Jari Maijala

ICT Controller -palvelun kehittäminen

Metropolia Ammattikorkeakoulu

Tradenomi

Liiketalouden tutkinto-ohjelma

Opinnäytetyö

Lokakuu 2018

Metropolia

Tekijä Otsikko Sivumäärä Aika	Jari Maijala ICT Controller -palvelun kehittäminen 42 sivua + 4 liitettä Lokakuu 2018
Tutkinto	Tradenomi
Tutkinto-ohjelma	Liiketalous
Suuntautumisvaihtoehto	
Ohjaaja	Lehtori Heikki Hyvärinen

Tämän toiminnallisen opinnäytetyön tarkoituksena oli rakentaa toimeksiantajayritykselle uusi palvelu – ICT Controller -palvelu. Palvelu kattaa GDPR:n vaatimuksenmukaisuuden varmistamisen ja ICT:n toiminnan kontrolloinnin sisäisen valvonnan keinoin. Palvelukokonaisuuteen luotiin käyttöönottoon tarvittavat ohjeet ja työkalut. Opinnäytetyö rajattiin koskemaan pieniä ja keskisuuria yrityksiä, joilla ei ennestään ollut sisäisen valvonnan toimintoa. Lisäksi opinnäytetyössä oli tarkoitus koota kaikki tarvittava ohjeistus helposti saatavaksi yhteen kokonaisuuteen ja luoda uutta palvelua tukeva ymmärrettävä dokumenttikokonaisuus.

Opinnäytetyö toteutettiin toiminnallisena työnä: se muodostui taustoittavasta osiosta, jossa käsiteltiin palvelun teoreettinen viitekehys niin sisäisestä valvonnasta, lainsäädännöstä kuin ICT:n hallinnostakin, sekä toiminnallisesta osasta, joka kokosi yhteen käyttöönottoon ja jatkuviin palveluihin tarvittavat keskeiset työkalut.

Hyödynnetty viitekehys koottiin sisäisen valvonnan ohjeista, EU:n GDPR-asetuksesta sekä ICT-standardeista. Teoriaosuudessa perusteltiin myös valittu sisäisen valvonnan raportointimalli. Lisäksi teoriaosuudessa arvioitiin standardien ja määräysten soveltuvuutta pieniin ja keskisuuriin yrityksiin.

Toiminnallinen osuus koostui tyypillisistä palvelun rakentamiseen ja palvelun käynnistämiseen liittyvistä vaiheista ja tehtävistä. Opinnäytetyön palvelukehityksen sisällöksi valikoitui palvelua varten kehitettävien uusien työkalujen tekeminen.

Johtopäätöksenä todettiin, että rakennettu ICT Controller -palvelu täytti sille asetetut odotukset, ja sitä päätettiin testata pilottiasiakkaiden kanssa. Lisäksi todettiin, että vaikka kehitetty palvelu antaa hyvän pohjan pilottiprojekteille, sitä on syytä kehittää edelleen uusien palveluasiakkuuksien yhteydessä.

Avainsanat	sisäinen valvonta, ICT-Controller, GDPR, vaatimuksenmukaisuus

Author Title Number of Pages Date	Jari Maijala Developing ICT Controller Service 42 pages + 4 appendices October 2018
Degree	Bachelor in Business Administration
Degree Programme	Economics and Business Administration
Specialisation option	
Instructor	Heikki Hyvärinen, Senior Lecturer

The purpose of this thesis was to build a new service - the ICT Controller service for the sponsor company. The service covered the enforcement of GDPR's compliance and the control of ICT activities through internal controls. The service set covered guidelines and tools for deployment. This thesis was limited to small and medium-sized enterprises that did not already have acting internal control function. In addition, the aim of this thesis was to gather all the necessary instructions easily accessible to one document set and to create an understandable document entity that would support the new service.

The thesis was implemented as a functional piece of work: it consisted of a background section that covered the theoretical reference framework for internal control, legal and ICT administration, as well as a practical component that brought together key tools needed for deployment and implementing continuous services.

The utilized reference framework was compiled from internal control guidelines, EU GDPR regulation and ICT standards. The theoretical part also justified the selected internal control reporting model. The theory section had an evaluation of the impact of standards and regulations on small and medium-sized enterprises.

The operational part described typical phases and tasks related to service construction and service launch. The content of the service development work of this Bachelor's Thesis was the development of new tools for the implemented service.

As a conclusion, the built-in ICT Controller service fulfilled its expectations and the sponsor company decided to test it with pilot customers. In addition, it was found that although the developed service provides a good basis for pilot projects, it is vital to further develop it in connection with new service customers.

Keywords	Internal Control, ICT Controller, GDPR, Compliance

Sisällys

1 Johdanto

1.1 Opinnäytetyön tavoite

ICT Controller -palvelun avulla johdon näkyvyyttä ICT-toimintoihin parannetaan dramaattisesti ja palvelun myötä liikkeenjohdolle syntyy luonnollinen mahdollisuus saada asiantuntijamielipide ICT:n tilasta ostopalveluna hankitun palvelun kautta. Yritysten tietohallintojen ja varsinaisen liikkeenjohdon välinen suhde on varsin haastava. Liikkeenjohdon toiminta-alueella keskitytään yleensä markkinoiden hallintaan ja asiakkuuksien kehittämiseen, ja uutta liiketoimintaa haetaan myös tuotekehityksen ja palvelujen muotoilun avulla. Tietohallintojen toiminta-alue taas perustuu voimakkaasti tekniikkaan, tietoliikenteeseen, laitteistoihin ja ohjelmistoihin. Tekeminen tietohallinnoissa pohjautuu ICT-standardeihin ja tietohallintojen parhaiden käytäntöjen hyödyntämiseen. Vastaavasti liiketoiminnan painopisteet löytyvät asiakkuuden ja talouden hallinnan sekä muun hyvän hallinnon alueilta. Ulkoistamisten ja lisääntyneen palvelujen ostamisen vuoksi myös talouden hallinnan käsitteet ovat laajemmin käytössä myös tietotekniikassa. (Kari 2017a.)

Vaikka tietohallintojen toiminta on lähentynyt liiketoimintajohtoa, on yhteistyössä vielä paljon kehitettävää. Sofigaten, TIVIAn ja Aalto-yliopiston 2016 toteuttamassa valtakunnallisessa Tietohallintojen johtaminen Suomessa -tutkimuksessa kysyttiin liiketoiminnalta, onko sen helppo ymmärtää tietohallinnon toimintakenttää. Liiketoimintaa edustavista vastaajista 49 prosenttia vastasi, että heistä on pääosin helppoa ymmärtää tietohallintoa, 29 prosenttia totesi, että heidän on harvoin helppo ymmärtää ja 4 prosenttia vastaajista kertoi, ettei heidän ole lainkaan helppo ymmärtää tietohallinnon toimintakenttää. Siten 33 prosenttia liiketoiminnan edustajista näki, että tietohallintoa oli vaikea ymmärtää. (Kolesnik & Seren & Helenius 2016, 24.)

Tutkimuksessa vastaajille esitettiin myös seuraava kysymys: Pystytäänkö yrityksen tietohallintoa ohjaamaan ja kehittämään luotettavien ja toistettavien mittareiden avulla? Oli varsin yllättävää, että vastaajista 67 prosentin mukaan tietohallintoja ohjattiin vain osittain mittarien avulla ja 24 prosentin mukaan ei ollenkaan. Ainoastaan 4 prosentin osuus vastaajista näki, että Tietohallintoja ohjattiin ja kehitettiin kaikilta osin mittareiden avulla. (Kolesnik ym. 2016, 20.)

Tutkimuksen perusteella on selvää, että liiketoiminnan ja tietohallinnon välistä yhteistoimintaa tulisi kehittää. Koska tämän opinnäytetyön toimeksiantaja on ICT-palveluyritys,

tässä opinnäytetyössä liiketoiminnan ja tietohallinnon välistä yhteistyön parantamista lähestytään tietohallinnon näkökulmasta ja sen tulokset pyritään linkittämään liikkeenjohdon tuntemaan toimintaympäristöön.

Tässä opinnäytetyössä kehitettiin toimeksiantajayritykselle myytäväksi uusi palvelu, ICT Controller -palvelu. Palvelun avulla luodaan liikkeenjohdolle näkymä yrityksen tietohallintoon ja tietotekniikkaan käyttäen raportoinnissa hyödyksi liiketoiminnan viitekehyksiä. Vaikka tavoitteena on raportoida tietohallinnon toiminnasta liikkeenjohdon viitekehyksessä, ovat raportoitavat asiat pääosin tekniikkaan liittyviä ja käsitellään tässä opinnäytetyössä tietohallinnossa ja tietotekniikassa käytetyn termistön kautta.

Toimeksiantajayritys toimii ICT-palvelujen toimittajana ja työskentelee siten läheisessä yhteistyössä erityisesti pienten ja keskisuurten yritysten kanssa. Taustana kehitysprojektille ja tälle opinnäytetyölle oli toimeksiantajayrityksessä havaittu kysyntä ja siten palvelun kehittäminen oli liiketoiminnallisesti mahdollista. Asiakasyrityksissä oli siis tarve palvelulle, jossa asiakasyrityksen johdon tietoisuutta tietotekniikan ja erityisesti tietoturvan ja tietosuojan alueilla parannetaan. Projektin ensisijainen tavoite oli kehittää uusi palvelukokonaisuus, jossa toimeksiantajayritys voi tarjota ICT Controller -roolissa työskentelevää henkilöä asiakasyrityksen käyttöön. (Kari 2017a.)

Palvelun kehittäminen tehtiin kehitysprojektina vuosien 2017–2018 aikana. Erityisen painoarvon uudelle palvelulle loi vuoden 2018 toukokuusta alkaen sovellettava EU:n tietosuoja-asetus (Asetus 2016/679). Projektissa perehdyttiin controller-toiminnan viitekehykseen ja vallitseviin standardeihin sekä kyseiseen EU:n tietosuoja-asetukseen. Viitekehyksen perusteella luotiin kehitysmallit ja työkalut, joiden avulla uuden asiakkaan ympäristöön luodaan sisäisen valvonnan prosessit tietohallinnon valvomiseksi ja EU:n tietosuoja-asetuksen vaatimuksenmukaisuuden varmistamiseksi.

Tämä opinnäytetyö nojaa ensisijaisesti toimeksiantajayrityksen johdon ja myynnin sekä markkinoinnin henkilöiden asiantuntemukseen tarjottavan palvelun kehittämisessä. Opinnäytetyön tuloksena kehitetty palvelukokonaisuus ja sen työkalujen arviointi tehdään valittujen pilottiasiakkaiden kanssa kehitysprojektin loppuvaiheessa. Saatua palautetta hyödynnetään palvelun jatkokehittämisessä ja markkinoinnin suunnittelussa.

Toimintamallien ja työkalujen kehittämisessä päätettiin lähtökohtaisesti hyödyntää mahdollisimman paljon niin tietotekniikan kuin sisäisen valvonnankin standardeja. Ratkaisumalleja haettiin ensisijaisesti jo käytössä olevista toimintamalleista, mutta tarvittaessa uusia työkaluja kehitettiin projektin puitteissa. Toimeksiantajayrityksen johto linjasi, että mikäli sopivia työkaluja ei ole suoraan tarjolla, arvioidaan mahdollisuudet kehittää sopiva täsmätyökalu juuri tätä tarkoitusta varten (Kari 2017a). Projektissa tehty standardien soveltuvuuden arviointi asetetulle kohderyhmälle perustui julkisista lähteistä saatavaan tietoon sekä palvelua kehittävän yrityksen avainhenkilöiden osaamiseen ja ammattitaitoon.

1.2 Opinnäytetyön tyyppi ja käytettävät tutkimusmenetelmät

ICT Controller -palvelun kehittäminen tehtiin toiminnallisena opinnäytetyönä. Opinnäytetyössä tavoiteltiin toimeksiantajayrityksen ammatillisen kentän toiminnan ohjeistamista ja järkeistämistä Vilkan ja Airaksisen kirjan *Toiminnallinen opinnäytetyö* mukaisesti (Vilkka & Airaksinen 2004).

Tämän toiminnallisen opinnäytetyön tarkoituksena oli rakentaa toimeksiantajayritykselle uusi palvelu – ICT Controller -palvelu. Palvelun kehittämisessä hyödynnettiin prototyyppilähestymistapaa, jossa palvelukokonaisuuden prototyyppi kehitettiin ensin toimeksiantajayrityksessä (jatkossa Palveluyritys) omaan käyttöön ja sen jälkeen sovellettiin kuvitteelliselle palvelua ostavalle yritykselle (jatkossa Asiakasyritys). Kohderyhmää edustavan kuvitteellisen Asiakasyrityksen keskeiset piirteet on kuvattu kappaleessa 1.4 Tausta ja lähtökohdat.

Opinnäytetyön rakenne on seuraava: Johdannossa kuvataan opinnäytetyön aihe, toimeksiantajan työlle asettamat tavoitteet, opinnäytetyön toimeenpanon näkökulma/teoreettinen lähestymistapa sekä työn tausta, lähtökohdat sekä rajaukset. Luvussa 2 kuvataan ICT Controller -palvelulle keskeinen viitekehys: lakitausta, ICT-hallintamallit ja relevantit standarditLuvussa 3 ICT Controller -palvelun raportoinnin rakenne esitetään valittu raportointirakenne. luvussa 4 Tyypillinen palvelun käyttöönotto kuvataan tyypillinen ICT Controller -palvelun käyttöönottoprojekti vaiheineen. Luvussa kuvataan, miten ICT Controller -palvelu rakennetaan, otetaan käyttöön ja millaisia työkaluja palvelun käyttöönottoon kehitettiin.

Luvussa 6 COSO-IC:tä hyödyntävä ICT Controller -raportointi kuvataan kappaleessa 3 asetettujen linjausten perusteella. Luvussa 7 kuvataan opinnäytetyön eteneminen ja arvioidaan syntyneet työn tulokset. Luvusssa 8 arvioidaan opinnäytetyön tulokset ja työn hyödyt toimeksiantajalle. Luvussa arvioidaan myös, millaisen pohjan työ antaa jatkokehitykselle ja palvelujen tuottamiselle.

1.3 Keskeiset käsitteet

1.3.1 EU:n tietosuoja-asetus

EU:n tietosuoja-asetus (Asetus 2016/679) on Euroopan parlamentin, Euroopan unionin neuvoston ja Euroopan komission asetus, joka yhtenäistää tietosuojaa koskevan lainsäädännön Euroopan unionin jäsenmaiden kesken. Asetusta kutsutaan usein englanninkielisellä nimellä General Data Protection Regulation, joka lyhennetään GDPR. Asetus on annettu 27. huhtikuuta 2016 ja siitä tulee täytäntöönpanokelpoinen kahden vuoden siirtymäajan jälkeen 25. toukokuuta 2018 ja on siten suoraan velvoittava ja sovellettava myös Suomessa. (Asetus 2016/679.).

Tietosuoja-asetuksen kansallista liikkumavaraa täydennetään ja täsmennetään kansallisella lainsäädännöllä. Hallitus on antanut eduskunnalle ehdotuksen uudeksi kansalliseksi tietosuojalaiksi. Uuden tietosuojalain tulisi esityksen mukaan tulla voimaan 25.5.2018 samalla, kun myös EU:n yleistä tietosuoja-asetusta ryhdytään soveltamaan Suomessa. (Tietosuojavaltuutetun toimisto 2018.)

1.3.2 EU:n ePrivacy-asetus

ePrivacy-asetus on käsittelyssä oleva EU:n tietosuoja-asetusta täydentävä asetus, joka sääntelee yksityisyyttä ja sähköistä viestintää. Asetus korvaa ePrivacy-direktiivin 2002/58/EC (Regulation on Privacy and Electronic Communications). Viralliselta nimeltää asetusehdotus on todennäköisesti ”Asetus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus)”, lyhyemmin ePrivacy-asetus. (European Commission 2017a.)

