Niklas Syväkuru

VALMISTAUTUMINEN ISO/IEC 27001 -STANDARDIN MUKAISTA SERTIFIOINTIA VARTEN

Tieto- ja viestintätekniikan koulutusohjelma
2018

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VALMISTAUTUMINEN ISO/IEC 27001 -STANDARDIN MUKAISTA SERTIFIOINTIA VARTEN

Syväkuru, Niklas
Satakunnan ammattikorkeakoulu
Tieto- ja viestintätekniikan koulutusohjelma
Elokuu 2018
Sivumäärä: 24

Asiasanat: tietoturva, standardi, sertifikaatit

Tämän opinnäytetyön tarkoituksena on selvittää mitä tulisi tehdä, jotta Boliden Harjavalta Oy olisi kykenevä aloittamaan ISO/IEC 27001-tietoturvastandardin sertifiointiprosessin. Katsastetaan yksityiskohtaisesti standardin sisältö ja sen vaatimukset, sekä käydään läpi nykyisen tietoturvan taso ja sen dokumentointi. Dokumentointia verrataan standardin vaatimuksiin ja ryhdytään kehittämään sitä edelleen. Hankkeen perinpohjainen ajatus on saada Boliden Harjavallalle tietoisuus standardista ja valmistella pohja mahdolliselle sertifikaatille tulevaisuudessa.

PREPARATION FOR ISO/IEC 27001-STANDARD CERTIFICATION

Syväkuru, Niklas
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information and Communications Technology
August 2018
Number of pages: 24

Keywords: Information security, standard, certificates

The objective of this thesis is to clarify what needs to be done for Boliden Harjavalta Oy to be able to start certification process for ISO/IEC-27001 information security standard. The details and requirements of the standard are looked over in detail. The current level of information security and its documentation is reviewed and compared to the standard's requirements. Project's base idea is to improve Boliden Harjavalta's awareness to the standard and build a foundation for a possible certificate in the future.

SISÄLLYSLUETTELO

LYHENTEET

ISO	International Organization of Standardization, kansainvälinen standardisoimisjärjestö
IEC	International Electrotechnical Commission, kansainvälinen sähköalan standardointijärjestö
ISMS	Information Security Management System, tietoturvallisuuden hallintajärjestelmä
JTC1	Joint Technical Committee, ISO:n ja IEC:n tietotekniikan alan standardeja tekevä yhteistyöryhmä
PDCA	Plan-Do-Check-Act, Suunnittele-Toteuta-Arvioi-Toimi jatkuvan kehityksen malli.
SFS	Suomen Standardisoimisliitto

1 JOHDANTO

Tietoturvan tarve yritysorganisaatiossa on kasvanut vuosi vuodelta suuremmaksi. Tietoturva on tärkeä osa jokaista organisaation prosessia. Tietoturvan laiminlyönti voi johtaa liiketoiminnan vaarantumiseen ja voi näin vaikuttaa yrityksen maineeseen. Uusia tietoturvauhkia syntyy päivittäin ja yrityksen tulisi suojautua niiltä mahdollisimman tehokkaasti.

