheessa, voi jakaa kahteen osioon. Ensimmäiseen osioon siirryttäessä SAP-koulutuksen päätteeksi tarkasteltiin yhdessä Authorizations-tiimin Service Managerin kanssa kolmea eri Excel-tiedostoa. Näihin tiedostoihin oli koostettu listaukset terminoiduista (eli jo yrityksen palveluksesta poistuneista) käyttäjistä, joiden käyttäjätunnuksilla kuitenkin ilmeni olevan aktiivisia roolipaketteja, yksittäisiä rooleja sekä komposiittirooleja voimassa. Nämä aktiiviset turhat roolit olivat näkyvissä sekä IDM- sekä SAP-järjestelmien perspektiivistä katsoen. Kunkin käsiteltävän Excel-tiedoston käyttäjäryhmät oli eroteltu kolmen eri ympäristön käyttäjiin.

Suuren tietomäärän vuoksi oli luontevaa lähteä asettamaan dataa erilaisiin kategorioihin, ja seuraavassa vaiheessa tehdä korjaustoimenpiteitä johdonmukaisesti kategoria kerrallaan. Analysointityön ensimmäisessä osiossa (terminoitujen käyttäjien aktiiviset roolit) ilmenneitä tilanteita on kategorisoitu taulukkoon 2.

Taulukko 2. Analysointityön ensimmäisen osion kategoriat (inaktiiviset käyttäjät)

Kategorian nimi	Selite
Poistettu käyttäjä, roolit yliviivattu IDM:ssä, käyttöoikeudet päättyneet SAP:ssä ja roolit vielä paikoillaan	• Käyttäjän aktiivisuuden status IDM-järjestelmässä on ”poistettu” • Kyseenomainen yksittäinen rooli näkyy yliviivattuna, eli inaktiivisena, IDM:ssä • Käyttäjätunnuksen voimassaolo SAP-järjestelmässä on umpeutunut • Kyseenomainen yksittäinen rooli näkyy aktiivisena SAP:ssa

Terminoitu käyttäjä, roolit yliviivattu IDM:ssä, käyttöoikeudet päättyneet SAP:ssä ja roolit vielä paikoillaan	• Käyttäjän aktiivisuuden status IDM-järjestelmässä on ”terminoitu” • Kyseenomainen yksittäinen rooli näkyy yliviivattuna, eli inaktiivisena, IDM:ssä • Käyttäjätunnuksen voimassaolo SAP-järjestelmässä on umpeutunut • Kyseenomainen yksittäinen rooli näkyy aktiivisena SAP:ssa
Terminoitu käyttäjä, business-roolipaketti aktiivisena IDM:ssä, käyttöoikeudet päättyneet SAP:ssä ja roolit vielä paikoillaan	• Käyttäjän aktiivisuuden status IDM-järjestelmässä on ”terminoitu” • Kyseenomainen business-roolipaketti näkyy aktiivisena IDM:ssä • Käyttäjätunnuksen voimassaolo SAP-järjestelmässä on umpeutunut • Kyseenomainen yksittäinen rooli näkyy aktiivisena SAP:ssa
Duplikaattirooli, terminoitu käyttäjä, roolit yliviivattu IDM:ssä, käyttöoikeudet päättyneet SAP:ssä ja roolit vielä paikoillaan	• Käyttäjällä on useampi samanlainen rooli aktiivisena • Käyttäjän aktiivisuuden status IDM-järjestelmässä on ”terminoitu” • Kyseenomainen yksittäinen rooli näkyy yliviivattuna, eli inaktiivisena, IDM:ssä • Käyttäjätunnuksen voimassaolo SAP-järjestelmässä on umpeutunut • Kyseenomainen yksittäinen rooli näkyy aktiivisena SAP:ssa
Poistettu käyttäjä, roolit aktiivisena IDM:ssä, käyttöoikeudet päättyneet SAP:ssä ja roolit vielä paikoillaan	• Käyttäjän aktiivisuuden status IDM-järjestelmässä on ”poistettu”