Lähtökohtaisesti uudessa ePrivacy-asetuksessa ei tavoitteena ole tiukentaa sähköisten palvelujen sääntelyä, vaan ottaa kattavuuteen mukaan uusia direktiivin hyväksymisen

jälkeen kehitettyjä palveluja. Vanhaan ePrivacy-direktiiviin verrattuna uudessa asetuksessa otetaan huomioon uusia sähköisiä palveluja. tarkennetaan vaatimuksia muun muassa suostumuksen käsittelylle (opt-in versus opt-out) sekä keksien hyödyntämiselle. (European Commission 2017a, 8.)

1.3.3 Tietosuojavastaava

Tietosuojavastaava on organisaation erityisasiantuntija, joka toimii ensisijaisesti EU:n tietosuoja-asetuksen 37–37 artiklojen (Asetus 2016/679) mukaisesti rekisterinpitäjän tukena ja auttaa lakisääteisten velvoitteiden toteuttamisessa. Tehtäviin kuuluu myös asiantuntija-avun antaminen yrityksen henkilöstölle ja johdolle tietosuojaan liittyvissä kysymyksissä. Tietosuojavastaava valvoo organisaatiossa henkilötietojen käsittelyä sekä toimii yhteyshenkilönä valvontaviranomaisiin, joka Suomessa on Tietosuojavaltuutettu.

Tietosuojavastaavasta käytetään usein englanninkielistä nimitystä Data Protection Officer, lyhennettynä DPO. Tietosuoja-asetuksen mukainen tietosuojavastaavan asema on erittäin itsenäinen, eikä hänen tule ottaa määräyksiä ja ohjeita linjajohdolta toimiessaan tietosuojavastaavana.

1.3.4 ISO

International Organization for Standardization eli ISO on kansainvälinen standardisoimisjärjestö ja se tuottaa kansainvälisiä standardeja. Suomea järjestössä edustaa Suomen Standardisoimisliitto SFS. ISOn standardit ovat luonteeltaan suosituksia.

Tietotekniikkaan liittyvä standardisointityö tehdään yhdessä IEC-organisaation kanssa (ISO 2018). Tunnetuimpia ISO-standardeja ovat ISO9000-perheen laatustandardit sekä erilaiset tekniset standardit.

1.3.5 COBIT

ISACA on itsenäinen voittoa tuottamaton maailmanlaajuinen yhdistys, jonka tehtävänä on kehittää ja edistää maailmanlaajuisia, hyväksyttyjä tietojärjestelmäkäytänteitä. Yhdistys tunnettiin aiemmin nimellä *Information Systems Audit and Control Association,* josta lyhenne ISACA alun perin tulee.

COBIT (Control Objectives for Information and Related Technologies) on ISACA:n kehittämä parhaiden käytäntöjen puite, jota se ylläpitää. COBIT5 on puitteen uusin versio.

1.3.6 Asiakasyritys

Opinnäytetyön kannalta kuvitteellinen kohdeyritys, jolle kehitettävä palvelu kohdistetaan. Kohdeyrityksen keskeisten piirteiden ja reunaehtojen kuvaus on kappaleessa 1.4 Tausta ja lähtökohdat.

Tämän opinnäytetyön kannalta asiakasyritys voi ostaa opinnäytetyön toimeksiantajalta muitakin palveluja, mutta se ei ole palvelun kannalta välttämätöntä.

1.3.7 Palveluyritys

Tässä opinnäytetyössä mainittu palveluyritys on tietoturvaan ja toiminnan jatkuvuuteen erikoistunut ICT-alan palveluyritys. Yritys toimii tässä opinnäytetyössä toimeksiantajana ja on siten kehitettävää palvelua jatkossa tuottava yritys.

Tässä opinnäytetyössä kehitettävä palvelu toimitetaan yrityksen muusta palvelusta erillisenä palveluna, joten se on riittävän riippumatonta. Palveluyrityksen organisointi tukee itsenäistä palvelun toimittamista.

1.3.8 Tietoturvan hallintajärjestelmä

Tietoturvan hallintajärjestelmä (Information Security Management System, ISMS) on hallintajärjestelmä, jonka avulla johto asettaa tietoturvalle ja siihen liittyville prosesseille ja kontrolleille vaatimukset ja tietoturvan hallinta tuodaan johdon ohjaukseen ja hallintaan. Tunnetuin tietoturvan hallintajärjestelmä perustuu ISO27000-perheeseen (Suomen standardisoimisliitto SFS 2013a).

ISO27000-perheessä kuvataan tietoturvan hallintaa eri ympäristöissä. Esimerkiksi riskien arviointi ja hallinta on kuvattu tarkemmin omassa standardissaan. Tietoturvan hallintajärjestelmän vaatimukset kuvataan standardissa ISO/IEC27001, jonka esittämien vaatimusten täyttyminen yrityksissä auditoidaan ja siitä osoituksena saadaan sertifikaatti (Suomen standardisoimisliitto SFS 2013b).

1.3.9 Liiketoiminnan jatkuvuuden hallintajärjestelmä

Liiketoiminnan jatkuvuuden hallintajärjestelmä (Business Continuity Management System, BCMS) on hallintajärjestelmä, jonka avulla johto asettaa liiketoiminnan jatkuvuudelle ja siihen liittyville prosesseille ja kontrolleille vaatimukset. Jatkuvuuden hallintajärjestelmän avulla liiketoiminnan jatkuvuuden hallinta tuodaan johdon ohjaukseen ja hallintaan.

ISO/IEC27001 sisältää jo runsaasti liiketoiminnan jatkuvuuden varmistavia prosesseja. Tunnetuin varsinainen tietoturvan hallintajärjestelmästandardi on ISO/IEC22301-standardi. (Suomen standardisoimisliitto SFS 2013c.)

1.3.10 Sisäinen valvonta

Sisäinen valvonta on yrityksen toiminto, jonka avulla yrityksen johto ohjaa henkilöstöä tahtotilansa mukaiseen suuntaan. Toiminnon englanninkielinen nimitys *Internal Control* käännettynä sisäiseksi ohjaukseksi kuvaa paremmin sisäisen valvonnan roolia.

COSO-standardin mukaisesti organisaation sisäinen valvonta on hallituksen, yrityksen johdon ja henkilökunnan yhteinen prosessi, jonka tavoitteena on varmistaa, että toiminnan, raportoinnin ja lakien sekä vaatimusten noudattamisen tavoitteet toteutuvat. COSO-mallin mukaisen sisäisen valvonnan avulla organisaation johto saa kohtuullisen varmuuden organisaation vaatimusten mukaisesta toiminnasta. (Ratsula 2016, 13 - 17.)

1.4 Tausta ja lähtökohdat

1.4.1 Palvelun kohderyhmä

Palvelua suunniteltiin tässä opinnäytetyöprojektissa kuvitteelliselle asiakasyritykselle. Palvelun kohderyhmää suunniteltaessa oletettiin, että palvelun kohdeyritys on pientä ja keskisuurta yrityssektoria edustava yksikkö. Kyseisellä asiakasyrityksellä ei ole omaa sisäisen valvonnan tai sisäisen tarkastuksen toimintoa. Yrityksen johtaminen perustuu linjajohtamiseen ja esimies-alaissuhteisiin.

Yrityksellä oletetaan olevan organisaatiossaan 50-250 henkilöä ja tietotekniset toiminnot on pääosin ostettu usealta ulkoiselta palvelutoimittajalta. Yrityksellä on tietohallinnossaan 1–3 omaa ICT-asiantuntijaa. Usein yrityksen oma tietohallinto vastaa palvelujen ostamisesta, mutta myös itse osallistuu tietoteknisten palvelujen tuottamiseen.

1.4.2 Palvelun suunnittelun näkökulmat

Perinteisesti ICT ja yritysjohdon välillä on ollut osassa yrityksistä varsin vähän yhteistyötä. Tietohallinto hoitaa tietotekniikkaa omalla tahollaan ja siihen suhtaudutaan johdossa usein lähinnä kuluja tuottavana toimintona. Suhtautuminen perustuu asiallisesti siihen, että liikkeenjohdon ja talousjohdon ICT-osaaminen on moni paikoin varsin kevyttä. Tästä osaamiskuilusta seuraa usein johdolle epävarmuutta tietohallinnon toiminnan tarkoituksenmukaisuudesta.

Toinen liikkeenjohdon suhtautumismuutos ICT:n suhteen on seurausta EU:n tietosuoja-asetuksen voimaan tulosta. EU:n tietosuoja-asetuksen 83 artiklan mukaan tiettyjen säännösten rikkomisesta viranomainen voi määrätä hallinnollisen sakon, joka on suurimmillaan 20 000 000 euroa tai neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta (Asetus 2016/679). EU:n tietosuoja-asetus edellyttää myös tehokasta tietoturvaa, ja se on yleensä juuri ICT-yksikön vastuulla (Asetus 2016, artikla 24).

Edellä esiteltyä taustaa vasten tarkasteltuna ICT Controller -palvelun tuottamiksi suurimmiksi asiakashyödyiksi arvioitiin seuraavat hyödyt: EU:n tietosuoja-asetuksen mukaisen toiminnan varmistaminen ja yleinen ICT:n toiminnan arviointi ja sen raportointi ulkopuolisin silmin. ICT Controller -palvelun ydinkomponenteiksi valikoituivat nämä kaksi näkökulmaa. (Kari 2017b.)

Toimeksiantajayrityksen lähtökohdista tärkein arvioitava liiketoiminnallinen asia oli, voidaanko johdon epävarmuus tietohallinnon toiminnasta muuttaa palveluyrityksen liiketoiminnaksi? Toinen arvioitava näkökulma oli, onko teknisistä viitekehyksistä hyötyä palvelulle kehittämisessä? Kolmas arvioitava kokonaisuus on, kannattaako palvelussa raportoida COSO-viitekehyksen avulla vai räätälöidysti?

1.4.3 Palvelun DPO-näkökulma

Suomessa tulee sovellettavaksi EU:n uusi yleinen tietosuoja-asetus, General Data Protection Regulation (GDPR). Se on suoraan voimassa sellaisenaan koko EU:n alueella. Joihinkin asetuksessa mainittuihin asioihin liittyy kansallinen liikkumavara, joita tarkennetaan paikallisella lainsäädännöllä. Suomessa uuden asetuksen soveltaminen alkaa 25.5.2018 ja yritysten tulee täyttää siihen mennessä asetuksen asettamat vaatimukset. (GDPR, Asetus 2016, artikla 99.).

Palveluyrityksessä uskotaan, että ICT Controller -toiminto on kohdeyritykselle jatkossa tärkeä, koska EU:n tietosuoja-asetuksen kautta myös kyberturvallisuuden muun tietoturva- ja tietosuojan vaatimustaso nousee olennaisesti lainsäädännön kiristymisen takia.

1.4.4 Palvelun ICT Governance- ja tietoturva-näkökulma

Asetus vaatii taustakseen tehokkaan ja ajantasaisen teknisen tietoturvan ja sen hallinnan. EU:n tietosuoja-asetus määrää 24. artiklassaan seuraavaa (Asetus 2016/679):

> ”Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.”

Kyseisen artiklan perusteella yritykset on velvoitettu tekemään säännöllinen riskiarviointi tietosuojan ajanmukaisuuden arvioimiseksi ja tarvittaessa parantamaan tietoturvaa ja sitä kautta tietosuojan tasoa. Liikkeenjohdon kannalta tämä tarkoittaa myös, että yrityksellä tulee olla kyky tehdä itse säännöllisiä riskiarviointeja tai hankkia ne toimittajilta. Toisaalta artiklan mukaan kehittäminen tulee tehdä riskipohjaisesti, eikä pelkästään taloudellisten reunaehtojen kautta.

1.5 Kehitettävän palvelun yhteenveto

Toimeksiantajayrityksen asettamien reunaehtojen mukaisesti opinnäytetyön tavoitteena on rakentaa sisäisen valvonnan toiminto, joka varmistaa EU:n tietosuoja-asetuksen vaatimuksenmukaisuuden täyttymisen sekä luo raportoinnin kautta johdolle tiedon yrityksen ICT:n tarkoituksenmukaisesta toiminnasta, tehokkuudesta ja tietoturvan tasosta. (Kari 2017a.)

Asetetut osatavoitteet ICT Controller -palvelua kehittävälle opinnäytetyöprojektille on selvittää viitekehys ja olennaiset palveluun liittyvät standardit, etsiä sopivat työkalut ja toimintamallit, rakentaa tarvittaessa sopivia uusia työkaluja sekä luoda edellytykset markkinoinnille ja pilottiprojekteille.

Palveluyritys asetti kehitettävälle palvelulle seuraavat toiminnalliset puitteet (Kari 2017b): Kustannukset asiakasyritykselle voivat olla 6 000–18 000 euroa vuodessa. Työmääräksi muutettuna palvelu pitää tuottaa 0,5–1,5 henkilötyöpäivän panoksella kuukaudessa. Raportoinnin tulee kuvata tietoturvan ja tietosuojan tilaa yrityksessä sekä toiminnan GDPR-vaatimuksenmukaisuutta yleisjohdon ymmärtämällä tavalla. Palvelun raportoinnin tulee tuottaa GDPR:n vaatimuksenmukaisuuden osoittamiseksi tarvittavan dokumentaation.

Tausta ja asetetut tavoitteet huomioon ottaen Palveluyrityksessä nähtiin palvelun kehittäminen mahdolliseksi ja siten kehitysprojekti käynnistettiin keväällä 2017 (Kari 2017a).

1.6 Rajaus

Kehitettävässä palvelussa päätettiin rajata ICT-talouden seuranta toteutettavaksi yrityksen omilla taloudenhallinnan menettelyillä. Taloudenhallinnan työkalujen kehitys rajattiin siten ulos määriteltävästä ICT Controller -palvelusta. Asiakaskokemusten perusteella talousseuranta on yrityksissä jo lakivelvoitteiden ja tilitarkastuksenkin takia tyydyttävällä tasolla. (Kari 2017a.)

Mikäli asiakas näkee tarpeellisena, palvelussa raportoidaan myös ICT-talouden tilannetta siten, että tietotekniikkaan liittyvät erityispiirteet, kuten palvelusopimukset sekä leasing- ja lisensointi-mallit otetaan tarkemmin huomioon ja myös niistä annetaan suositukset yrityksen johdolle.

EU:n tietosuoja-asetusta ei tässä opinnäytetyössä avata kokonaisuudessaan auki, ainoastaan ICT Controller -toimintaan liittyvät vaateet otetaan esille (Kari 2017b).

2 Kehitettävän palvelun puitteet

2.1 Lainsäädännön määräykset yritykselle

Lainsäädäntö luo yritykselle pakottavan toiminnan viitekehyksen. Yrityksen toimintaa ohjaavat esimerkiksi kirjanpitolaki, työsopimuslaki sekä työehtosopimuslaki. Lisäksi yrityksen toiminnassa ja sitä kautta palvelun muotoilussa tulee ottaa huomioon toimialaan sidonnaiset säädökset ja määräykset.

ICT Controller -toiminnan kannalta palvelun keskeisen viitekehyksen luo toukokuussa 2018 voimaan tulevan EU Tietosuoja-asetuksen lisäksi myös direktiivistä asetukseksi uudistuva ePrivacy-kokonaisuus sekä Tatti-mietintöön pohjautuvaa paikallista tietosuojalainsäädäntö. (Asetus 2016/679, European Commission 2017a; Nurmi ym. 2017.) EU:n tietosuoja-asetus on suoraan jäsenmaissa voimaan saatettua lainsäädäntöä, jossa on jossain määrin kansallista liikkumavaraa. Kansallinen liikkumavara sidotaan uudessa Tietosuojalaissa.