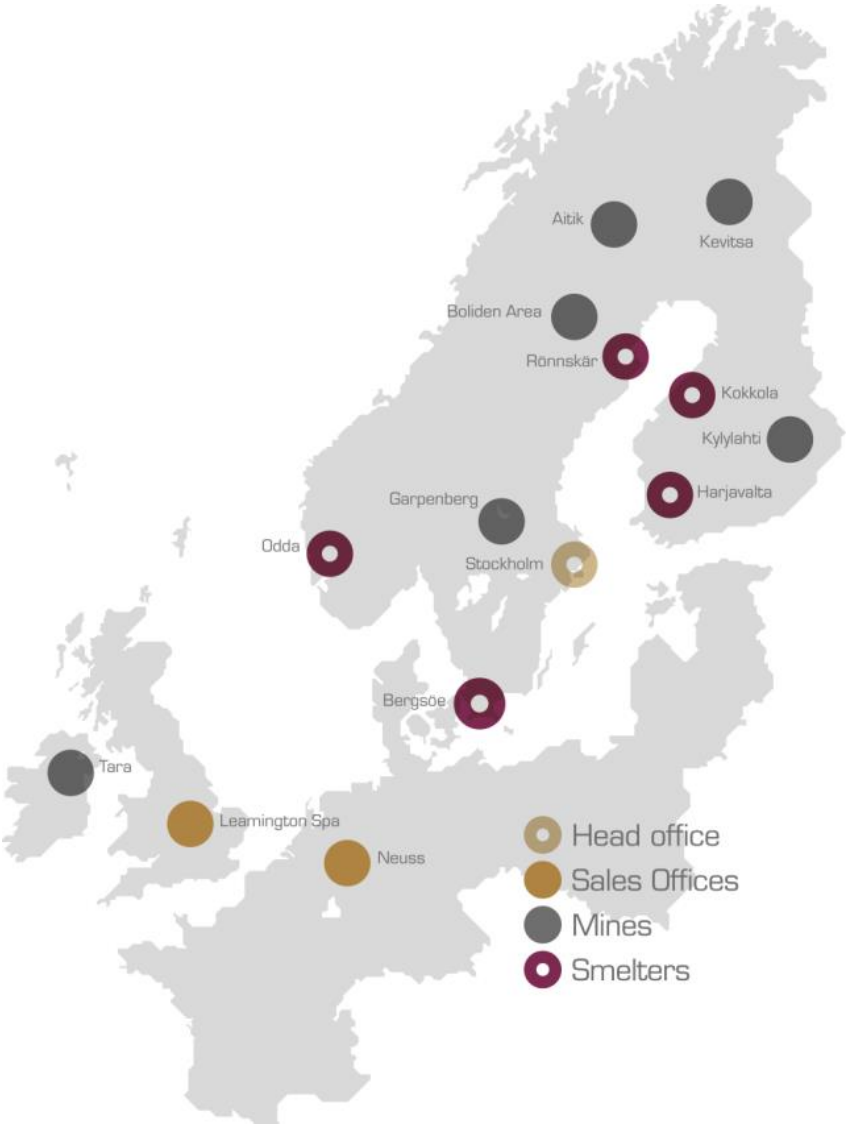
Täysin riskitöntä ympäristöä on lähes mahdoton rakentaa ja joidenkin riskien poistaminen voi olla haitallista tuotannolle, minkä seurauksena riskien korjaaminen ei ole taloudellisesti kannattavaa. Jo käsitteenä tietoturvallisuus on hyvin laaja ja siihen kuuluu paljon muutakin kuin laitteita ja ohjelmistoja, jotka taas ovat korkeintaan yhtä varmoja kuin niitä käyttävät ihmiset.

Yritysten toimintojen siirtyessä riippuvaisiksi tietojärjestelmistä hyvän tietoturvasuunnitelman ja dokumentoinnin tarve kasvaa. Havaitut ja tapahtuneet uhat sekä niiden korjaavat toimenpiteet tulisi dokumentoida, jotta vahvistettaisiin uhkien ennaltaehkäisemistä tulevaisuudessa. Tietoturvaansa panostava yritys nähdään luotettavana yhteistyökumppanina, ja ISO 27001 -sertifiointi voi olla myös kaupanteon edellytys.

2 YRITYSESITTELY

2.1 Boliden-konserni

Opinnäytetyön toimeksiantajana on Boliden Harjavalta Oy (BOHA). Boliden Harjavalta Oy on osa Boliden–konsernia, joka koostuu metallialan yrityksistä. Bolidenin toiminnot on jaettu kahteen eri liiketoiminta-alueeseen: kaivoksiin ja sulattoihin. Boliden konserni työllistää noin 5 700 henkilöä.



Kuva 1. Boliden-konsernin toimipisteet. (Boliden Harjavalta 2018)

Bolidenin kaivosten vastuulla on erottaa ja rikastaa malmi, joka tulee kuudesta kaivosalueesta: Aitikista, Garpenbergistä ja Bolidenin alueelta Ruotsista, Kylylahdesta ja Kevitsasta Suomesta sekä Tarasta Irlannista.

Bolidenin sulatoissa jalostetaan Bolidenin kaivoksista ja muista kaivoksista saatava malmirikaste sekä prosessoidaan toissijaiset raaka-aineet. Lisäksi Sulatot-liiketoiminta-alue vastaa malmirikasteen ja kierrätetyn raaka-aineen hankinnasta sekä Bolidenin metallien ja sivutuotteiden myynnistä.

Bolidenin Sulatot-liiketoiminta-alueeseen kuuluvat sinkkisulatot Kokkolassa ja Oddassa, kuparisulatot Rönnskärissä ja Harjavallassa sekä lyijysulatto Bergsöessä. (Boliden 2018.)