	• Kyseenomainen yksittäinen rooli näkyy aktiivisena IDM:ssä • Käyttäjätunnuksen voimassaolo SAP-järjestelmässä on umpeutunut • Kyseenomainen yksittäinen rooli näkyy aktiivisena SAP:ssa
Terminoitu käyttäjä, roolit aktiivisena IDM:ssä, käyttöoikeudet päättyneet SAP:ssä ja roolit vielä paikoillaan	• Käyttäjän aktiivisuuden status IDM-järjestelmässä on ”terminoitu” • Kyseenomainen yksittäinen rooli näkyy aktiivisena IDM:ssä • Käyttäjätunnuksen voimassaolo SAP-järjestelmässä on umpeutunut • Kyseenomainen yksittäinen rooli näkyy aktiivisena SAP:ssa

Taulukosta 2 voi havaita, että terminoiduilla sekä poistetuilla käyttäjillä ilmenee edelleen olevan vielä runsaasti paikallaan olevia rooleja. Tämä löydös tukee jo luvussa *2.4 Lähtötilanne* mainittua oletusta, jonka mukaan Case-yrityksen Leaver-prosessi eli identiteettien deprovisiointiprosessi ei toimi, korjaustoimenpiteistä huolimatta. Mikäli prosessi olisi automatisoitu sekä toimiva, taulukon mukaisia roolilöydöksiä inaktiivisilta identiteeteiltä ei pitäisi olla mahdollista löytyä.

Analysointityön toisen osion keskiössä olivat aktiiviset, vielä Case-yrityksen palveluksessa työskentelevät henkilöt, joilla ilmeni vanhentuneen prosessin mukaisesti myönnettyjä yksittäisiä rooleja, roolipakettien (ks. kuva 2) sijasta. Kuten inaktiivisten käyttäjien suhteen toimittiin analysointivaiheen ensimmäisessä osiossa, myös aktiiviset käyttäjät ja heidän käyttöoikeutensa oli listattu Excel-tiedostoon ja suuri tietomäärä jaettiin kategorioihin. Kategorioita sekä niiden sisältöä on avattu taulukossa 3.

Taulukko 3. Analysointivaiheen toisen osion kategoriat (aktiiviset käyttäjät)