GDPR asettaa EU-tason vaatimustason tietosuojalle ja tietoturvalle. EU:n tietosuoja-asetus lähtee tiukentamaan EU-kansalaisten henkilötietojen suojaamista globaalilta tasolta aina yksittäisen yrityksen tasolle. EU:n Tietosuoja-asetus edellyttää tietosuojan pohjaksi tehokkaan ja ajantasaisen tietoturvan. EU:n tietosuoja-asetuksen periaatteet vastaavat monilta osiltaan nykyisin voimassa olevan henkilötietolain periaatteita (Henkilötietolaki 1999; Tietosuojavaltuutetun toimisto 2017, 12). Asetuksessa osaa näistä periaatteista on täsmennetty.

Tietosuoja-asetuksen tietosuojaperiaatteita ovat (Tietosuojavaltuutetun toimisto 2017, 12): Henkilötietojen käsittelyn tulee olla lainmukaista, kohtuullista ja läpinäkyvää, henkilötietojen käsittelyn tulee olla käyttötarkoitussidonnaista, talletettavat tiedot tulee minimoida. Talletettavien tietojen tulee olla täsmällisiä, niiden säilytysaikaa tulee rajoittaa, rekisterinpitäjän tulee varmistaa tietojen eheys ja luottamuksellisuus. Rekisterinpitäjälle syntyy myös osoitusvelvollisuus asetuksen noudattamisesta.

Verrattuna ennen asetusta vallitseviin tietosuojaperiaatteisiin, ei niihin tule erityisen suuria muutoksia, mutta vaatimuksia vastaamaton toiminta muuttuu sanktioitavaksi. EU:n tietosuoja-asetuksen 37-37 artiklojen (Asetus 2016/679) mukaisesti osaan yrityksistä syntyy uusi vastuuhenkilötehtävä (tietosuojavastaava, Data Protection Officer, DPO).

Mikäli yritys ei noudata EU tietosuoja-asetuksen määräyksiä, aiheutuu niistä yritykselle pahimmillaan huikeat sanktiot: EU:n tietosuoja-asetuksen 83 artiklan mukaan (Asetus 2016/679) maksimissaan 20 miljoonaa euroa tai 4 prosenttia konsernin globaalista liikevaihdosta, kumpi on suurempi. Pahimmillaan viranomaispäätöksen seurauksena voi olla myös esimerkiksi liiketoiminnan keskeyttäminen.

ICT Controller -palvelun kannalta EU:n tietosuoja-asetus ja sitä täydentävät lait ja asetukset ovet merkitykseltään omaa luokkaansa, koska se asettaa vaatimustason tietosuojalle ja tietoturvalle sekä myös liiketoiminnan jatkuvuudelle. Koska EU:n tietosuoja-asetuksella saattaa pahimmillaan olla dramaattiset seuraukset yrityksen liiketoimintaan, on sen vaatimuksenmukaisuuden varmistaminen sisäisen valvonnan keinoin perusteltua.

EU:n tietosuoja-asetuksesta johtuvat keskeiset vaatimukset ICT Controller -palvelulle ovat tietoturvan ajantasaisuuden arviointi, EU:n tietosuoja-asetuksen mukaisen vaatimuksenmukaisuuden arviointi sisäisissä prosesseissa, rekisteröidyn prosesseissa sekä toimittajasuhteissa ja dokumentaation ajantasaisuuden valvonta.

2.2 Sisäistä valvontaa koskevat määräykset ja ohjeet Suomessa

Suomessa listattujen yritysten hallinnointi on määritelty Keskuskauppakamarin julkaisemassa Suomen listayhtiöiden hallinnointikoodissa (Corporate Governance) (Keskuskauppakamari 2015). Hallinnointikoodi sisältää suosituksia yhtiön sisäisen valvonnan, riskienhallinnan ja sisäisen tarkastuksen järjestämiseksi (Keskuskauppakamari 2015, 42). Seuraavassa on esitetty hallinnointikoodin suositus 25:

> SUOSITUS 25 – Sisäinen valvonta
>
> SUOSITUKSEN PERUSTELUT
>
> Tuloksellinen liiketoiminta edellyttää, että yhtiö ohjaa ja valvoo jatkuvasti toimintaansa. Hallitus huolehtii siitä, että yhtiössä on määritelty sisäisen valvonnan toimintaperiaatteet ja että yhtiössä seurataan ohjauksen ja valvonnan toimivuutta. Sisäisen valvonnan toimintaperiaatteiden avulla pyritään varmistamaan, että yhtiön tavoitteet liittyen esimerkiksi yhtiön strategiaan, toimintaan, käytäntöihin ja erityisesti taloudelliseen raportointiin toteutuvat. Sisäisen valvonnan toimintaperiaatteiden avulla pyritään varmistamaan myös osaltaan lakien ja määräysten noudattamista yhtiössä. Sisäisen valvonnan menetelmät ja toimintaperiaatteet tulee määritellä yhtiökohtaisesti yhtiön omista lähtökohdista käsin ottaen huomioon muun muassa yhtiön koko, toimiala, toiminnan maantieteellinen ulottuvuus ja rakenne. Sisäisen valvonnan toimintaperiaatteet selostetaan selvityksessä hallinto- ja ohjausjärjestelmästä.

Samansuuntaiset suositukset koskevat myös listaamattomia yhtiöitä. Myös Kuntaliiton asiantuntijat ovat julkaisseet ohjeen tavoitteenaan antaa käytäntöön sovellettavia neuvoja kunnan sisäiseen valvontaan ja riskienhallintaan. (Kuntaliitto 2016.) Kaikilla edellä mainituilla tahoilla sisäisen valvonnan perustana on COSO-IC tai COSO-ERM-malli.

Kuten jo aiemmin todettiin, vuonna 2016 tehdyn tutkimuksen mukaan 33 prosenttia liiketoiminnan edustajista näki, että tietohallintoa oli vaikea ymmärtää. (Kolesnik ym. 2016, 24.) Koska tietohallinnon toimintaa on niinkin vaikea ymmärtää, täydentää ICT Controller -palvelu osaltaan yritykselle asetettuja sisäisen valvonnan velvoitteiden toteuttamista.

2.3 COSO-mallit raportoinnin rakenteena

Nina Ratsulan kirjan *Yrityksen sisäinen valvonta* mukaan hyvän yleisesti tunnetun sisäisen valvonnan määritelmän tarjoaa COSO-malli. COSO-mallin mukaan organisaation valvontaprosessi on yrityksen hallituksen, johdon ja henkilökunnan yhteisesti toteuttamaa, ja sen tarkoitus on tuottaa kohtuullinen varmuus seuraavien tavoitteiden toteutumisesta: toiminnot (operations), raportointi (reporting) ja vaatimuksenmukaisuus (compliance). (Ratsula 2016, 59.) Toiminnan tavoitteena on tarkoituksenmukaisuus, taloudellisen raportoinnin luotettavuus, lakien ja säädösten noudattaminen.

Hyvä perehdytys COSO-malliin on luettavissa mallin kotisivuilta https://www.coso.org/ ja sieltä on myös luettavissa hyvä johdanto malliin COSO-IC ja COSO-ERM (McNally 2013).

Kuvio 1. COSO-kuutio (McNally 2013, 4).

Kuvio 1 havainnollistaa erinomaisesti COSO-mallin eri näkökulmia tarkasteltavan yrityksen toimintaan. Kuution yläpinnan näkökulmat (operations, reporting, compliance) kuvaavat raportoinnin pääasiallisia näkökulmia. Etusivun rivit kuvaavat sisäisen valvonnan osatoimintoja: ohjausympäristö, riskien arviointi, valvontatoimenpiteet, informaatio ja viestintä sekä seurantatoimenpiteet. Kuution kolmas sivu kuvaa yrityksen organisaatiota ja sen eri tasoja. Kuution yläsivun näkökulmissa tarkastellaan toimintaa seuraavissa suhteissa: Toiminta-näkökulmassa (operations) arvioidaan yrityksen toimintojen tehokkuutta ja tarkoituksenmukaisuutta. Raportointi-näkökulmassa (reporting) arvioidaan taloudellisen raportoinnin luotettavuutta ja vastaavasti vaatimuksenmukaisuus-näkökulmassa (compliance) arvioidaan lakien ja säädösten noudattamista. (Ratsula 2016, 59 - 62.)

Kuution etusivun näkökulmassa tarkastellaan sisäistä valvontaa viidestä toisiinsa liittyvästä osatekijästä lähtien. Ohjausympäristö kuvaa sisäisen valvonnan toimintaympäristöä kokonaisuutena, hallitusta ja toimivaa johtoa sekä organisaation sitoutumista sisäisen valvonnan toteuttamiseen. Riskien arviointi -osatekijässä kuvataan puitteet riskien hallinnan mahdollistamiseksi ja niiden tunnistamiselle. Riskien arvioinnissa otetaan huomioon myös väärinkäytösten mahdollisuudet ja organisaation toiminnan muutoksista aiheutuvat riskit. Valvontatoiminnot-näkökulmassa kehitetään valvontatoimenpiteitä, jotka tukeva yrityksen tavoitteisiin pääsemistä. Informaatio- ja kommunikaationäkökulmassa varmistetaan sisäisen valvonnan näkyvyys ja rooli osana yrityksen muuta toimintaa.

Seuranta-näkökulmassa yritys arvioi sisäisen valvonnan tehokuutta ja tarkoituksenmukaisuutta. (Ratsula 2016, 62 - 64):

COSO-IC viitekehyksen seuraava kehitysaskel on COSO-ERM-viitekehys. Viitekehyksen uudessa versiossa on tavoitteena tiivis ja kiinteä yhteistyö valvottavan toiminnon ja valvontaa suorittavan sisäisen valvonnan yksikön kesken. Erityinen painoarvo COSO-ERM mallissa on pureutuminen riskinarviointiin ja riskinhallintaan.

Kuten edellisessä kappaleessa (2.2. Sisäistä valvontaa koskevat määräykset ja ohjeet Suomessa) huomattiin, kaikki sisäisen valvonnan suositukset on luotu COSO-IC tai COSO-ERM mallin mukaisesti ja siksi kehitettävä palvelu kannattaa myös rakentaa COSO-puitteen mukaisesti. Seuraavassa arvioidaan eri COSO-mallien soveltuvuutta palvelun puitteeksi.

Kuten yllä todettu, COSO-IC antaa mahdollisuuden selkeään raportointiin niin tietohallinnon toiminnan vaatimuksenmukaisuuden ja lainmukaisuuteen kuin myös esimerkiksi EU:n tietosuoja-asetuksen mukaisuuden osalta. Kun tarkastelemme COSO-ERM-viitekehystä ICT Controller -palvelun tarpeisiin, on todettava, että uudessa versiossa on palveluntarjoajan kannalta merkittäviä rajoitteita palvelun tuottamisen suhteen. Jatkuva ja kiinteä yhteistyö valvottavan organisaation kanssa tekee vaikeaksi tuottaa palvelua kohtuullisin kustannuksin. COSO-ERM-mallin mukainen kiinteä yhteistyö vaatii merkittävästi suurempaa läsnäoloa asiakasorganisaatiossa. COSO-IC-malli sopii siten helpommin ulkoisen palveluntarjoajan toimittamaksi kustannustehokkaaksi valvontapalveluksi. Kiinteässä ja luonteeltaan jatkuvassa yhteistyössä muodostuu myös riskiksi tilanne, jossa pienen tietohallinto-organisaation jokapäiväisessä johtamistyössä on läsnä varsinainen linjajohto ja riskinäkökulman kautta myös sisäinen valvonta. Koska kohderyhmäksi palvelulle on valittu pieni ja keskisuuri yritysmaailma, on silloin pienissä organisaatioissa todellisena riskinä ristiriitojen kasvaminen kahden rinnakkaisen johtamisjärjestelmän välille. COSO-ERM-mallissa syntyvä matriisijohtamisen malli on sopiva isommissa yrityksissä, esimerkiksi pörssiyrityksissä, joissa linjajohdon ja sisäisen valvonnan läsnäolo on suotavaa. Ulkoisena palveluna tarjottavan ICT Controller -palvelun osalta saumaton yhteistyö on siis toisaalta mahdollisuus, mutta myöskin haaste kustannustehokkaan palvelun muotoilussa.

2.4 Raportointimallin valinta

Vaihtoehtona standardien mukaiselle raportoinnille oli tehdä raportoinnista asiakaskohtainen ja välttää siten ennakkoon määriteltyjä rakenteita. COSO-mallin ja räätälöidyn raportoinnin vertailun helpottamiseksi kummallekin vaihtoehdolle tehtiin SWOT-analyysi.

S (Vahvuudet)	**W (Heikkoudet)**
Standardi	Vieras käsite pienten yritysten johdolle
Monistettavissa (edullinen)	Hyöty vaikeasti hahmotettavissa
Tehokas palvelutuotanto (edullinen)	
O (Mahdollisuudet)	**T (Uhat)**
Tuodaan kumppanina uutta toimintamallia	COSO koetaan vieraaksi ja epämiellyttäväksi
Tuodaan kumppanina ICT-osaamista yritykseen	

Kuvio 2. COSO-mallin mukaisen raportoinnin SWOT.

S (Vahvuudet)	**W (Heikkoudet)**
Asiakkaan toiveiden mukainen	Yksilöllinen palvelu per asiakas (kallis)
Välitön asiakashyöty	Tehoton palvelutuotanto (kallis)
O (Mahdollisuudet)	**T (Uhat)**
Kehitetään palvelua vähitellen COSO:n suuntaan	Palvelu on liian kallista. Ei synny liiketoimintaa.
Tuodaan kumppanina ICT-osaamista yritykseen	

Kuvio 3. Räätälöidyn raportoinnin SWOT.

COSO-pohjaisen raportoinnin vahvuutena on standardin mukaisuus. COSO-standardia voi käyttää markkinoinnissa vahvana argumenttina. Räätälöidyn raportoinnin ehdottomana etuna on asiakaslähtöisyys. Raportointi rakennetaan juuri asiakkaan tarpeiden perusteella. Räätälöidyssä raportoinnissa on kuitenkin haittana sen kalleus ja huonompi monistettavuus ja soveltuvuus tehokkaaseen palvelutuotantoon. Kummassakin vaihto-

ehdossa palvelun avulla tuodaan asiakkaan käyttöön ICT-osaamista ja uusia toimintamalleja. Edelle esitetyistä syistä johtuen palvelu päätettiin rakentaa perustuen COSO-IC-viitekehykseen. (Kari 2017b.)

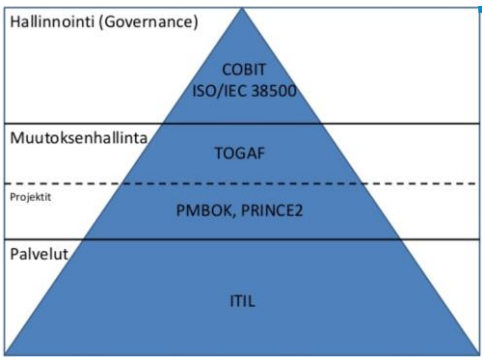
COSO-IC mallin mukaisessa ICT Controller -palvelussa yritysjohto saa tiiviin sisäisen valvonnan raportoinnin, jonka perusteella se vakuuttuu toiminnan lain- ja vaatimuksenmukaisuudesta, saa sparrauskumppanin tietohallinnon toiminnan kehittämiseen, käynnistää ripeästi korjaavat toimenpiteet sekä säilyttää ehdottoman johtajuuden organisaatiossa.

2.5 ICT Governance

2.5.1 Standardoitut toimintamallit

Tietotekniikkaan on kehitetty vuosin saatossa lukuisia eri standardeja ja toimintamalleja. Opinnäytetyössä kehitettävän palvelun kannalta olennaisimpia ovat tietohallinnon ja tietotekniikan kokonaisuutta hallitsevat standardit ja ICT Governance -mallit. IT Governance on käsitteellisesti yritystason hallintomallien osajoukko, joka keskittyy tietotekniikkaan, sen suorituskykyyn sekä riskinhallintaan.