2.2 Boliden Harjavalta Oy

Kuparisulaton historia alkaa Imatralta, jossa toimi Outokumpu Oy:n kuparisulatto vuosina 1936-1944. Sulatto oli siirrettävä itärajalta sodan tieltä nykyiseen sijaintiinsa Harjavaltaan, jossa se myös sijaitsi hyvin lähellä Porin kuparielektrolyysitehdasta. Kuparisulaton viereen rakennettiin 1947 rikkihappotehdas, joka tuotti sulaton kaasuista raaka-ainetta lannoitetuotannolle. Metallurgian alan mullistava liekkisulatusmenetelmä kehitettiin Harjavallassa 1949, ja vuonna 1959 alkoi myös nikkelin valmistus samalla menetelmällä.

Vuonna 2000 Outokumpu myi nikkelibisneksensä amerikkalaiselle OM Groupille, joka taas myi sen jälleen venäläiselle Norilsk Nickelille 2007. Vuonna 2004 Outokumpu Harjavalta Metals Oy:stä tuli ruotsalaisen Boliden AB:n ja Outokumpu Oyj:n yritysjärjestelyjen seurauksena osa Boliden-konsernia, ja nimeksi tuli Boliden Harjavalta Oy. (Harjavallan Suurteollisuuspuisto 2010.)

Boliden Harjavalta Oy työllistää noin 530 henkilöä.

3 ISO/IEC 27001 -STANDARDI

Standardisoinnilla luodaan yhteisiä toimintatapoja helpottamaan jokapäiväistä elämää. Standardien avulla varmistetaan tuotteiden, palvelujen ja järjestelmien yhteensopivuus, turvallisuus sekä toiminnan järkeistäminen. (SFS 2018.)

3.1 Tietoturvan hallintajärjestelmä, ISMS

ISO/IEC 27001- standardi on osa ISO/IEC 27000 -standardiperhettä, joka sisältää organisaation taloustietojen, henkilötietojen ja informaation turvallisuutta koskevia standardeja. ISO/IEC 27001 -standardi on parhaiten tunnettu tietoturvallisuuden hallintajärjestelmä eli ISMS. ISMS on systemaattinen lähestymistapa hallitsemaan yrityksen arkaluonteista tietoa. Se kokoaa organisaation ihmisiä, prosesseja ja IT-järjestelmiä riskienhallintaprosessikokonaisuudeksi. (ISO 2018.)

3.2 ISO, IEC ja JTC1

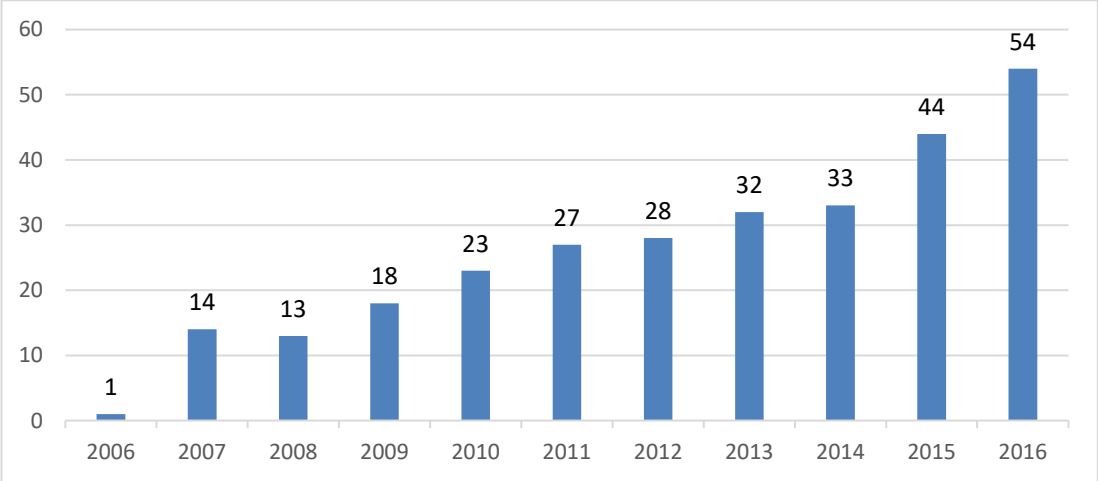
ISO eli International Organization for Standardization on yksityinen ja voittoa tavoittelematon kansainvälinen organisaatio, joka perustettiin vuonna 1947. ISO:hon kuuluu 161 jäsenmaata. ISO on julkaissut yhteensä 22041 kansainvälistä standardia ja asiakirjaa koskien lähes jokaista teollisuuden alaa. (ISO 2018.)