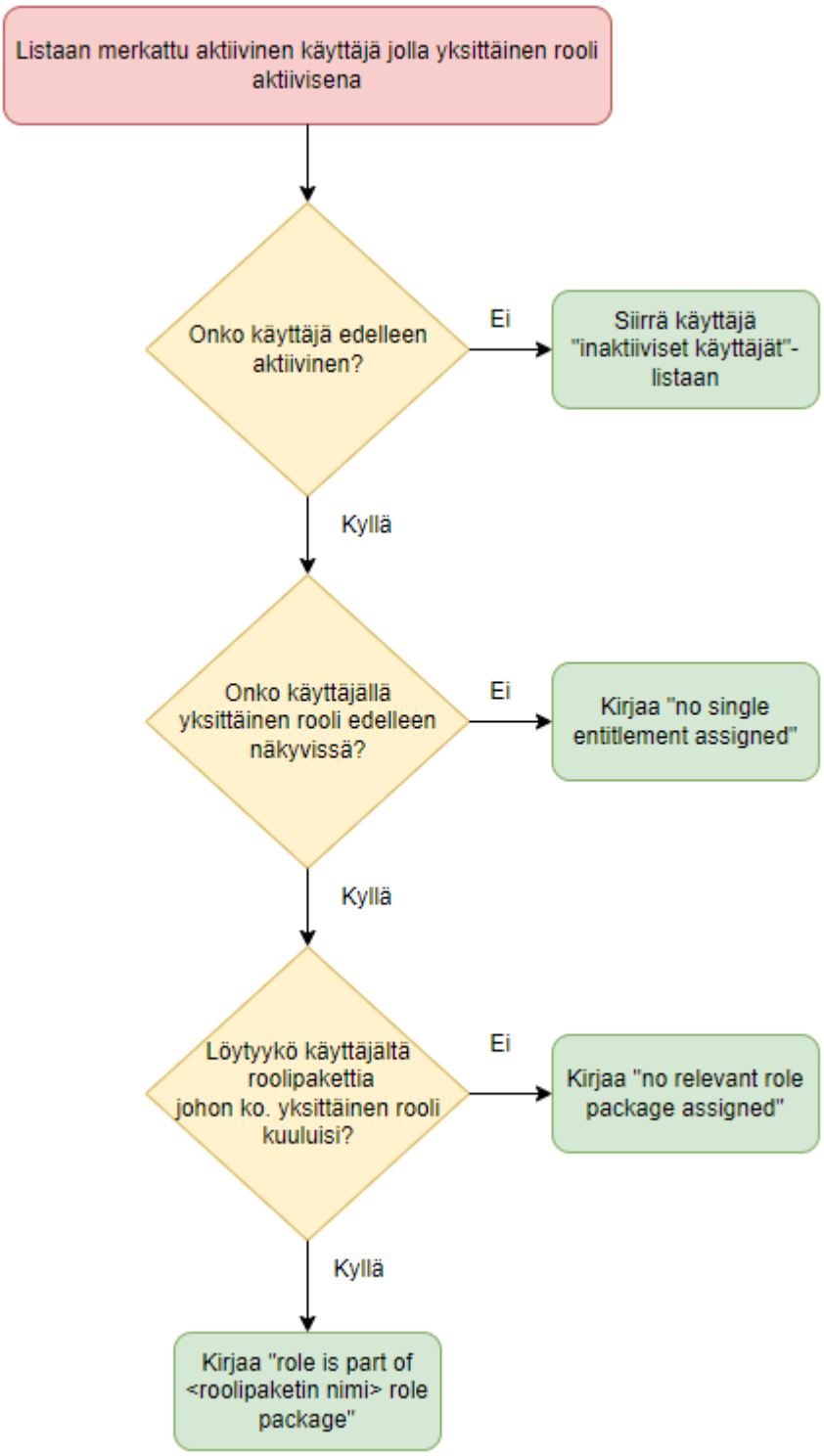
Kategorian nimi	Selite
Komposiittirooli, aktiivinen IDM:ssä, ei relevanttia roolipakettia *assigned*	• Käyttäjällä on aktiivinen komposiittirooli näkyvissä identiteetinhallinnassa • Kyseenomainen komposiittirooli on roolipaketin ulkopuolella, sopivaa roolipakettia ei ole myönnetty käyttäjälle
Yksittäinen rooli, aktiivinen IDM:ssä, ei relevattia roolipakettia *assigned*	• Käyttäjällä on yksi tai useampi yksittäinen aktiivinen rooli näkyvissä identiteetinhallinnassa • Rooli(t) ovat roolipaketin ulkopuolella, sopivaa roolipakettia ei ole myönnetty käyttäjälle
Yksittäinen rooli, inaktiivinen IDM:ssä, ei relevanttia roolipakettia *assigned*	• Käyttäjällä on yksi tai useampi yksittäinen inaktiivinen (yliviivattu) rooli näkyvissä identiteetinhallinnassa • Rooli(t) ovat roolipaketin ulkopuolella, sopivaa roolipakettia ei ole myönnetty käyttäjälle
Terminoitu/poistettu käyttäjä	• Käyttäjä virheellisesti listattu aktiivisten käyttäjien listaan
Yksittäinen rooli, ei näkyvissä IDM:ssä	• Listan mukaan käyttäjälle on myönnetty yksi tai useampi yksittäinen (roolipaketin ulkopuolinen) rooli, mutta tätä ei ole näkyvissä identiteetinhallinnassa
Yksittäinen rooli, aktiivinen IDM:ssä, käyttäjällä relevantti roolipaketti	• Käyttäjällä on yksi tai useampi yksittäinen aktiivinen rooli näkyvissä identiteetinhallinnassa • Käyttäjällä on tämän lisäksi myös sopiva roolipaketti myönnetty ja aktiivisena

Taulukossa 3 näkyvistä kategorioista kolmessa ensimmäisessä kategoriassa aktiivisella käyttäjällä oli vanhentuneen prosessin mukaisesti myönnettyjä yksittäisiä rooleja, ja heiltä puuttui roolipaketti, johon kyseenomainen yksittäinen rooli olisi kuulunut. Näiltä käyttäjiltä ylimääräistä yksittäistä roolia ei voi poistaa suoraan, vaan oli sovittava seuraavista toiminta-askeleista ja asianmukaisten roolipakettien lisäämisestä käyttäjäryhmien edustajien kanssa. Tällä haluttiin välttää tilanne, jossa käyttäjien järjestelmien käyttöoikeuksiin ilmenisi katkoksia ja heidän työtehtävänsä keskeytyisivät väliaikaisesti.