Kehitettävän palvelun kannalta ylätason kansainväliset hallintamallit antavat hyvän pohjan tietohallinnon ja tietotekniikan muodostaman kokonaisuuden hallinnan arviointiin. Kuvio 4 kuvaa hyvin kansainvälisten standardien suhdetta toisiinsa. ICT Governance -standardeista keskeisimpiä ovat COBIT5 ja ISO/IEC 38500. (Karttaavi 2014.)



Kuvio 4. Tietohallinnon johtamisen ja suunnittelun viitekehykset (Karttaavi 2014, 11).

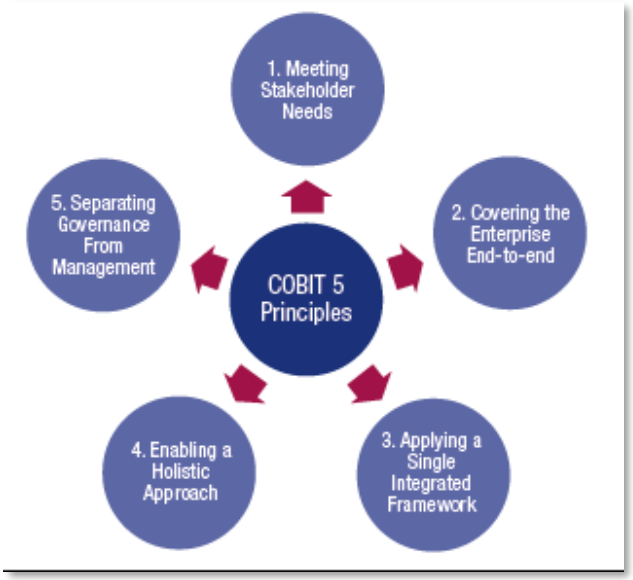
COBIT ja ISO/IEC38500 ovat ylätason hallintomalleja. TOGAF keskittyy järjestelmien kehittämiseen hallitun muutoksen kautta. Vastaavasti PMBOK ja PRINCE2 ovat projektitoiminnan standardeja. Palvelutuotannon osalta ITIL (ISO20000) on vakiinnuttanut asemansa tietoteknisten palvelutuotannon standardiksi.

Toinen tarkasteltavaksi valittu hallintamalli on Tietohallintomalli. Se on Suomessa hyvin yleinen, jopa De Facto -standardin aseman saavuttanut ICT Governance -malli. Se on alun perin Suomessa avoimesti kehitetty tietohallinnon hallintamalli, joka kattaa kaikki tietohallinnon alueet. Tietohallintomallissa on myös hyödynnetty yllä mainittuja kansainvälisiä standardeja ja malleja (Tietohallintomalli 2018). Mallin suosiota Suomessa kuvaa esimerkiksi se, että muun muassa Helsingin yliopiston kokonaisarkkitehtuurimalli on rakennettu sen mukaisesti. (Helsingin yliopisto 2009.)

Tässä opinnäytetyössä tarkastellaan tarkemmin COBIT5 -standardia ja Tietohallintomallia, koska ne ovat yleisimpiä Suomessa käytettyjä viitekehyksiä. Tietohallintomallia kehittävän tahon mukaan mallin hyödyntämistä ollaan laajentamassa myös ulkomaille.

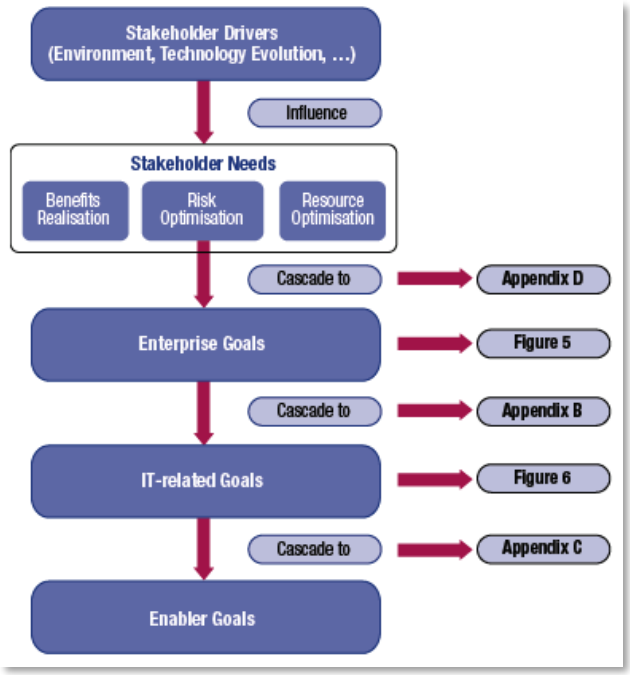
2.5.2 COBIT5

COBIT5 on uusin versio ISACA-yhteisön kehittämästä tietohallinnon Governance-mallista. Tietotekniikan hallinnan tavoitteet rakennetaan COBIT5:n periaatteista lähtien kuvion 5 mukaisesti. Malli on karkeimmalla tasollaan selkeä ja ottaa huomioon johdon asettamat tavoitteet ja pakottaa toiminnan haluttuun kokonaisrakenteeseen.



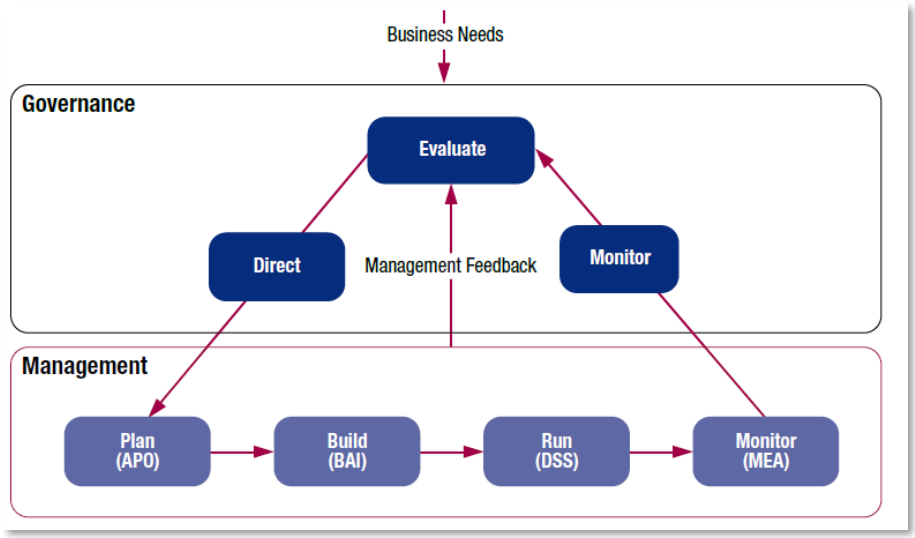
Kuvio 5. COBIT5 Periaatteet (ISACA 2018, 13).

Edellä esitetyn kuvion 5 mukaisesti COBIT5 johtaa tavoitteet ylätason sidosryhmien odotuksista ja johtaa niistä eri organisoinnin tasoille omat tavoitteensa. Kunkin tason käsittely on ohjeistettu COBIT5:ssa omilla ohjeistuksillaan. COBIT5 tarjoaa kokoelman kontrolleja ja organisoi ne loogisen rakenteeseen. Rakenne perustuu prosesseihin (processes) ja mahdollistajiin (enablers).



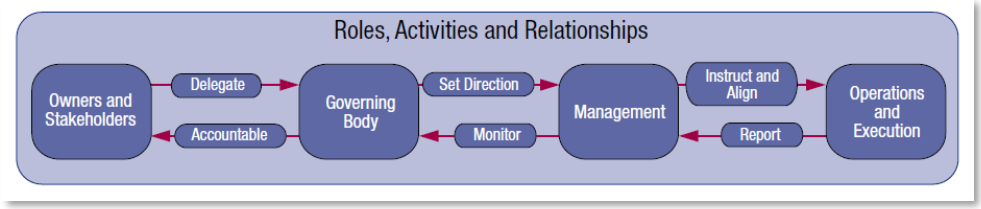
Kuvio 6. COBIT5 Tavoitteiden hiearkinen rakentuminen (ISACA 2018, 18).

COBIT5:n etuna on hierarkisuus siten, että ylemmän tason tavoitteista johdetaan alemman tason tavoitteet. Rakenteen kerroksittaisuudesta johtuen alimmankin tason tavoitteille on löydettävissä yritystason päämäärä. COBIT5:n olennainen periaate on erottaa johtaminen hallinnasta. Johto vastaa tavoitteiden asettamisesta hallinnon valvonnasta. Hallinto vastaa tavoitteiden saavuttamisesta kuvattujen prosessien avulla. COBIT5-mallissa ICT Governance jaetaan esitetyllä tavalla kahteen tasoon alla esitetyn kuvion 7 mukaisesti:



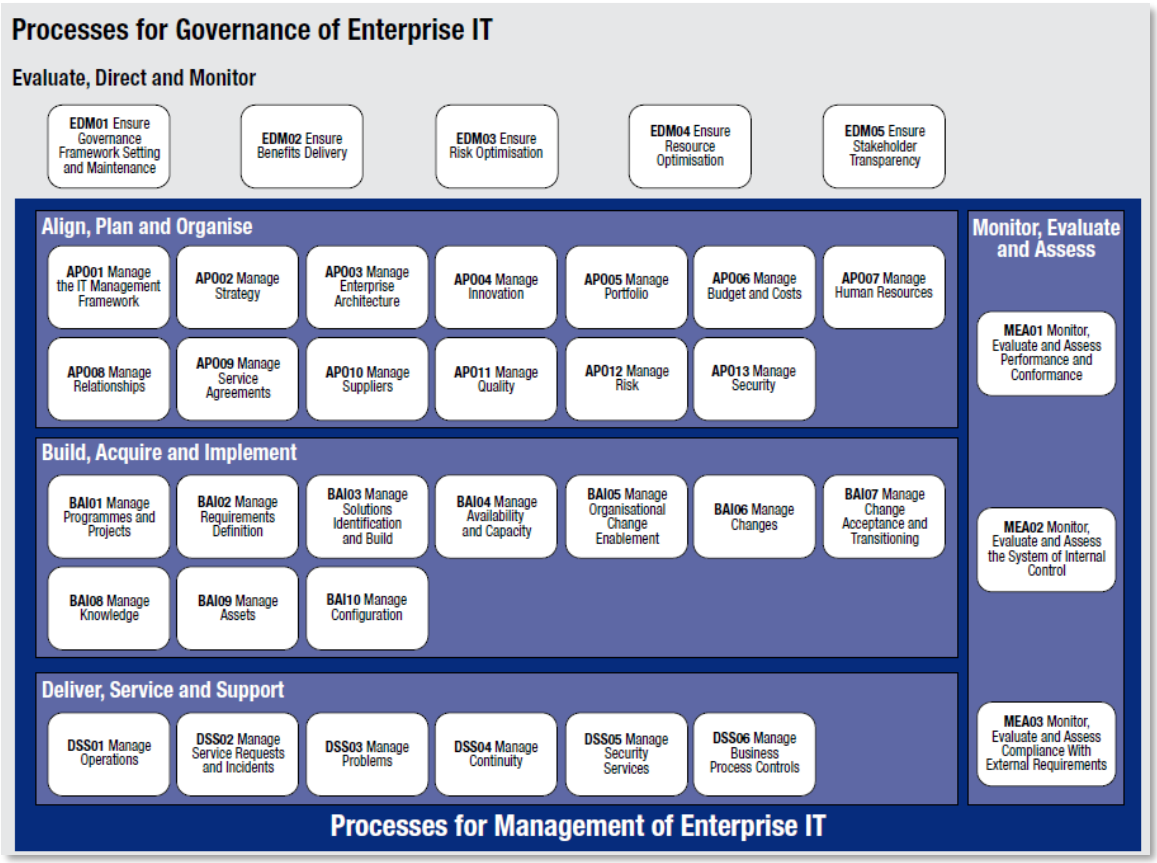
Kuvio 7. COBIT5 Hallinnon (Governance) ja johtamisen avainalueet (Management) ja niiden suhde toisiinsa (ISACA 2018, 32).

Vastaavasti COBIT5:ssä esitetään eri osapuolien roolit ja tehtävät selkeällä tavalla. Yrityksen johdosta alas tekijätasolle on määritelty eri tasot ja niille vastuut ja vuorovaikutus muiden tasojen kanssa. Kuviossa 8 on kuvattu eri tasojen suhteet:



Kuvio 8. COBIT5 Roolien, aktiviteettien ja niiden väliset suhteet (ISACA 2018, 24).

Tuloksena COBIT5:n mukaisesta ICT hallintamallin referenssitoteutuksesta syntyy seuraavan kuvion 9 mukainen standardi prosessikartta, johon kaikki tietohallinto-organisaation tehtävät voidaan sijoittaa. Kullakin prosessilla on nimilyhenne sekä kuvaava nimi.



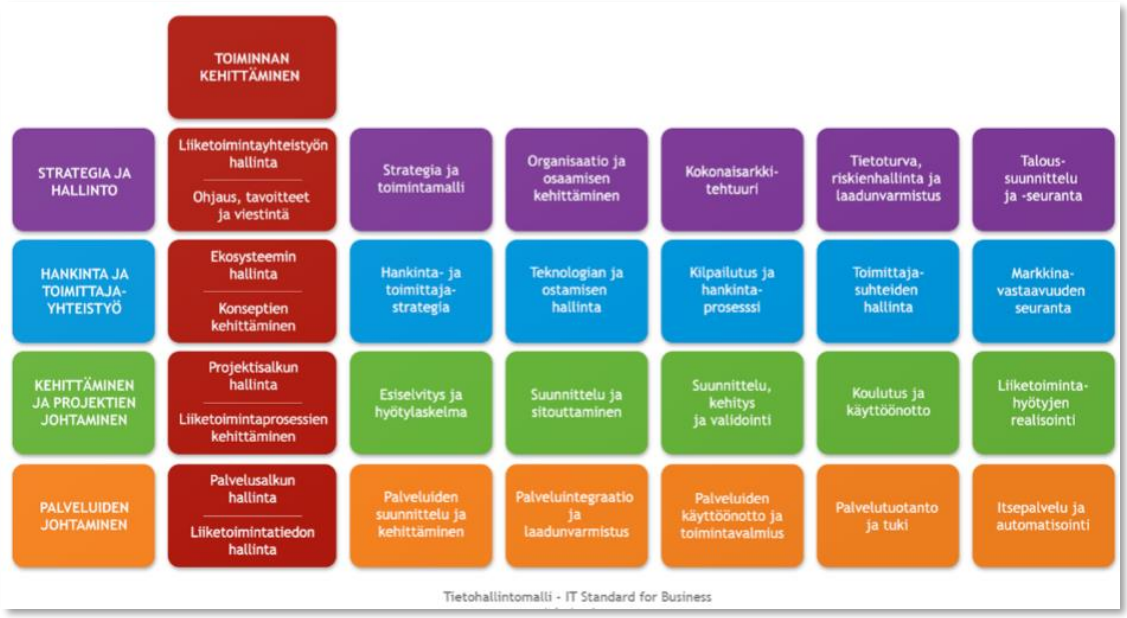
Kuvio 9. COBIT5 Prosessien referenssimalli (ISACA 2018, 32).

Kuviossa 9 esitettynä COBIT5 prosessien kokonaisuus ei ota suoraan kantaa organisaation miehitykseen, vaan tehtävien resursointi jää paikallisen organisaation vastuulle. Pienissä ja keskisuurissa yrityksissä on COBIT5:n toteuttaminen hankalaa, koska toimintoketjut on mallissa jaettu pieniin erillisiin vaiheisiin ja prosesseja ja koko tietotekniikkaa hallinnoimassa on vain kourallinen henkilöitä. Monimutkaisuuden takia COBIT5:n rakennetta noudattelevan hallintomallin rakentaminen koko laajuudessaan ei ole kohderyhmän yrityksissä perusteltua. Mikäli yrityksessä on jo rakennettu COBIT5:n mukainen hallintamalli, on se mallin prosessiluonteen takia helposti hyödynnettävissä COSO-mallin mukaiseen sisäisen valvonnan raportointiin. Liiketoimintajohdon kannalta COBIT5-mallin soveltaminen sisäisen valvonnan käyttöön on myös sen takia hankalaa, että rakenne ei ole yleisjohdon kannalta yleistajuinen ja siten helposti ymmärrettävä pohja COSO-raportoinnille.