IEC eli International Electrotechnical Commission on myös voittoa tavoittelematon, vuonna 1906 perustettu maailman johtava sähkö-, elektroniikka- ja vastaavien teknologioiden kansainvälisten standardien valmistaja. IEC:hen kuuluu 84 jäsenmaata. (IEC 2018.)

Yhdessä ISO ja IEC muodostivat vuonna 1987 tieto- ja viestintätekniikan standardeja julkaisevan komitean ISO/IEC JTC1. JTC1 on julkaissut 3116 standardia, joista yksi on JTC1:en alakomitean julkaisema ISO/IEC 27001 -standardi. (ISO 2018.)

3.3 ISO/IEC 27001

Suomessa kiinnostus ISO/IEC 27001 -standardiin kasvaa joka vuosi. Vuonna 2016 54 organisaatiota olivat hankkineet ISO/IEC 27001 -standardin sertifikaatin Suomessa (Kuvio 1). Maailmanlaajuisesti samaisen raportin mukaan sertifikaatteja oli myönnetty 33290. (ISO 2016.)



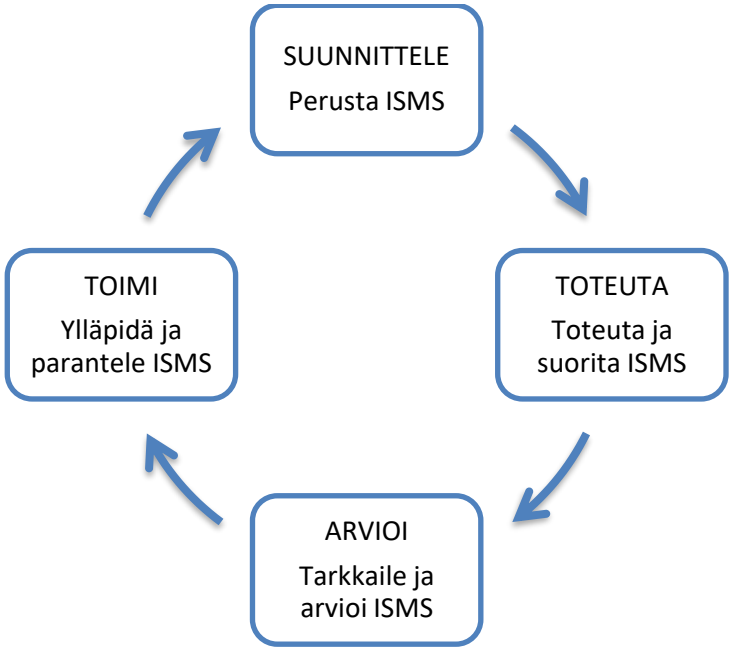
Kuvio 1. ISO/IEC 27001 -standardin sertifioinnin yleistyminen Suomessa (ISO 2016).

Kirjoitushetkellä viimeisin versio ISO/IEC 27001 -standardista on vuodelta 2013. Se pohjautuu aikaisempaan vuoden 2005 versioon. 2013 versio on sovellettu paremmin sopimaan ISO 9000 ja 20000 -standardiperheiden kanssa. Uudessa versiossa on myös paremmin huomioitu myöhemmin yleistyneitä tietotekniikan sovelluksia, kuten pilvipalveluita. (Kosutic 2013.)

ISO 27001 julkaistiin vuonna 2005 korvaamaan British Standards Instituten BS7799-2 -standardi, johon se pohjautuu. 2005 versio perustuu vahvasti PDCA -malliin (Plan-Do-Check-Act) (Kuvio 2). Paino PDCA -mallilta on hieman hellittänyt 2013-vuoden versiossa, jossa paino siirtyi enemmän organisaation tietoturvan suorituskyvyn arviointiin ja mittaamiseen. (ISO 27000 Directory 2013.)

PDCA-malli noudattaa niin kutsuttua jatkuvaa kehitystä, koska mallia seuraten hallintajärjestelmää tarkistetaan säännöllisesti. Näin tehtyjä toimenpiteitä ei laiminlyödä ja ne pysyvät yhtä tehokkaina. Malli koostuu seuraavista vaiheista:

1. **suunnittele** (Plan):
   Määritä hallintajärjestelmä, määränpäät, prosessit ja toimintatavat riskien hallintaa ja tietoturvan kehittämistä varten.
2. **toteuta** (Do):
   Toteuta suunnitellut toimenpiteet.
3. **arvioi** (Check):
   Tarkastele ja arvioi prosesseja, toteutettua hallintajärjestelmää ja prosessien suorituskykyä. Vertaile tuloksia määriteltyyn tietoturvapolitiikkaan ja tavoitteisiin ja raportoi tulokset johdolle.
4. **toimi** (Act):
   Dokumentoi ja ryhdy mahdollisiin korjaaviin ja ennaltaehkäiseviin toimenpiteisiin arvioinnin tulosten perusteella. Dokumentaation pohjalta kehitä edelleen hallintajärjestelmää.