Neljänteen kategoriaan sisällytettiin käyttäjät, jotka olivat ehtineet poistua yrityksen palveluksesta ennen kuin aktiivisten käyttäjien lista luotiin, tai inaktiivisia käyttäjiä päätyi listalle inhimillisen erehdyksen vuoksi. Heidät lisättiin taulukossa 2 käsiteltyihin kategorioihin. Viidennessä kategoriassa olivat käyttäjät, joilla yksittäisiä rooleja ei ollut enää näkyvissä, eli heidän tilanteensa oli prosessin mukainen ja muutoksia heidän käyttöoikeuksiinsa ei enää tarvittu. Nämä käyttäjät poistettiin listalta.

Viimeisessä kategoriassa käyttäjällä oli asetettuna prosessinmukainen roolipaketti, sekä sen lisäksi vanhan prosessin mukaisesti lisätty yksi tai useampi yksittäinen rooli. Nämä roolipaketin ulkopuoliset yksittäiset roolit tuli poistaa.

Kategorioihin jakamisen prosessia on kuvattu tarkemmin kuvassa 4.



Kuva 4. Vuokaavio aktiivisten käyttäjien yksittäisten roolien käsittelyprosessista.

Kuvassa 4 näkyvien vihreiden osioiden jälkeisiä toimenpiteitä käsitellään tarkemmin osiossa 4.2 *Virheellisen datan siivous.*

4.2 Virheellisen datan siivous

Kun analysointivaiheiden kategorisointi käyttäjien tilanteesta oli suoritettu, inaktiivisten käyttäjien listan eri kategorioista luotiin käsittelypyynnöt Service Now -järjestelmän kautta roolien poistamiseksi. Pyynnöt delegoitiin SAP-järjestelmästä sekä identiteetinhallinnasta vastaaville tiimeille, jotka poistivat rooleja käyttäjiltä omista kohdejärjestelmistään.

SAP-järjestelmää koskeva pyyntö piti sisällään 15 käyttäjää. Kaikki pyydetyt roolit saatiin poistettua kaikilta 15 käyttäjältä alle vuorokaudessa. IDM-järjestelmän osuus osoittautui mutkikkaammaksi, sillä roolit eivät poistuneet odotetusti. Roolien poistamiseksi tehtiin useampi roolien poistokierros, ja jokaisen kierroksen jälkeen käyttäjät ja heidän roolinsa tarkastettiin manuaalisesti identiteetinhallinnasta uudestaan.

Ensimmäiseen poistokierrokseen aikaa kului noin 1,5 kuukautta ja kolmeen viimeiseen n. 2-3 viikkoa/kierros. IDM-tiketin eri poistokierrosten etenemistä käyttäjien osalta on havainnollistettu taulukossa 4.

Taulukko 4. IDM-pyynnön käsittelykierrosten eteneminen

Kierros 1	Ympäristö P01: 173 inaktiivista käyttäjää joilla poistettavia rooleja	Ympäristö P34: 121 inaktiivista käyttäjää joilla poistettavia rooleja	Ympäristö PG1: 47 inaktiivista käyttäjää joilla poistettavia rooleja
Kierros 2	Ympäristö P01: 111 inaktiivista käyttäjää joilla poistettavia rooleja	Ympäristö P34: 51 inaktiivista käyttäjää joilla poistettavia rooleja	Ympäristö PG1: 9 inaktiivista käyttäjää joilla poistettavia rooleja
Kierros 3	Ympäristö P01: 23 inaktiivista käyttäjää joilla poistettavia rooleja	Ympäristö P34: 7 inaktiivista käyttäjää joilla poistettavia rooleja	Ympäristö PG1: 1 inaktiivinen käyttäjä jolla poistettavia rooleja
Kierros 4	Ympäristö P01: 21 inaktiivista	Ympäristö P34: 6 inaktiivista	Ympäristö PG1: 1 inaktiivinen

	käyttäjää joilla poistettavia rooleja	käyttäjää joilla poistettavia rooleja	käyttäjä jolla poistettavia rooleja

Taulukosta nähdään, että inaktiivisten käyttäjien roolien poisto on ollut haastavaa. Toistuvista yrityksistä huolimatta rooleja ei ole saatu täysin poistettua, vaan käyttäjien lukumäärä, joiden roolit ovat jääneet poistoprosessista huolimatta olemassaoleviksi, vähenee epäsäännöllisesti kierrosten edetessä. Tällaisiin roolien poistamisen haasteisiin ei osattu varautua aikataulua suunnitelessa ensimmäisessä vaiheessa, ja tämä oli omiaan vaikuttamaan myös insinöörityön aikana tartuttaviin ongelmiin. Syitä sille, miksi roolien poistamisen prosessi estyy kerta toisensa jälkeen, saatiin hyvin rajatusti.