2.5.3 Tietohallintomalli

ICT Standard Forumin kehittämä Tietohallintomalli on niin tietohallinnolle kuin liiketoiminnallekin tarkoitettu tietohallinnon johtamisen viitekehys. Ensisijaisesti kohderyhmänä ovat eri liiketoiminta- ja tietohallintojohtajat, mutta se tarjoaa aiheesta kiinnostuneille tiiviin kokonaiskuvan tietohallinnon johtamisesta. Tietohallintomallin tavoite on helpottaa tietohallintojen johtamista liiketoimintalähtöisesti. (Tietohallintomalli 2018,12.)

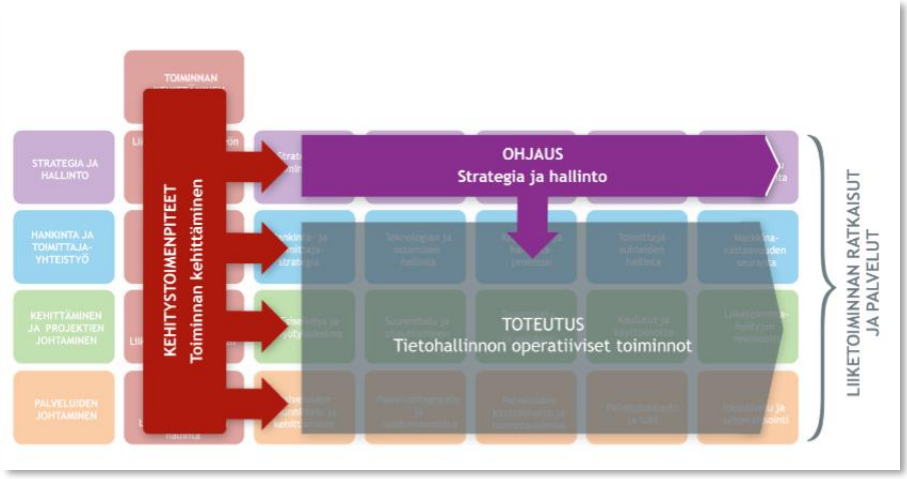
Tietohallintomalli on jaettu alla esitetyn kuvion 10 esittämällä tavalla toiminnallisesti eri tasoille. Tietohallinnon johtaminen kuvataan ylimmällä tasolla (Strategia ja hallinto), jonne on koottu kehitettävän palvelun kannalta tärkeät toiminnot, kuten tietoturva ja riskienhallinta sekä taloussuunnittelu ja -seuranta. Hankintaan ja toimittajayhteistyöhön liittyvät asiat on koottu toiselle tasolle. Kolmannella tasolla on yrityksen kehittämiseen ja projektien johtamiseen liittyvät toiminnot. Alimmalle tasolle on koottu tietohallinnon palvelujen hallinta. Kaikkia vaakatasoja leikkaa niille yhteinen liiketoimintayhteistyö ja toiminnan kehittäminen. Vertikaalin avulla mallinnetaan niin yrityksen toiminnan kuin tietohallinnonkin kehittäminen ja liiketoiminnan kanssa tehtävä yhteistyö.



Kuvio 10. Tietohallintomallin rakenne (Tietohallintomalli 2018,1).

Kuviossa 10 esitetyt osa-alueet ovat varsin yleistajuisesti esitettyjä ja siten ne tarjoavat hyvän pohjan raportoinnille yleisjohdon suuntaan. Mallin vaakarivien toiminnot liittyvät loogisesti toisiinsa ja vastaavasti eri kerroksilla on oma vastuualueensa. Mallin toiminta

on selkeästi viestittävissä tietohallinnon toimintaa tarkemmin tuntemattomille. Kuviossa 11 esimerkkinä tietohallinnon toiminnan ohjaus. Sen perusteella on helppo viestiä tietohallinnon johtamisen periaate ja luoda yhteinen ymmärrys Tietohallinnon johtamiseen.



Kuvio 11. Tietohallinnon hallintomalli (Tietohallintomalli 2018,57).

Tietohallintomallissa johtaminen (Strategia ja hallinto) päärooleihin kuuluvat tietohallintojohtajan lisäksi kehityspäällikkö, pääarkkitehti, tietoturvapäällikkö ja IT:n taloudesta vastaava kontrolleri (IT Controller). Nämä roolit kuuluvat usein tietohallinnon johtamistoimistoon (CIO Office). Tässä opinnäytetyössä on merkittävää, että Tietohallintomallissa IT-kontrolleri on asetettu vastuuseen ainoastaan tietohallinnon budjetoinnista, talussuunnittelusta ja -seurannasta yhteistyössä yrityksen talous- kuin tietohallintojohdon kanssa. Mallin mukaan IT-kontrolleri tehtävänä on myös huolehtia mahdollisesta sisäisestä laskutuksesta varmistaen tietohallinnon kulujen oikea kohdentamisen. (Tietohallintomalli 2018, 59.) Tietohallinnon oman toiminnan valvonnan kannalta sisäinen valvonta on mallinnettu CIO-Officeen, joka on tietohallintojohtajan esikuntatoiminto, mutta muuten sisäinen valvonta on Tietohallintomallin kannalta ulkopuolinen toiminto.

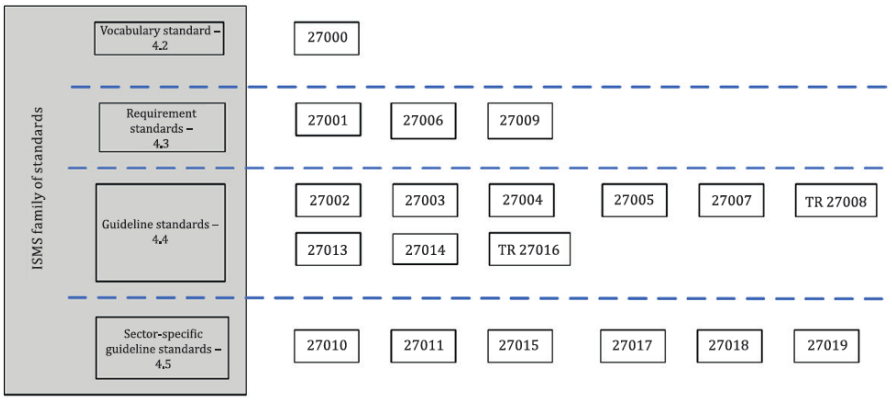
Mikäli yrityksen tietohallinnon johtaminen on rakennettu Tietohallintomallin mukaisesti, tässä opinnäytetyössä kehitettävä ICT Controller -palvelu soveltuu hyvin palvelua hyödyntäväksi asiakasyritykseksi. Kehitetty palvelu tuo selkeää lisäarvoa tietohallinnon tehokkuuden ja vaatimuksenmukaisuuden varmistamiseen.

2.6 Tietoturvan hallintajärjestelmät

ICT Governance -mallit eivät ota kantaa tietoturvan hallintajärjestelmiin tai niiden toteutukseen. EU:n tietosuoja-asetuskaan ei ota kantaa, millainen tietoturvan hallintajärjestelmä yrityksellä tulisi olla. GDPR edellyttää ajantasaista ja tehokasta tietoturvan hallintaa ja asetus asettaa yritykselle toiminnallisia vaatimuksia, jotka yrityksen tulisi hallintajärjestelmissään täyttää. Valtionhallinnon Vahti-ryhmä suosittelee ISO27001-standardin mukaista tietoturvan hallintajärjestelmää GDPR:n vaatimusten täyttämiseksi. (Vahti 2016, 24).

Koska kehitettävästä palvelusta halutaan rakentaa hyvien käytäntöjen mukainen, on suunniteltavan ICT-palvelun perustana tietoturvan hallintamalli ISO/IEC27001 ja soveltuvin osin mukaillaan liiketoiminnan jatkuvuuden hallintamallia ISO/IEC22301. Kyseiset standardit kuvaavat hyvän hallintotavan mukaisen tietoturvallisuuden ja liiketoiminnan jatkuvuuden hallintajärjestelmien vaatimukset.

Kuviossa 12 on esitetty eri standardien suhde toisiinsa nähden. ICT Controller -palvelun kannalta ISO/IEC27001 on olennainen standardi, koska siinä kuvataan tietoturvan hallintajärjestelmän vaatimukset. ISO/IEC27002 antaa kuvaukset referenssitoteutuksesta, mutta kyseistä standardia ei palvelussa standardin laajuuden ja sitovuuden takia huomioida.



Kuvio 12. ISMS-standardiperheen osien suhteet (Suomen standardisoimisliitto SFS 2013a, 25).

ISO/IEC27001-standardia mukaillen rakennettu tietoturvan hallintajärjestelmä täyttää hyvin kehitettävälle ICT Controller -palvelulle asetetut tavoitteet. Se tarjoaa tietoturvan

hallinnan prosessien läpinäkyvyyden yrityksen johtoon muun muassa johdon katselmusten kautta, se varmistaa johdon sitoutumisen EU:n tietosuoja-asetuksen mukaiseen tietosuojan ylläpitoon ja kehittämiseen sekä tarjoaa prosessit poikkeamien hallintaan. Lisäksi standardin mukainen toiminta varmistaa hallintajärjestelmän ajantasaisuuden ja vaatimuksenmukaisuuden vuosikellon mukaisten toistuvien tehtävien avulla

Mikäli yrityksen tietoturvan hallintajärjestelmä on rakennettu ICT Controller -palvelun työkalujen avulla, on yrityksellä mahdollisuus hankkia vaatimuksenmukaisuutta kuvaava julkinen ISO/IEC27001-sertifikaatti varsin kohtuullisella panostuksella.

Yrityksellä on mahdollisuus toimia myös muiden standardoitujen toimintamallien mukaisesti. Niiden mukainen toiminta ei ole ristiriidassa kehitettävän palvelun kanssa. Koska kohderyhmäksi valitut asiakasyritykset edustavat pieniä ja keskisuuria yrityksiä, ei muita standardeja otettu mukaan ICT Controller -palvelun viitekehykseen. Yrityksen toimialasta riippuen joidenkin standardien mukaisten toimintamallien käyttöönotto voi käytännössä olla hyvinkin olla perusteltua (esimerkiksi ISO20000, ISO 9000). Liiketoiminnan jatkuvuutta varmistava ISO/IEC22301 BCMS-standardin mukainen sertifiointi on suhteellisen helppo hankkia yritykselle, jonka toiminta on jo sertifioitu ISO/IEC27001:n mukaisesti, samoin ISO31000:n mukainen riskienhallinta sopii täydentävänä ICT Controller -palveluun.

2.7 Palvelulle suositellut tekniset viitekehykset

Edellä olevissa kappaleissa on arvioitu teknisten viitekehysten soveltuvuutta ICT Controller -palvelun käyttöön. Kuviossa 13 on koottu yhteen eri viitekehysten ominaisuuksia kehitettävän palvelun suhteen.

		Pienet yritykset	Keskikokoiset yritykset	Suuret ja globaalit
ICT hallintamallit	COBIT5	-	Sovellettavissa	Suosittu hallintamalli, turvallinen valinta
	Tietohallintomalli	Sovellettavissa pieniin ympäristöihin	Suosittu hallintamalli Suomessa	Riippuu johdon tahtotilasta
Tietoturvan hallintamallit	ISO/IEC27000-perhe	ISO27001-tyyppinen hallintamalli sovellettuna	Standardin ISO27001 mukainen tietoturvan hallinnassa	Koko ISO27000-perheen hyödyntäminen tietoturvan hallinnassa
	Muut (esim NIST)	Harvinaisuutensa takia ei käsitelty		

Kuvio 13. Teknisten viitekehysten soveltuvuus palveluun.

Koska ensisijainen kohderyhmä on pienet yritykset, on niille soveltuva tietoturvan hallinnan viitekehys ISO27001-tyyppinen sovellettu rakenne. Vastaavasti Tietohallintomalliin

pohjautuva rakenne on Suomessa yleinen ja yksinkertaisemman rakenteensa ansiosta helpompi soveltaa. Rakentamalla palvelu näihin standardeihin perustuen voidaan sitä helpommin skaalata myös suurempiin ympäristöihin. Standardoitu palvelu voidaan tuottaa monistamalla ja siten tehokkaammin ts. edullisemmin kuin räätälöity. ICT Controller -palvelun pohjaksi valittiin ISO27001 ja Tietohallintomalli. (Kari 2017b.)

3 ICT Controller -palvelun raportointirakenne

Työssä päädyttiin hyödyntämään sisäisen valvonnan COSO-IC-viitekehystä. COSO-IC-viitekehys koettiin palveluyrityksessä raportointiin paremmin soveltuvaksi kuin COSO-ERM-pohjainen malli. Perusteena oli, että ICT Controller -palvelun asiakkaat kohdeyrityksissä ovat yleensä toimitusjohtajia tai talousjohtajia. (Kari 2017b.)

Tässä opinnäytetyössä kehitettävä palvelun on tarkoitus olla osa yrityksen sisäistä valvontaa. Kuviossa 14 on kuvattu kehitetyn palvelun suhdetta yrityksen sisäisen valvonnan kokonaisuuteen. Suhde on kuvattu COSO-rakenteen ja siihen liittyvien 17 periaatteen avulla. Osatekijät 1 (Ohjausympäristö) ja 5 (Seurantatoimenpiteet) arvioitiin kuuluvan ensisijaisesti yrityksen sisäisen valvonnan vastuulle. Muut osa-alueet nähtiin tarkoituksenmukaiseksi organisoida sisäisen valvonnan ja ICT Controller -palvelun yhteiselle valvontavastuulle.

Tavoitteet	Osatekijät	Ohjausympäristö	1. Organisaatio osoittaa sitoutumista eheyteen ja eettisiin arvoihin	2. Hallitus osoittaa riippumattomuutta	3. Toimiva johto luo rakenteet raportoinnin ja toimivaltuudet	4. Osoittaa sitoutumista tavoitteiden mukaisuuteen	5. Huolehtii henkilöstön sisäisen valvonnan vastuista	Riskein arviointi	6. Organisaatio määrittelee selkeät tavoitteet mahdollistamaan riskien tunnistamisen	7. Organisaatio tunnistaa ja analysoi riskit	8. Organisaatio huomioi väärinkäytösten mahdollisuudet	9. Organisaatio tunnistaa ja arvioi riskit	Valvontatoimenpiteet	10. Organisaatio valitsee ja kehittää valvontatoimenpiteet	11. Organisaatio kehittää valvontatoimenpiteitä	12. Valvontatoimenpiteet toteutetaan politiikkojen ja menettelytapojen avulla	Informaatio ja viestintä	13. Organisaatio tuottaa ja hankkiin relevanttia informaatiota	14. Sisäinen valvonta ja sen roolit viestitään organisaatiossa	15. Organisaatio viestii ulkoisten sidosryhmien kanssa sisäiseen valvontaan vaikuttavista asioista	Seurantatoimenpiteet	16. Organisaatio seuraa ja arvioi jatkuvasti sisäisen valvonnan toimintaa	17. Sisäisen valvonnan puutteista raportoidaan vastuulliselle johdolle
1) Toiminnalliset tavoitteet toimintojen tehokkuus ja tarkoituksenmukaisuus	1. valvontaympäristö	Yrityksen sisäinen valvonta						Yrityksen sisäinen valvonta ICT:n ja GDPR:n osalta myös ICT Controller -palvelu														Yrityksen sisäinen valvonta		
	2. riskien arviointi																							
	3. valvontatoiminnot																							
	4. informaatio ja kommunikaatio																							
	5. seuranta.																							
2) Taloudellinen raportointi taloudellisen raportoinnin luotettavuus	1. valvontaympäristö																							
	2. riskien arviointi																							
	3. valvontatoiminnot																							
	4. informaatio ja kommunikaatio																							
	5. seuranta.																							
3) Lakien ja sääntöjen mukaisuus lakien ja säädösten noudattaminen.	1. valvontaympäristö																							
	2. riskien arviointi																							
	3. valvontatoiminnot																							
	4. informaatio ja kommunikaatio																							
	5. seuranta.																							