Kuvio 2. PDCA-malli.

3.4 Standardin vaatimukset

Tärkein vaatimus ISO/IEC 27001 -standardissa on yrityksen sitoutuminen koko prosessiin. Prosessi sisältää hallintajärjestelmän kehittämisen, toteuttamisen, käyttämisen, ylläpitämisen, valvomisen, katselmoinnin ja parantamisen. Tietoturvallisuuden hallintajärjestelmä on dokumentaatio, johon sisältyy tietoturvan

johtaminen, valvominen, hallinnoiminen ja toimenpiteet. ISO/IEC 27001:2013 -standardi on jaettu seuraavanlaisesti osiin (Lahnalahti 2013):

1. soveltamisala
2. velvoittavat viittaukset
3. termit ja määritelmät
4. organisaation toimintaympäristö
5. johtajuus
6. suunnittelu
7. tukitoiminnot
8. toiminta
9. suorituskyvyn arviointi
10. parantaminen
11. liite A (velvoittava) Hallintatavoitteiden ja -keinojen viiteluettelo.

Standardissa esitetyt vaatimukset ovat yleisluontoisia, sillä standardin tulee olla soveltuva kaikenlaisille organisaatioille koosta, tyypistä ja luoneesta riippumatta. Vaatimusmäärittely sisältää vaatimukset kullekin organisaation osa-alueelle siitä, kuinka hallintajärjestelmän luominen, toteuttaminen ja ylläpito tulee suorittaa. Organisaatio, joka ilmoittaa noudattavansa ISO/IEC 27001 -standardia, ei voi rajata pois mitään kohdista 4-10. (ISO 2018.)

3.4.1 Organisaation toimintaympäristö

Vaatimusmäärittelyn neljännessä luvussa käydään läpi kuinka organisaatiossa tulisi määrittää ulkoiset ja sisäiset asiat, jotka ovat organisaation tarkoituksen kannalta olennaisia. Organisaation tulee vaatimusten mukaisesti luoda, parantaa ja ylläpitää hallintajärjestelmä. (SFS ISO/IEC 2013.)

3.4.2 Johtajuus

Vaatimusmäärittelyn viidennessä luvussa käsitellään keinoja, joilla organisaation ylempi johto osoittaa johtajuutta ja sitoutuu tietoturvallisuuden hallintajärjestelmään.

Ylemmän johdon tulee varmistaa, että tietoturvapolitiikka laaditaan ja tavoitteet asetetaan organisaation toimintasuunnitelman mukaisesti. Ylin johto selvittää, onko hallintajärjestelmän vaatimukset mahdollista yhdistää organisaation prosesseihin, ja että siihen on riittävät resurssit. Lopuksi johto varmistaa, että halutut tulokset on mahdollista saavuttaa. (SFS ISO/IEC 2013.)

Ylin johto laatii tietoturvapolitiikan, joka sopii yrityksen toimintaan ja varmistaa, keillä organisaatiossa on vastuut mihinkin tietoturvan osaan. Tietoturvapolitiikkaan on sisällytettävä tietoturvallisuutta koskevien vaatimusten täyttäminen. (SFS ISO/IEC 2013.)

3.4.3 Suunnittelu

Vaatimusmäärittelyn kuudennessa luvussa listataan, kuinka organisaation tulee huomioida erilaisia asioita tietoturvallisuuden hallintajärjestelmää suunnitellessa. Varmistetaan, että hallintajärjestelmä toimii halutulla tavalla, ennaltaehkäistään haittaavat vaikutukset ja saavutetaan tila, joka mahdollistaa tietoturvan ja sen hallintajärjestelmän jatkuvan kehittämisen. (SFS ISO/IEC 2013.)