4.3 Viestintä tiimien välillä

Insinöörityön ollessa alkutekijöissään pidettiin ongelman sidosryhmiä koskeva palaveri, jossa käsiteltiin muun muassa insinöörityön ajalle varattujen resurssien käyttöä, tehtävien- ja vastuunjakoa, viestinnän ja edistymisen dokumentoinnin toimintamalleja sekä mahdollisten virhe- ja kriisitilanteiden prosessia.

Auditoinnin perspektiivistä haluttiin aloittaa pienestä spesifistä alueesta, joka olisi nopeasti hoidettu ja josta olisi saatu konkreettista näyttöä etenemisestä auditoijille sekä johtoryhmälle asian etenemisestä, sillä auditoinnissa ilmitulleille ongelmallisten löydösten korjaamiselle oli annettu määräajaksi vuoden 2023 loppu. Kuitenkin eri osapuolet löysivät yhteisen sävelen ja päättivät, että strukturoitu, järjestelmällinen eteneminen aloittaen perusmuotoisista ongelmakäyttäjistä järjestelmä kerrallaan toisi pidemmällä aikavälillä ratkaisun, jota olisi helpompi ylläpitää. Yhdessä katsottiin, että yksinkertaisempiin ongelmatilanteisiin tarttuminen voisi auttaa myös kahden järjestelmän välisen datankulun ymmärtämistä, johon olisi luontevaa lisätä asteittain haastavampien lieveilmiöiden korjaamista.

Kun analysointityön ensimmäinen vaihe oli tehty, tarvittiin apua SAP-järjestelmän ja identiteetinhallinnan parissa työskenteleviltä tiimeiltä. SAP-

järjestelmän parissa työskentelevän Service Managerin kanssa analysointityön vaiheista, haasteista sekä erilaisista vaadituista toimista viestintä sujui mutkattomasti: yhteydenpito oli viikottaista ja työote proaktiivista sekä tukea ongelmatilanteisiin sai nopealla aikataululla.

Roolien poistamisprosessin etenemisestä, ongelmien juurisyistä tai haasteista ei toiselta asianomaiselta tiimiltä saatu lukuisista yrityksistä huolimatta kommenttia. Toimintojen toteutuksen vasteaika oli usein pidempi kuin luvattiin ja läpinäkyvyyttä toiminnasta tarjottiin vähäisesti. Mahdollisia syitä tälle on esitetty muun muassa kyseenomaisen tiimin ylityöllistyneisyys resurssipulan vuoksi, tiukka aikataulu sekä ympäristöjen uudelleentestaukseen ja uudistamiseen tarvittavan rahoituksen puute. Tiimin jäseniä yritettiin tavoitella Teams-viestien, sähköpostin sekä tikettijärjestelmän välityksellä, mutta vastauksia näihin saatiin harvoin, jos ollenkaan.

5 Tulokset

Uusi auditointi koskien identiteetinhallintaa ja toiminnanohjausjärjestelmää siirrettiin vuodenvaihteesta 2023-2024 maaliskuuhun 2024, joka myös saattoi insinöörityön päätökseensä.

Konkreettisesti ”Mistä duplikaattiroolit johtuvat?” -tutkimuskysymykselle löydettiin vastaus syyskuussa 2023. IT-projektin aikaisempien vaiheiden aikaan prosessi oli erilainen ja roolit myönnettiin eri tavalla (ennen IDM-työkalun varsinaista käyttöönottoa oli mahdollista lisätä yksittäisiä rooleja suoraan SAP-järjestelmään, sekä IDM:n että SAP:n puolella). Kun Case-yrityksessä siirryttiin nykyiseen prosessiin ja identiteetinhallinnan piiriin (roolipakettien käyttöönotto, roolit haetaan IDM:n kautta josta tieto siirtyy SAP:iin), resursseja ei kohdennettu jo olemassaolevien, vanhentuneen prosessin mukaisesti myönnettyjen yksittäisten roolien poistamiseen. Näin ollen käyttäjillä oli jo olemassa rooleja, ja lisäksi he saivat roolipaketteja (jotka sisälsivät jo ennaltamyönnetyt roolit), jolloin syntyi duplikaattirooleja. Analysointityön perusteella kasattiin listoja

päällekkäisistä rooleista, ja kohdejärjestelmien parissa työskenteleviä tiimejä ohjattiin poistamaan näitä duplikaattirooleja.