Kuvio 14. COSO-kuution sisäiset suhteet ja sisäisen valvonnan painopisteet.

Ohjausympäristö-osatekijän avulla arvioidaan organisaation sitoutumista eheyteen ja eettisiin arvoihin sekä hallituksen riippumattomuutta. Osatekijään kuuluu myös toimivan

johdon luomat rakenteet raportointiin ja toimivaltuuksiin. Samalla kokonaisuudella arvioidaan johdon sitoutumista tavoitteiden mukaisuuteen ja henkilöstön sisäisen valvonnan vastuiden huolehtimisesta. Ohjausympäristö-osatekijä katsottiin kuuluvan ensisijaisesti yritystason sisäisen valvonnan arvioitavaksi. Kehitettävän palvelun osalle jää yritystason mallien toimeenpanon arviointi tietohallinnon organisaatiossa.

Riskien arviointi -osatekijästä katsottiin, että yrityksen sisäinen valvonta vastaa yritystason riskien arvioinnin kokonaisuudesta ja kehitettävä ICT Controller -palvelu vastaa osatekijän toimeenpanosta tietotekniikassa. Toimeenpanossa organisaatio määrittelee selkeät tavoitteet mahdollistamaan riskien tunnistamisen myös tietotekniikassa ja edellyttää samalla kehitettävän palvelun tunnistamaan ja analysoimaan riskit tietotekniikan osalta. Toteuttaessa arviointia kehitettävän palvelun tulee ottaa arvioinnissaan huomioon teknisten riskien lisäksi myös väärinkäytösten mahdollisuudet sekä tunnistaa ja arvioida niihin liittyvät riskit.

Valvontatoimenpiteet-osatekijä on myös yhteisesti yrityksen sisäisen valvonnan ja ICT Controller -palvelun vastuulla oleva osatekijä. Yritystason sisäinen valvonta valitsee ja kehittää valvontatoimenpiteet yritystasolle ja vastaavasti kehitettävä palvelu tietoteknisille toiminnoille. Kumpikin vastaa valvontatoimenpiteiden ja poliitikkojen kehittämisestä ja valvonnasta omalla vastuualueellaan.

Edellisten osatekijöiden mukaisesti Informaatio ja viestintä -osatekijä organisoidaan vastaavalla tavalla. Yritystaso vastaa kokonaisuudesta, ja ICT Controller -palvelu hoitaa tietotekniikkaan liittyvän sisäisen valvonnan. Tavoitteena on tuottaa ja hankkia relevanttia informaatiota. Lisäksi tavoitteena on viestiä sisäinen valvonnan sekä kehitettävän palvelun roolit organisaatiossa niin yrityksen sisällä kuin ulkoisten sidosryhmienkin kanssa.

Koska kehitettävä palvelu on yrityksen kannalta ostopalvelu, sisäisen valvonnan seurantatoimenpiteet-osatekijä osuu luontevasti yrityksen sisäisen valvonnan vastuulle. Seurantatoimenpiteillä yritys seuraa ja arvioi sisäisen valvonnan kokonaisuuden toimintaa, ja arvinointi sisältää myös ICT Controller -palvelun arvioinnin ja raportoinnin sen kehityskohteista ja puutteista.

ICT Controller -palvelussa päädyttiin raportoimaan COSO-IC:n mukaisesti jakaen raportointi kolmeen kokonaisuuteen (Ratsula 2016, 60):

1) Toiminnalliset tavoitteet: Arvioidaan organisaation resurssien käytön tarkoituksenmukaisuutta ja käytön tehokkuutta. Tavoite toteutuu, kun käytetään resursseja tarkoituksenmukaisesti ja tehokkaasti.

2) Taloudellinen raportoinnin tavoitteet: Raportointi onnistuu, kun ylimmällä johdolla sekä muulla johdolla on päätöksentekoa varten luotettavaa tietoa oikea-aikaisesti ja ulkoiset sidosryhmät voivat luottaa taloudelliseen tietoon.

3) Lakien ja sääntöjen mukaisuuden tavoite toteutuu, kun organisaatiossa noudatetaan lakeja ja itselleen luotuja sääntöjä ja toimintatapoja.

COSO-IC-viitekehyksen mukaista raportointia kehitettäessä linjattiin, että raportointi muotoillaan kolmeen pääryhmään: 1 Toiminnalliset tavoitteet, 2 Taloudellinen raportointi ja 3 Lakien ja sääntöjen mukaisuus. Osatekijät (1 Valvontaympäristö, 2 Riskien arviointi, 3 Valvontatoiminnot, 4 Informaatio ja kommunikaatio sekä 5 Seuranta) mallinnetaan osaksi ICT Controller -palvelun toiminnallista kuvausta. COSO-periaatteista (17 kpl) muodostetaan tarkistuslistat raportoinnin muodostamista varten.

4 Tyypillinen palvelun käyttöönotto

4.1 Palvelun käynnistys

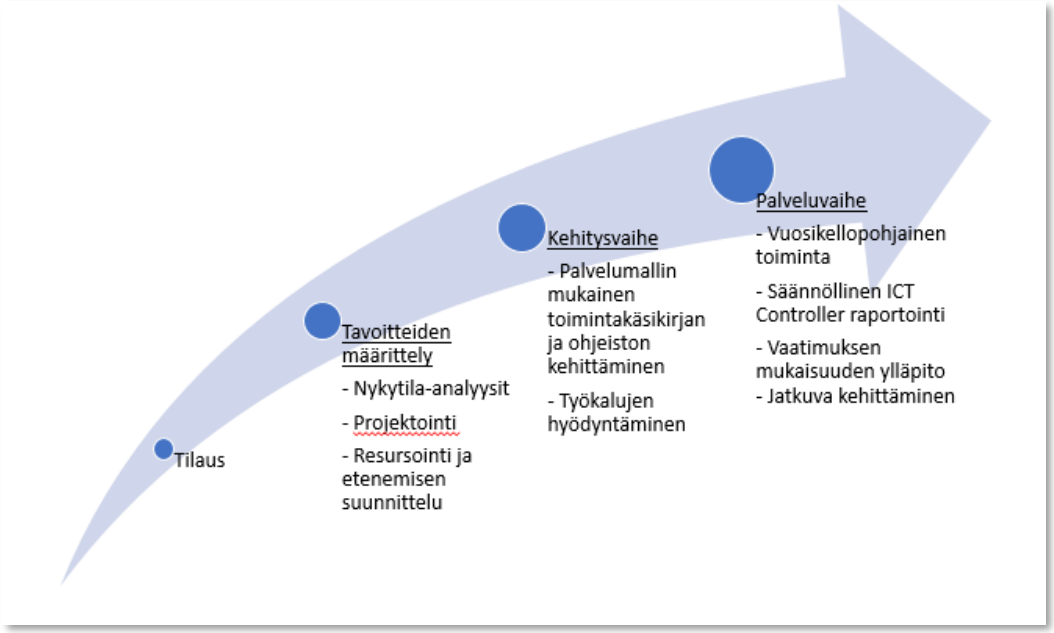
Luvussa 3 esiteltiin ICT Controller -palvelun tavoitteellinen raportointi COSO-IC-mallin mukaisesti. Jotta raportointi voidaan tuottaa jatkuvana palveluna, tulee yrityksen ohjeisto ja prosessit useimmiten arvioida, kehittää ja dokumentoida. Vuonna 2016 tehdyn tutkimuksen mukaan yritysten tietohallinnon prosessit oli noin kolmanneksella (34 prosenttia) täysin määritelty ja 42 prosentilla osin määritelty. Vastaajista 24 prosentilla prosesseja ei ollut määritelty tai vastaajilla ei ollut tietoa asiasta. Kehitettävän palvelun kannalta kahdella kolmasosalla yrityksistä on tarvetta kehittää tietohallinnon prosesseja. (Kolesnik ym. 2016, 16.)

Tutkimuksen perusteella yritykset eivät oletettavasti ole lähtötilanteessa valmiita prosessiensa puolesta toimimaan riittävällä mitattavuuden ja raportoinnin tasolla. Siksi palvelun käynnistysvaiheessa tarvitaan ohjeistuksen tilan arviointi ja soveltuvin osin prosessien kunnostus ja päivitettyjen toimintamallien käyttöönotto. Kuviossa 15 kuvataan tyypillinen

palvelun käyttöönottoprojektin eteneminen ohjeiston kunnostamiseksi ennen varsinaisen ICT Controller -palvelun käynnistämistä.

4.2 Palvelun hankinnan vaiheet

Palvelun hankinta käynnistyy myyjän ja asiakkaan välisillä myyntineuvotteluilla. Mikäli neuvotteluissa päädytään tilanteeseen, jossa ICT Controller -palvelu ja sen käynnistämiseen liittyvä kehitysvaihe kiinnostavat asiakasta, pyritään projekti käynnistämään matalalla kynnyksellä siten, että asiakas tilaa tiiviin kahdesta kolmeen konsultointipäivää kestävän alkukartoituksen.



Kuvio 15. Palvelun käynnistäminen ja jatkuva palvelu.

Alkukartoituksessa määritellään palvelun tavoitteet, suunnitellaan projekti ja arvioidaan tarvittava resursointi asiakkaan ja palvelun toimittajan taholta. ICT Controller -toiminta vaiheistuu sen jälkeen kahteen osaan. Palvelun tilaamisen ja tavoitteiden asettamisen jälkeen ensimmäinen vaihe on kehitysvaihe, jota seuraa palveluvaihe. Kehitysvaiheessa palveluyritys rakentaa yritykselle ICT Controller -toiminnon, jonka tärkein tavoite on varmistaa asiakasyrityksen EU:n tietosuoja-asetuksen ja tulevan tietosuojalainsäädännön mukaisen vaatimuksenmukaisuuden saavuttaminen. Palveluvaiheessa kehitetty palvelu jatkaa kontrolleripalveluna, jossa raportoidaan sisäisen valvonnan periaatteiden mukaisesti yrityksen johdolle niin ICT:n tila tietoturvan ja liiketoiminnan jatkuvuuden kannalta kuin myös koko yrityksen EU:n tietosuoja-asetuksen vaatimuksenmukaisuuden suhteen.

4.3 Kehitysvaihe

Kehitysvaiheessa kunnostetaan yrityksen tietohallinnon toiminnan keskeiset ohjeet ja rakennetaan ICT Controller -toiminto pohjautuen opinnäytetyössä tuotettuihin työkaluihin. Ohjeiston kehittämiseen luotiin kaksi eritasoista työkalua: kevyt ja laaa

Laajemmalla työkalulla (Liite 1 ICT Controller -ympäristön rakentaminen asiakkaalle) rakennetaan asiakkaalle päivitetty ohjeisto ja prosessit projektimallia hyödyntämällä. Liitteen työkalussa on kuvattu kehitysprojektin organisointi ja vaiheistus sekä tarvittavat analyysit nykytilan ja tavoitetilan kuilun määrittelemiseen. Kevyemmällä työkalulla (Liite 2 Dokumentoinnin kehittäminen √-mallin avulla) ohjeisto ja toimintamallit kehitetään suoraan konsulttityönä asiakkaan työnjohdossa.

Kumpaakin mallia hyödyntäessä tulee huomioida asiakasyrityksen liiketoiminnan erityisvaatimukset ja alan muu säännöstö. ICT Controller -toiminnon organisointia varten päivitetään opinnäytetyössä luotu ohjerunko (Liitteen 4 ICT Controller -toiminnan ja Turvatoiminnon ohje) asiakasympäristöön sovitettua palvelua varten. Palveluvaiheeseen siirryttäessä miehitetään luotu ICT Controller -organisaatio ja käynnistetään sen toiminta. Vaiheessa hyödynnettävät työkalut ovat palvelun käyttöönoton projektimalli (Liite 1), ohjeiston kehittämisen √-malli (Liite 2) sekä ICT Controller -toiminnan ja Turvatoiminnon ohje (Liite 4).

4.4 Palveluvaihe

Palveluvaiheen tavoitteena on ylläpitää ICT Controller -palvelua kustannustehokkaalla tavalla. Palvelun toteuttamisen tulee olla mahdollisimman kevyt ja tuotteistettu niin, että jatkuvat kustannukset asiakkaalle pysyvät tavoitteen rajoissa.

Palvelua ohjataan vuosikellolla, josta toistuvat tehtävät käynnistetään ennalta suunnitellusti. Vuosikellon mukaiset toistuvat tehtävät ovat GDPR-yhteensopivuusarviointi, ICT Governancen kypsyysanalyysi, Tietotilinpäätöksen sekä ICT Controller -raportin tuottaminen (COSO-IC -raportti). Lisäksi tehdään säännöllinen riskinarvioinnin päivitys, käyttöoikeuksien tarkistus. Kunkin tehtävän tuloksista poimitaan kehityskohteet, jotka kootaan yrityksen kehitysroadmapille.

4.5 Yhteenveto palvelun käyttöönotosta

ICT Controller -palvelun asiakkaat voivat edustaa hyvin eri kypsyystasoilla olevia yrityksiä. Palvelun käyttöönottoprojektin laajuutta voidaan tarvittaessa sopeuttaa siten, että kuilu nykytilan ja tavoitetilan välillä poistuu. Palvelun kehitysvaiheessa tavoitteena on päivittää yrityksen ohjeisto ja toimintaprosessit yrityskohtaisen tilanteen mukaisesti siten, että saavutetaan GDPR-yhteensopivuus ja toimiva tietoturvan hallintajärjestelmä.

Kehitysvaihe on aina yrityskohtainen ja siten yksiköllinen. Palveluvaihe on asiakkaille standardoitua palvelutoimintaa, jossa ICT Controller -palvelun tehokkuus saavutetaan eri asiakkaille toimitettavien yhtenäisten toimintamallien avulla.

5 Kehitetyt työkalut

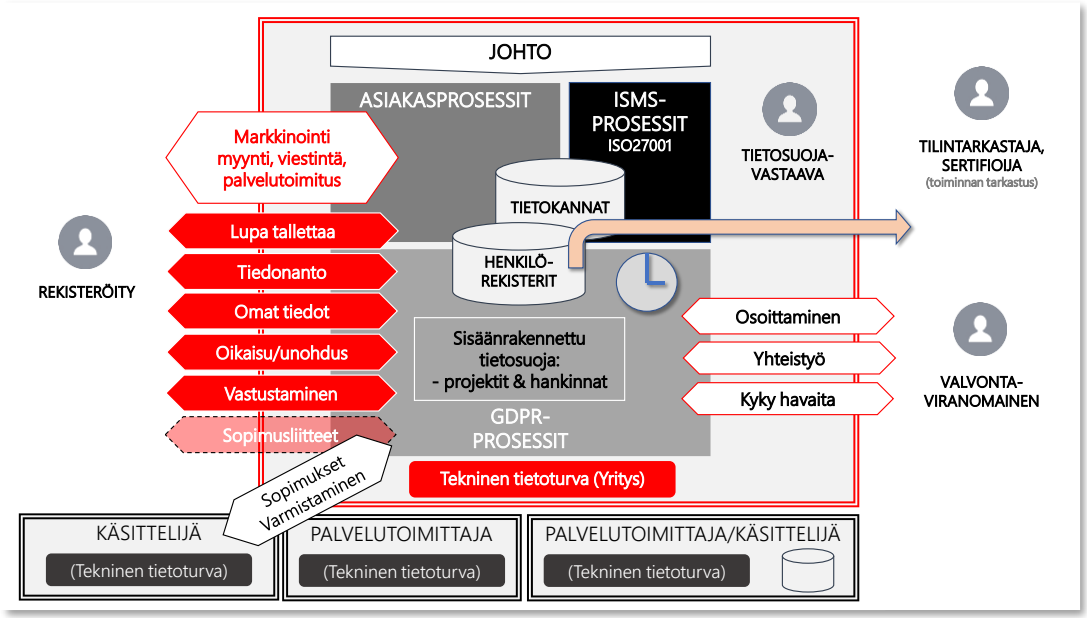
5.1 Tavoitteena kustannustehokas palvelun käynnistäminen

Palvelun käyttöönoton helpottamiseksi ja aloituskustannusten kurissa pitämiseksi tässä opinnäytetyössä kehitettiin ICT Controller -palvelun runko sekä sitä varten työkalut palvelun käynnistämiseksi ja tuottamiseksi. Työssä nähtiin tarpeen kehittää myös tarvittavat apuvälineet, joiden avulla ICT Controller -toiminto rakennetaan sellaiseenkin asiakasyritykseen, jonka toiminnan kypsyystaso ei alun perin tue prosessien mittaamista.