Marraskuussa 2023 havaittiin tekijä, joka osittain selittää ”Miksi IDM- ja SAP-järjestelmien data ei pysy synkronoituna?” tutkimuskysymystä. Havaittiin, että AD collection (eli aktiviteetti, joka synkronoi tiedot Active Directoryn ja identiteetinhallinnan välillä) päivittyy kahdesti vuorokaudessa – noin kello 12 päivällä sekä 2.15 aamuyöllä (Suomen aikaa). Mikäli SAP-oikeuksia haetaan ja lisätään käyttäjälle ennen kuin tämän Active Directory-käyttäjätunnus on muodostunut täysin (sAMAccountname-attribuutti puuttuu identiteetinhallinnassa), tunnus muodostuu SAP-järjestelmään vajaavaisilla tiedoilla. Tämä johtaa tilanteeseen, jossa SAP lisää automaattisesti käyttäjän käyttäjätunnuksen eteen ”ACC”-liitteen.

Etuliitteen johdosta identiteetinhallinta ei tunnista käyttäjätunnusta samaksi käyttäjäksi, jonka provisiointiprosessi on jo aloitettu, ja katsoo, ettei aloitetun identiteetin provisiointi ole valmis eikä oikeuksia ole lisätty. Tällöin vastikään lisätyt SAP-oikeudet eivät ole näkyvissä identiteetinhallinnassa, vaikka SAP:n näkökulmasta oikeudet ovat paikallaan. Tämä on vältettävissä ohjeistamalla eri sidosryhmiä tarkastamaan käyttäjätunnuksen valmistuminen AD collectionin päivittymisen jälkeen ennen SAP-oikeuksien hakemista uusille käyttäjille.

Roolien hyväksymisprosessissa ja -toiminnoissa esiintyi aikaisemmin viiveitä, sillä avoimien haastattelujen sekä epävirallisen tiedonkeruun perusteella hyväksyjät eivät välttämättä saaneet asiaankuuluvaa sähköposti-ilmoitusta hyväksyntää odottavista pyynnöistä. He eivät tienneet tai ymmärtäneet pyydettävien roolien tarkoitusta ja/tai laajuutta taikka olleet varmoja siitä, kuuluuko vastuu pyynnön hyväksynnästä primääriselle vai sekundääriselle hyväksyjälle. Nämä epäselvyydet voivat johtua eri tekijöistä. Case-yrityksen prosessin dokumentaatio ei ollut tarpeeksi selkeä hyväksyjille, materiaalia ei ollut saatavilla kyseisille henkilöille tai sitä ei syystä tai toisesta luettu, ajantasaista tietoa uusien roolipakettien sisällöstä ja/tai laajuudesta ei välittynyt, joten hyväksyjät saattoivat toimia vanhentuneen tiedon varassa.

”Kuinka saada käyttäjille myönnetyksi vain asianmukaisia roolipaketteja, sekä välttää tarpeettomien roolien myöntämistä?” tutkimuskysymykseen vastaukseksi todettakoon, että hyväksyjille on taattava prosessinmukainen ymmärrys pyyntöjen sisällöstä ennen niiden hyväksymistä, jotta tarpeettomien tai liian laajojen oikeuksien myöntämiseltä voidaan välttyä.

Luku *4.1 Analysointityö* sekä taulukon 2 sisältö osoittavat, että yrityksen identiteettien deprovisiointiprosessissa osoittautuu olevan merkittäviä puutteita, sen automatiikka ei ole luotettava ja ongelmallisten löydösten manuaalinen poistaminen identiteetinhallinnasta on osoittautunut haastavaksi. Deprovisioinnissa ilmenevät puutteet ovat omiaan altistamaan Case-yrityksen kohdejärjestelmät ja käyttäjät sekä tietoturvaan että oikeuksien väärinkäyttöön liittyville uhille.