Palvelurunkojen ja työkalujen avulla saadaan markkinointiin ja viestintään palveluasenne ja myytävää sisältöä. Asiakkaat saavat palvelukuvauksen mukaisen, suunnitellun palvelun ja asiakaskohtainen räätälöinti vähenee.

5.2 GDPR:n vaatimuksenmukaisuuden analyysi

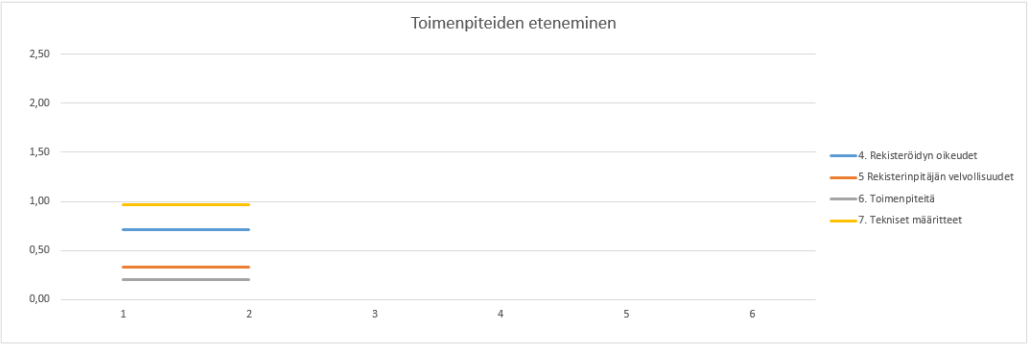
Yksi ICT Controller -palvelun keskeisistä päämääristä on varmistaa yrityksen EU:n tietosuoja-asetuksen vaatimusten täyttyminen. Kaikilla yrityksillä toiminta ei ole vielä lähtötilanteessa vaatimukset täyttävää. Yrityksen tilanne kartoitetaan käynnistysvaiheessa opinnäytetyön toimeksiantajayrityksen aiemmin kehittämän ja opinnäytetyössä jatkokehitetyn GDPR-analyysityökalun avulla. Analyysissä raportoidaan kehityskohteet kuvion 16 mukaan jaoteltuna. Vaatimuksenmukaisuuden tila arvioidaan eri toiminta-alueille: Rekisteröidyn GDPR-prosessit, käsittelijöiden GDPR-prosessit, viranomaisprosessit sekä yrityksen sisäiset GDPR-prosessit.



Kuvio 16. GDPR-vaikutukset yrityksen toimintaan.

Analyysityökalu perustuu Vahti-ryhmän luomaan arviointityökaluun, jota palveluyrityksessä on täydennetty kattamaan myös tekninen tietoturva. Analyysityökalua on täydennetty myös raportoinnin osalta ja siten työkalua voidaan käyttää myöhemmin vaatimuksenmukaisuuden kehittymisen seurantaan koko kehitysvaiheen aikana.

Toimenpiteiden eteneminen			Arvio kvartterin lopussa					
Osa-alue	Lähtötila	Arvio	Analyysi	Q1-2018	Q2-2018	Q3-2018	Q4-2018	Q1-2019
4. Rekisteröidyn oikeudet	0,89	25% valmiusaste	0,71	0,71				
5 Rekisterinpitäjän velvollisuudet	0,55	25% valmiusaste	0,33	0,33				
6. Toimenpiteitä	0,35	25% valmiusaste	0,20	0,20				
7. Tekniset määritteet	1,19	75% valmiusaste	0,97	0,97				
Kokonaisuus	0,74	25% valmiusaste	0,55	0,55				
			pp.kk.2018	(ei arvioitu)				



Kuvio 17. Esimerkkiraportti yrityksen GDPR-vaatimuksenmukaisuudesta.

Kuviossa 17 esitetyssä raporttimallissa nähdään vaatimuksenmukaisuuden nykytilan raportti ja sen etenemistä pystytään jatkossa seuraamaan uusinta-analyyseillä tarkistuspisteestä toiseen. Graafisen esityksen lisäksi analyysin tuloksena asiakkaille tuotetaan sanallinen arvio ja kehitysehdotukset roadmapin muodossa.

5.3 Tietoturvan ja toiminnan jatkuvuuden analyysi

Kehittämisvaiheessa on usein perusteltua tehdä myös tietoturvan ja liiketoiminnan jatkuvuuden analyysi. Analyysissä kartoitetaan yrityksen toiminnan tietoturvan ja toiminnan jatkuvuuden taso. Analyysissä hyödynnetään palveluyrityksen aiemmin kehitettyjä ja opinnäytetyössä jatkokehitettyjä teknisiä arviotyökaluja.

Analyysissä tunnistetaan yrityksen tietovarastot ja niiden osalta toiminnan jatkuvuuden edellytykset. Analyysissä dokumentoidaan tietovarastot ja tuloksena kootaan yhteenveto, jossa kuvataan tietovaraston tai palvelun nimi, prioriteetti ja tärkeys yrityksen toiminnalle, mahdollisten varajärjestelyjen kuvaus sekä palautumisaika häiriötilanteissa. Analyysissä arvioidaan myös mahdollinen toipumaton aikaikkuna (ts. häiriötilanteessa menetetyt tapahtumat) tehdään liiketoimintavaikutusten yhteenveto.

Teknisen tietotekniikkaympäristön osalta kartoitetaan seuraavat kokonaisuudet: Pääsynhallinta ja salaukset, palomuurit ja verkko. Lisäksi kartoitetaan päivitysten hallinta, verkon palvelut ja kyky havaita tunkeutuminen ja tiedon vuotaminen. Olennainen osa analyysia on arvioida asiakasyrityksen dokumentaation taso. Analyysi suoritetaan haastattelemalla yrityksen avainhenkilöitä ja mahdollisia toimittajia työpajassa. Työpajan jälkeen asiakasyritykselle toimitetaan raportti analyysin tuloksista ja tehdään kehityssuositukset.

Liitteessä 3 (Tietoturvan ja liiketoiminnan jatkuvuuden varmistaminen) on kuvattu kehittämismalli, jolla yrityksen tekninen toimintaympäristö ja ohjeistus parannetaan ICT Controller -palvelun edellyttämälle tasolle.

5.4 Palvelun käyttöönoton projektointi

Kehittämisvaiheessa hyödynnetään palvelun käyttöönottoon kehitettyä projektointimallia. Kehitetty malli soveltuu asiakasyrityksiin, joissa muutokseen osallistutetaan useita asiantuntijoita ja kehittäminen on syytä tehdä projektina hyödyntäen ohjaus- ja projektiryhmätyöskentelyä.

Alla yhteenveto ja karkean tason suunnitelma kehittämistyön päävaiheista. Vaiheet toteutetaan peräkkäin alla esitetyssä järjestyksessä. Kokonaisuuden läpivienti kestää arviolta 3 kuukautta. Projektointimalli on kuvattu tarkemmin liitteessä 1 (ICT Controller -ympäristön rakentaminen asiakkaalle). Läpivienti vaiheistetaan seuraavasti:

1. Yrityksen nykytilan arvio haastattelujen avulla.
2. Nykytilan arviointi ja yhteenveto haastattelutulosten avulla.
3. Kuilu-analyysi nykytoiminnan ja vaatimusten välillä (GDPR, ISO-standardit, COSO-raportointi).
4. Tavoitetason asettaminen kuiluanalyysin perusteella yhdessä asiakasyrityksen johdon kanssa.
5. Tarvittaessa tehdään GDPR-vaatimusten mukaisten prosessien suunnittelu, dokumentointi ja käyttöönotto.
6. COSO-IC:n mukaisten sisäisen valvonnan prosessien suunnittelu, dokumentointi ja käyttöönotto.
7. Mahdollisten ISO27001- ja/tai ISO22301-kehitysprojektien käynnistäminen erillisinä hankkeina.
8. Jatkuvan raportoinnin ja kontrolloinnin organisointi osaksi yrityksen toimintaa.
9. Toimeenpanoprojektin lopetus.

5.5 Ohjeiston kehittämismalli (√-malli)

Kehittämisvaiheessa voidaan hyödyntää myös kevyempää ohjeiston kehittämiseen luotua niin kutsuttua √-mallia. Kehitetty malli soveltuu asiakasyrityksiin, joissa muutokseen ei tarvitse osallistuttaa useita asiantuntijoita, vaan kehittäminen tehdään yksilötyönä asiakkaan ohjauksessa.

Tässä kevyessä √-mallissa ohjeiston kehitysvastuu on nimetyllä työn ohjaajalla. Kehitysmalli on tehokas, mutta sen sitouttava vaikutus on ymmärrettävästi rajallinen. Toimintamalli on kuvattu Liitteessä 2 (Dokumentoinnin kehittäminen √-mallin avulla).

5.6 ICT Controller -toiminnan ohje

Palveluvaiheessa viimeistellään ICT Controller -yksikön toimintaohjeet opinnäytetyössä tehdyn ohjeistorungon avulla. Rungossa kuvataan asiakasyritykseen perustettava mat-

riisiyksikkö, Turvatoiminto, joka vastaa ICT Controller -palvelun toteuttamisesta. Rungossa Turvatoiminto on rakennettu hyvien sisäisen valvonnan periaatteiden mukaisesti muusta organisaatiosta erilliseksi riippumattomaksi toiminnoksi, joka raportoi yrityksen johdolle.

ICT Controller -palvelua varten kehitetty Turvatoiminnon ohjerunko on liitteessä 4 (ICT Controller ja Turvatoiminnon ohje). Kuvattu toimintamalli täyttää EU:n tietosuoja-asetuksen edellyttämät vaatimukset. Rakenteessa on pyritty huomioimaan toisaalta pienen yrityksen resurssirajoitteet ja toisaalta ISO/IEC27001-näkökulma ja siten rakentamaan toimiva tietoturvan hallintajärjestelmä.

EU:n tietosuoja-asetuksen määrittelemältä tietosuojavastaavalta edellytetään seuraavaa ammattitaitoa ja osaamista. Alla lainaus dokumentista 16/FI WP 243 rev.01 Tietosuojavastaavia koskevat ohjeet (European Commission 2017b, 25), jotka tulee ottaa huomioon palvelun henkilöstöä rekrytoitaessa:

> Tietosuojavastaavan ammattitaitoon ja asiantuntemukseen kuuluvat seuraavat:
> - asiantuntemus kansallisesta ja EU:n tietosuojalainsäädännöstä ja alan käytänteistä, myös yleisen tietosuoja-asetuksen perusteellinen tuntemus
> - suoritettujen käsittelytoimien tuntemus
> - tietojärjestelmien ja tietoturvan tuntemus
> - asianomaisen toimialan ja organisaation tuntemus
> - valmiudet edistää tietosuojakulttuuria organisaatiossaan.

5.7 Tietotilinpäätös

Palveluvaiheessa ICT Controller -palvelu tuottaa dokumentaation, jonka avulla asiakas voi osoittaa EU:n tietosuoja-asetuksen vaatimuksenmukaisuuden. Keskeinen dokumentti vaatimuksenmukaisuuden osoittamisessa on tietotilinpäätös. Tietotilinpäätös on asiakaskohtaisesti räätälöity yhteenveto kuluneen jakson aikana tapahtuneista tietosuojatapahtumista ja se sisältää myös kuvauksen tietosuojan varmistamiseksi luoduista prosesseista ja toimintamalleista.

Tietosuojavaltuutetun ohje LAADI TIETOTILINPÄÄTÖS (Tietosuojavaltuutetun toimisto 2012, kappale 1) kirjaa seuraavat linjaukset tietotilinpäätöksen sisällöstä:

> Tietotilinpäätös on osa tietojohtamista ja sitä voidaan käyttää organisaation sisäisenä tietojohtamisen raporttina. Tietotilinpäätöksellä voidaan myös raportoida organisaation sidosryhmille tietojen käsittelyä koskevista keskeisistä asioista.

Tietotilinpäätös on organisaation sisäisen tarkastelun tuloksena syntyvä raportti, joka esimerkiksi:

- antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta
- kuvaa mitä tietovarantoja organisaation hallussa on
- kuvaa organisaation toimintaan liittyvät tietovirrat
- kuvaa organisaation tietovirtojen yhteentoimivuuden tietojenkäsittelyn kanssa
- kuvaa miten tietosuoja ja -turva toteutuvat organisaation toiminnassa
- kuvaa miten tietojenkäsittelyyn liittyvä riskienhallinta on toteutettu
- toimii suunnittelun ja toiminnan ohjauksen tukena organisaatiossa
- toimii raportoinnin ja johtamisen tukena organisaatiossa
- toimii kehittämistoimenpiteiden seurannan apuvälineenä
- toimii organisaatiosta ulospäin tapahtuvan sidosryhmäraportoinnin välineenä
- varmistaa sovellettavan lainsäädännön noudattamisen

ICT Controller -palveluun kuuluu tietotilinpäätöksen tuottaminen kultakin vuodelta. Tietotilinpäätös tehdään Tietosuojavaltuutetun toimiston ohjeita hyödyntäen. Tätä opinnäytetyötä kirjoitettaessa ei valitettavasti ollut käytettävissä ajantasaisia ohjeita, vaan ohjeistus oli vielä vanhan lainsäädännön mukaista (Julkaistu 24.4.2012). Osana ICT Controller -palvelun jatkokehitystä määritellään tietotilinpäätös, joka noudattaa uutta vielä julkaisematonta ohjeistusta.

6 COSO-IC-mallia hyödyntävä ICT Controller -raportointi

6.1 Toiminnallisuuden raportointi

COSO-IC- ja COSO-ERM-mallien sopivuutta arviointiin palvelutoimittajan palveluun tarpeisiin nähden. Toimeksiantaja-yritys valitsi COSO-IC-mallin ICT Controller -palvelun jatkuvan palvelun raportoinnin pohjaksi (Kari 2017b).

Tietohallinnon toiminnalliset tavoitteet ovat tavoitteita, jotka liittyvät organisaation resurssien tarkoituksenmukaiseen ja tehokkaaseen käyttöön. Resursseilla tarkoitetaan tässä yhteydessä niin henkilöitä, tekniikan kapasiteettia kuin rahallisiakin resursseja.

Toiminnallisuuden raportoinnin osa-alueet ovat seuraavat:

1. Tietotekniikan ylläpidon prosessien toiminta: tuotannon häiriöt ja poikkeamat.
2. Tietoteknisten kehitysprojektien arviointi: suunnitellut tavoitteet verrattuna toteutuneisiin tavoitteisiin, aikataulujen ja budjettien pitävyys.
3. Tehdyt riskiarvioinnit.
4. Tietojärjestelmien käyttöoikeuksien tarkistusten toteutus.
5. Varmistusten palautustestien ja poikkeustilanneharjoitusten tulokset.
6. Tietohallinnon prosesseja arvioivien sisäisten auditointien tulokset.

Mittarit, joilla seurataan toiminnan trendejä ovat järjestelmien käytettävyys, ongelmien ja häiriöiden määrät, muutosten määrät, häiriöön päätyneiden muutosten määrä ja henkilöstön ylitöiden määrät. Lisäksi mitataan henkilöstön ajankäytön kohdentumista ei tehtäviin.