6 Yhteenveto

6.1 Arviointi

Työllä pyrittiin havinnoimaan identiteetinhallinnan sekä SAP-järjestelmän välisen datan eroavaisuuksia, synkroinoimaan näiden järjestelmien tiedot sekä selvittämään erilaisia syitä eroavaisuuksille. Tämän pyrkimyksen toteuttamiseksi tutustuttiin olemassaolevaan aikaisempien auditointien yhteydessä laadittuun aineistoon, teetettiin analysointityö aktiivisten ja jo terminoitujen käyttäjien osalta. Lisäksi luotiin ja delegoitiin roolien poistopyyntöjä analysoinnin pohjalta synkronoinnin toteuttamiseksi.

Työn aikana havaittiin, että deprovisiointiprosessi ei toimi aiemmista dokumentoiduista korjausyrityksistä huolimatta. Myös SAP-järjestelmässä käyttäjätunnusten eteen ilmestyneille ”ACC”-teksteille löydettiin syy. Analysointityö saatiin onnistuneesti aikataulussa valmiiksi ja tätä voidaan hyödyntää seuraavalla auditoinnin kierroksella joka alkaa maaliskuussa 2024. Myös tutkimuskysymyksiin onnistuttiin vastaamaan työn määrittelemässä aikataulussa. Kuitenkin aktiivisten käyttäjien osalta roolien konkreettinen

poistaminen jäi vielä neuvotteluvaiheeseen. Jotta tämä olisi voitu toteuttaa, työn aikataulua olisi tullut pidentää merkittävästi, sillä roolien poistoprosessi sisältää useamman kierroksen, ja roolien todellinen poistuminen on tarkastettava manuaalisesti. Toinen vaihtoehto olisi ollut useampien henkilöresurssien lisääminen aiheen pariin.

Mikäli työtä ei olisi suoritettu, Case-yritys ei olisi voinut vastata auditoinnin toteuttaneiden tarkastajien vaatimuksiin konkreettisten korjaustoimenpiteiden esittämisestä annetussa aikataulussa.

6.2 Jatkokehitys

Ennen insinöörityön virallista aloitusta sidosryhmät pohtivat, toimiiko case-yrityksen parhaaksi ja automatisoiduimmaksi prosessiksi kehuttu Leaver-prosessi, eli käyttäjän deprovisiointi, oikein – ja jos ei, onko poistuneen käyttäjän statuksella (”*Terminated*” vai ”*Deleted*”) merkitystä liittyen siihen, jäävätkö roolit (jolloin myös lisenssit ja niiden maksut) aktiiviseksi tarpeettomasti. Leaver-prosessin haasteisiin perehtyminen, poistumisstatuksen merkityksen selvittäminen sekä ongelmakohtien korjaaminen jouduttiin kuitenkin jättämään jatkokehityksen piiriin, sillä yrityksellä ei ollut resursseja asian perusteelliseen korjaamiseen insinöörityön aikataulun puitteissa.

Loppuosa tutkimuskysymykseen ”Miksi IDM- ja SAP-järjestelmien data ei pysy synkronoituna?” vastauksesta rajataan jatkokehityksen piiriin: vastineita kysymyksiin identiteetinhallinnasta vastaavalta tiimiltä ei saatu aikataulussa. Myös kaikkiin ongelmiin ei löydetty syytä tai ongelmaan ajankohtaisesti vaikuttavia tekijöitä ei saatu identifioitua siinä laajuudessa, kuin alunperin olisi toivottu, sillä näkökulma identiteetinhallinnan puolelta puuttui lähes täysin. Kun vastineita saadaan identiteetinhallinnan puolelta, asian selvittäminen ja korjaustoimet jatkuvat.

Hyväksyjä-roolissa työskentelevän henkilöstön uudelleenkouluttaminen muutaman vuoden välein on tarpeellista, mikäli roolien hyväksyntäprosessissa,

roolipakettien sisällössä tai järjestelmissä ilmenee muutoksia, tai mikäli käyttäjän työtehtäviin kuuluu niin harvoin roolien hyväksyntään liittyviä aktiviteetteja, että yksityiskohdat on mahdollista unohtaa niiden välissä. Jatkokehityksessä tarkastellaan tähän liittyen uudelleenkouluttamisen mahdollisuutta, ohjeistusmateriaalin sekä prosessin kehittämistä, tilanteen monitorointia ja tehokkaampaa viestintää loppukäyttäjien suuntaan.