6.2 Talouden raportointi

Talouden raportoinnin ja mittaamisen osa-alueet koostuvat budjettien seurannasta (kulu- ja investointibudjettien tilanne), tulevaisuuteen sidottujen menojen seurannasta (leasingit, palvelusopimukset) sekä talouden hallintaa arvioivien sisäisten auditointien tuloksista. Erityisesti arvioidaan ennustettavissa oleva kulurakenne sekä kehitysprojekteihin sitoutunut pääoma ja saavutetut hyödyt.

6.3 Lakien ja sääntöjen mukaisuuden raportointi

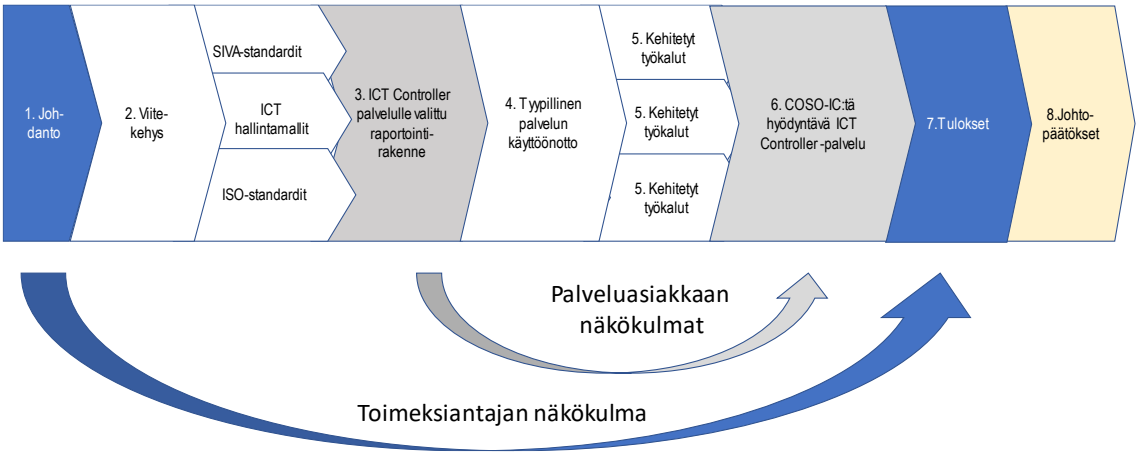
Lakien ja sääntöjen raportoinnin osa-alueet koostuvat seuraavista kokonaisuuksista:

1. Johdon katselmusten tulokset
2. EU:n tietosuoja-asetuksen (GDPR) noudattaminen
3. Kansallisen lain noudattamien
4. Uusien EU-asetusten huomiointi (GDPR-tarkennukset, ePrivacy)
5. Uusien kansallisten määräysten huomiointi
6. GDPR-prosessien raportointi
7. Tietosuoja-tapahtumien ja rikkeiden raportointi
8. Tietotilinpäätöksen toimittaminen johdolle
9. Tietohallinnon vuosikertomuksen toimittaminen johdolle
10. Tietosuojaprosessien kehitystarpeiden raportointi
11. Säännöllisen riskiarvioinnin tulokset
12. Vuosikellon mukaisen toiminnan raportointi
13. Toiminta- ja turvajärjestelmien auditointien tulokset
14. Ulkoisten auditointien tulosten raportointi.

Mittareina käytetään tietosuojatapahtumien ja rikkeiden määrä sekä GDPR-prosessien toiminnallisia mittareita.

7 Tulokset

Seuraavassa kuviossa 18 kuvataan, miten opinnäytetyön raportoinnin rakenne tukee palvelun kehitysprojektille asetettuja tavoitteita.



Kuvio 18. Opinnäytetyön eteneminen.

Toimeksiantajayrityksen lähtökohdista arvioitiin, että johdon epävarmuus tietohallinnon toiminnasta voidaan muuttaa palveluyrityksen liiketoiminnaksi. Toinen opinnäytetyön aikana tehty keskeinen päätelmä oli, että teknisistä viitekehyksistä oli hyötyä palvelun kehittämisessä. Kolmantena linjauksena toimeksiantaja päätti, että palvelussa raportoidaan COSO-viitekehyksen avulla.

Tehtyjen linjausten perusteella tässä opinnäytetyössä kehitettiin ICT Controller -palvelun runko sekä sitä varten työkalut palvelun käynnistämiseksi ja tuottamiseksi. Työssä luotiin myös tarvittavat apuvälineet, joiden avulla ICT Controller -toiminto rakennetaan sellaiseen asiakasyritykseen, jonka ohjeistuksen ja prosessien kypsyystaso ei alun perin olisi tukenut prosessien mittaamista. Lisäksi opinnäytetyössä päivitettiin palveluyrityksen työkaluja GDPR:n vaatimuksenmukaisuuden sekä tietoturvan ja toiminnan jatkuvuuden osalta.

Onnistuneen opinnäytetyön läpiviennin avulla saatiin rakennettua palvelumalli, joka on riittävän kevyt ja monistettavissa useisiin pienen ja keskisuuren sektorin yrityksiin. Onnistuneen kehityssuunnitelman läpiviennin kautta ICT Controller -palvelun rooli ja siihen liittyvät toimintamallit kehittyvät pilotointivalmiiksi ja palvelun koemarkkinointi voidaan

aloittaa. Jatkon osalta olennainen vaatimus kehityssuunnitelman läpiviennille asiakasyrityksissä on tasapainon löytäminen rakennetun ICT Controller -palvelun jatkuvien kustannusten ja asiakkaan kokemien hyötyjen välillä. (Kari 2018)

Kehitetylle palvelulle asetettiin tavoitteeksi tuottaa palvelu, jossa on seuraavat ominaisuudet:

1. Kustannukset asiakasyritykselle voivat olla: 6 000 euroa – 18 000 euroa vuodessa. Työmääräksi muutettuna palvelu pitää tuottaa 0,5–1,5 henkilötyöpäivän panoksella kuukaudessa.
2. Raportoinnin tulee kuvata tietoturvan ja tietosuojan tilaa yrityksessä sekä toiminnan vaatimuksenmukaisuutta yleisjohdon ymmärtämällä tavalla.
3. Raportoinnin tulee täyttää GDPR:n vaatimuksenmukaisuuden osoittamiseksi tarvittavan dokumentaation.
4. Lisäksi tulee mahdollistaa mahdollisuus kohdeyrityksen sertifioitumiseen ISO/IEC27001-standardin mukaisesti erillisenä jatkokehityksenä.

ICT Controller -palvelun jatkokehitykseen jäivät riskityökalun ja ohjeistuksen kehittäminen, tietoturvan tiketöintityökalun parametrointi sekä palveluun soveltuvan auditointiohjeen tuottaminen. Jatkokehitys on mahdollista tehdä ensimmäisten pilottiasiakkuuksien yhteydessä.

Projektin asetannassa ulos rajattuun talouden raportointiin liittyen huomioitiin, että tietohallinnon ja tietotekniikan talouden hallinnassa on joitain erityispiirteitä, esimerkiksi lisenssien ja ohjelmistojen käyttöoikeuksien hallinnan monimutkaisuus ja runsas leasingrahoitusmallien käyttö, joten niiltä osin talousseurannan alueet tullaan jatkossa todennäköisesti liittämään ICT Controller -palvelussa raportoitavaan kokonaisuuteen (Kari 2018).

8 Johtopäätökset

Toimeksiantajayrityksen lähtökohdista tärkein arvioitava liiketoiminnallinen asia oli se, voidaanko johdon epävarmuus tietohallinnon toiminnasta muuttaa palveluyrityksen liiketoiminnaksi. Nyt opinnäytetyön valmistuttua näyttää siltä, että kuvatulle palvelulle on kysyntää ja epävarmuus voidaan siten muuttaa liiketoiminnaksi. Toinen arvioitava näkökulma oli se, onko teknisistä viitekehyksistä hyötyä palvelulle kehittämisessä. Potentiaa-

listen asiakkaiden kanssa käytyjen keskustelujen perusteella näyttää ilmeiseltä, että laatuorientoituneille asiakkaista viitekehys on erittäin tärkeä, kun taas useimmille asiakkaille viitekehyksellä ei ole sittenkään käytännössä liiketoiminnallista merkitystä. Kolmas arvioitava kokonaisuus on se, kannattaako palvelussa raportoida COSO-viitekehyksen avulla vai räätälöidysti. COSO-viitekehys vaikuttaa asiakkaissa heikosti tunnetulta ja sen arvo on lähinnä markkinoinnillinen.

Nyt opinnäytetyön valmistuttua ovat mielestäni suurimpina riskeinä palvelun jatkossa seuraavat haasteet: Pilottiasiakkaiden hankkimisen haasteena on rakennetun ICT Controller -palvelun poikkeavuus aiemmista toimintamalleista. Rakennettu palvelu poikkeaa perinteistä talouskeskeisestä controller-toiminnasta. Syntynyt rakenne voi tuntua kohderyhmälle liian monimutkaiselta ja raskaalta. Jatkokehityksen tavoitteiksi tulisi siksi asettaa käyttöönottoprojektin ja myös dokumenttirunkojen yksinkertaistamisen.

Sopivimpia pilottiasiakkaita palvelulle ovat sellaiset asiakkaat, jotka oman liiketoimintansa edistämiseksi haluavat sertifioida oman toimintansa ISO/IEC27001-mukaisesti toimittaakseen omia palvelujaan edelleen omille asiakkailleen.

Opinnäytetyö eteni muiden tehtävien lomassa tekijän mielestä turhankin hitaasti. Nyt työn tekemiseen kului kaiken kaikkiaan noin yksi kalenterivuosi. Aikataulua olisi ollut mahdollista lyhentää 3–6 kuukaudella, jos työhön olisi pystynyt keskittynyt suuremmalla panoksella. Toisaalta työn pidentyneellä tekoajalla ei tiettävästi ollut muita haitallisia sivuvaikutuksia. Nyt työn tehtyäni haluan lämpimästi kiittää työn ohjaajia niin koulussa kuin työympäristössänikin.

Lähteet

Asetus 2016/679. 2016. Euroopan parlamentti ja neuvosto. Julkaistu 4.5.2016. Http://eur-lex.europa.eu/legal-content/fi/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Luettu 15.7.2017.

European Commission 2017a. Euroopan parlamentti ja neuvosto. Ehdotus - Asetus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus). Julkaistu 10.1.2017. Http://eur.lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A52017PC0010. Luettu 15.4.2017.

European Commission 2017b. Guidelines on Data Protection Officers ('DPOs') (wp243rev.01). Julkaistu 30.10.2018. Http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>. wp243rev01_fi.pdf. Luettu 14.4.2018.

Helsingin yliopisto 2009. Tietotekniikkaosasto/Tietohallinto. Korkeakoulujen kokonaisarkkitehtuurin käsikirja. Korkeakoulujen kokonaisarkkitehtuurin käsikirja. Toiminnan ja tietohallinnon kokonaisvaltainen kehittäminen. http://www.helsinki.fi/julkaisut/aineisto/hallinnon_julkaisuja_65_2009.pdf. Luettu 14.4.2018.

Henkilötietolaki 22.4.1999/523. Edilex. http://www-edilex-fi.ezproxy.metropolia.fi/lainsaadanto/19990523?allWords=henkil%C3%B6tietolaki&offset=1&perpage=20&sort=relevance&searchSrc=1&advancedSearchKey=90514. Luettu 14.4.2018.

Isaca 2018. COBIT 5 Framework. A Business Framework for the Governance and Management of Enterprise IT. Isaca. http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx. Ladattu 14.5.2018.

ISO 2018. International Organization for Standardization – All about us. http://www.iso.org/about-us.html. Luettu 14.4.2018.

Kari, Toni 2017a. CTO. OptimeSys Oy, Espoo. Opinnäytetyön käynnistys. Haastattelu 3.4.2017.

Kari, Toni 2017b. CTO. OptimeSys Oy, Espoo. Tavoitteen rajaus. Haastattelu 3.8.2017.

Kari, Toni 2018. CTO. OptimeSys Oy, Espoo. Viimeistelyvaiheen ohjaus. Haastattelu 2.2.2018.

Karttaavi, Tommi 201. Esitys FCG:n ICT-foorumissa 12.2.2014. Pidetty 12.2.2014. http://www.slideshare.net/tommikarttaavi/ict-foorumi20140212. Luettu 14.4.2018

Keskuskauppakamari 2015. Hallinnointikoodi. Corporate Governanace 2015. Arvopaperimarkkinayhdistys ry. http://kauppakamari.fi/wp-content/uploads/2012/04/hallinnointikoodi-2015.pdf. Luettu 14.4.2018.

Kolesnik, Katri & Seren, Robert & Helenius, Mika 2016. Tietohallintojen johtaminen Suomessa 2016. Tutkimusraportti 22.9.2016. http://docplayer.fi/26970590-Tietohallintojen-johtaminen-suomessa.html. Tivia, Sofigate, Aalto. Luettu 20.4.2018.

Kuntaliitto. Sisäinen valvonta ja riskienhallinta käytännössä. Julkaistu 21.12.2016. http://www.kuntaliitto.fi/sites/default/files/media/file/Liite%201_Sisainen-valvonta-ja-riskienhallinta-kaytannossa.pdf. Luettu 14.4.2018.

Lindros, Kim 2018. What is IT governance? A formal way to align IT & business strategy. IDG www.CIO.com. Julkaistu 31.6.2017. http://www.cio.com/article/2438931/governance/governanceit-governance-definition-and-solutions.html. Luettu 14.4.2018.

Mc Nally, J. The 2013 COSO Framework & SOX Compliance. Strategic Finance, June 2013. http://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf. Luettu 14.1.2018.

Nurmi, Pekka & Talus, Anu & Jaatinen, Tanja & Hänninen, Anna & Rankalankila, Leena & Vettenranta, Leena. 2017. Oikeusministeriö. EU:n yleisen tietosuoja-asetuksen täytäntöön-panotyöryhmän (TATTI) mietintö. Julkaistu 21.6.2017.http://urn.fi/URN:ISBN:978-952-259-612-3. Luettu 19.8.2017.

Ratsula, Niina 2016. Yrityksen sisäinen valvonta. 2. painos. Edita, Helsinki.

Suomen standardisoimisliitto SFS 2013a. ISO/IEC 27000 -tietoturvallisuusstandardi liitteineen.

Suomen standardisoimisliitto SFS 2013b. ISO/IEC 27001 -tietoturvallisuusstandardi liitteineen.

Suomen standardisoimisliitto SFS 2013c. ISO/IEC 22301 -liiketoiminnan jatkuvuusstandardi liitteineen.

Tietohallintomalli 2018. Versio 3.3, 15.1.2018. https://www.itforbusiness.org/content//uploads/2018/01/Tietohallintomalli-15-1-2018.pdf. Luettu 14.4.2018.

Tietosuojavaltuutetun toimisto 2012. Laadi tietotilinpäätös. www.tietosuoja.fi. Julkaistu 24.4.2012. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf. Luettu 14.4.2018.

Tietosuojavaltuutetun toimisto 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Selvityksiä ja ohjeita. Oikeusministeriö. Julkaistu 27.1.2017.http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf. Luettu 14.4.2018.

Tietosuojavaltuutetun toimisto 2018. EU:n tietosuojauudistus. Tietosuoja-asetus. Julkaistu 15.6.2015. Päivitetty 23.3.2018.http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html. Luettu 14.4.2018.

VAHTI-raportti 1/2016 EU-tietosuojan kokonaisuudistus. 2016. Valtiovarainministeriö. Julkaistu 2.6.2016. http://urn.fi/URN:ISBN:978-952-251-778-4. Luettu 15.6.2017.

Vilkka, Hanna & Airaksinen, Tiina 2004. Toiminnallinen opinnäytetyö. 2. painos. Tammi, Helsinki.