Seuraavina konkreettisina askeleina on aktiivisien käyttäjien yksittäisten, vanhentuneen prosessin mukaisten oikeuksien poisto, relevanttien roolipakettien myöntäminen poistettujen roolien tilalle sekä tilanteen seuranta ja ylläpito.

Lähteet

1 Pitt, Sally-Anne. 2014. Internal Audit Quality. E-kirja. <https://jabatanfungsionalauditor.files.wordpress.com/2016/06/internal-audit-quality-developing-a-quality-assurance-and-improvement-program.pdf>. Luettu 15.2.2024.

2 Dempsey, Kelley; Nieles, Michael; Yan Pillitteri, Victoria. 6/2017. An Introduction to Information Security. National Institute of Standards and Technology. Verkkojulkaisu. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf>. Luettu 16.1.2024.

3 Euroopan parlamentti ja Euroopan unionin neuvosto. 19.12.2009. Sähköisen viestinnän tietosuojadirektiivi. EUR-Lex. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32002L0058>. Luettu 7.2.2024.

4 Euroopan parlamentti ja Euroopan unionin neuvosto. 27.4.2016. EU:n tietosuoja-asetus GDPR. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC>. Luettu 7.2.2024.

5 Suomen eduskunta. 5.12.2018. Tietosuojalaki 1050/2018. Finlex. <https://www.finlex.fi/fi/laki/alkup/2018/20181050>. Luettu 7.2.2024.

6 Case-yritys. Identity and Access Management Policy (en). Sisäinen dokumentti. Luettu 7.2.2024.

7 BizTech. 7.9.2016. 3 Reasons to Deploy an Identity and Access Management (IAM) Solution. Verkkoartikkeli. <https://biztechmagazine.com/article/2016/09/3-reasons-deploy-identity-and-access-management-solution>. Luettu 8.2.2024.

8 Chunduru, Anilkumar; Subramanain, Sumathy. 1/2018. Security strategies for cloud identity management – a study. Research Gate. Verkkoartikkeli. <https://www.researchgate.net/publication/327032449_Security_strategies_for_cloud_identity_management_-_a_study>. Luettu 26.2.2024.

9 Oracle. What are the benefits of an ERP system? Verkkoaineisto. <https://www.oracle.com/erp/what-is-erp/erp-benefits>. Luettu 8.2.2024.

10 Ng, Alisa. 15.3.2023. 5 Common Ways Risk is Introduced to your ERP System and How Best to Manage it. Pathlock. Verkkoartikkeli. <https://pathlock.com/learn/5-common-ways-risk-is-introduced-to-your-erp-system-and-how-best-to-manage-it/>. Luettu 29.2.2024.

11 SAP Finland Oy. Mikä on SAP? Yrityksen verkkosivut. <https://www.sap.com/finland/about/what-is-sap.html>. Luettu 16.1.2024.

12 SAP Finland Oy. Mikä on ERP? Yrityksen verkkosivut. <https://www.sap.com/finland/products/erp/what-is-erp.html>. Luettu 16.1.2024.

13 Hyvärinen, Joonas. 2020. SAP-toiminnanohjausjärjestelmän käyttöönotto ja materiaalinhallinta. Jyväskylän ammattikorkeakoulu. Opinnäytetyö. <https://www.theseus.fi/bitstream/handle/10024/348253/SAP-toiminnanohjausj%E4rjestelm%E4n%20k%E4ytt%F6%F6notto%20ja%20materiaalinhallinta.pdf?sequence=2>. Luettu 8.2.2024.

14 Tietosuojavaltuutetun toimisto. Tietosuoja. Verkkoaineisto. <https://tietosuoja.fi/tietosuoja>. Luettu 26.2.2024.

15 Mohammed, Ishaq Azhar. 7/2017. Systematic review of identity access management in information security. Verkkoartikkeli. Research Gate. <https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887659_SYSTEMATIC_REVIEW_OF_IDENTITY_ACCESS_MANAGEMENT_IN_INFORMATION_SECURITY/links/61169c5d1ca20f6f861e4496/SYSTEMATIC-REVIEW-OF-IDENTITY-ACCESS-MANAGEMENT-IN-INFORMATION-SECURITY.pdf>. Luettu 26.2.2024.

16 Talend. What is data synchronization and why is it important? Talend Knowledge Center. Verkkoaineisto. <https://www.talend.com/resources/what-is-data-synchronization/>. Luettu 8.2.2024.