3.4.4 Tukitoiminnot

Vaatimusmäärittelyn seitsemännessä luvussa käydään läpi hallintajärjestelmän luomista, ylläpitoa ja jatkuvaa kehitystä. Siinä määritellään, kuinka paljon tulisi varata resursseja ja selvittää henkilökunta, joka työllään vaikuttaa tietoturvallisuuteen. Henkilön pätevyys katsotaan koulutuksen ja kokemuksen perusteella. Vaadittaessa henkilö koulutetaan toimimaan tavoitetulla tietoturvallisuuden tasolla. (SFS ISO/IEC 2013.)

3.4.5 Toiminta

Vaatimusmäärittelyn kahdeksas luku käsittelee, kuinka organisaation tulee suunnitella ja toteuttaa ne prosessit, jotka tarvitaan vaatimusten täyttymiseen. Prosessien toteutumista laaditun suunnitelman mukaan valvotaan dokumentoimalla riittävän paljon. Dokumentaatiossa tulee huomioida mahdollinen kehityksen tarve. Riskien arviointia suoritetaan tietyin ennaltamäärätyin aikavälein tai jos on tehty muutoksia. (SFS ISO/IEC 2013.)

3.4.6 Suorituskyvyn arviointi

Vaatimusmäärittelyn yhdeksännessä luvussa käydään läpi, kuinka yrityksen tulee arvioida tietoturvan tasoa. Yrityksen tulee määrittää, koska suorituskyvyn arviointi toteutetaan ja ketkä arvioinnin toteuttavat. Arviointi ja suoritetut toimenpiteet tulee dokumentoida, ja dokumentointi säilöä. (SFS ISO/IEC 2013.)

Hallintajärjestelmän ylläpitoa arvioidaan auditointiohjelmalla. Yrityksen sisäisissä auditoinneissa arvioidaan, vastaako hallintajärjestelmä yrityksen asettamia vaatimuksia sekä ISO/IEC 27001 -standardin vaatimuksia. Auditoinnissa otetaan huomioon aikaisempien auditointien tulokset ja eri prosessien tärkeys hallintajärjestelmän kannalta. Myös auditointien tulokset dokumentoidaan ja tulokset tulee raportoida johtohenkilöille. (SFS ISO/IEC 2013.)

Johdon tehtävänä on käydä läpi hallintajärjestelmä tietyin aikavälein ja varmistaa, että se on vielä yrityksen toimintaan sopiva ja tehokas. Johto arvioi mahdolliset parannusehdotukset ja tarpeet muutoksiin. (SFS ISO/IEC 2013.)

3.4.7 Parantaminen

Vaatimusmäärittelyn kymmenennessä luvussa määritellään, kuinka yrityksen on vastattava havaittuihin poikkeamiin ja ryhdyttävä niiden mahdollisiin korjaaviin toimenpiteisiin. Vaadittaviin toimenpiteisiin tulee ryhtyä ja arvioida niiden vaikuttavuus hallintajärjestelmän prosesseihin. Toimenpiteisiin sisältyy esimerkiksi

vastaavanlaisten poikkeamien etsiminen, poikkeamien katselmointi ja syiden selvittäminen. Poikkeamista ja niiden korjaavista toimenpiteistä pitää dokumentoida tehokkaasti välttääkseen samankaltaiset poikkeamat tulevaisuudessa. Yrityksen tietoturvallisuuden hallintajärjestelmää tulee jatkuvasti parantaa, lisäten soveltuvuutta, riittävyyttä ja tehokkuutta. (SFS ISO/IEC 2013.)

3.4.8 Liite A

ISO/IEC 27001 -standardin Liite A on tunnetuin liite kaikista ISO:n 27000-perheen standardeista, sillä se tarjoaa olennaisen työkalun yrityksen tietoturvan hallintaan. Se on lista tietoturvan suojakeinoja, jotka ovat tärkeä osa yrityksen riskien arviointi- ja korjausprosessia. Suojakeinot ovat jaettu seuraavanlaisesti:

- **A.5 Information security policies / Tietoturvapolitiikat**
  Määrää, kuinka politiikat kirjoitetaan ja käydään läpi.

- **A.6 Organization of information security / Tietoturvallisuuden organisointi**
  Määrää, kuinka vastuut nimitetään. Sisältää myös määräykset mobiililaitteille ja etätyölle.

- **A.7 Human resources security / Henkilöstöturvallisuus**
  Määräykset ennen työsuhteen alkua, työsuhteen aikana ja työsuhteen jälkeen.

- **A.8 Asset management / Suojattavan omaisuuden hallinta**
  Varainhoitoon ja hyväksyttyyn käyttöön liittyvät määräykset.

- **A.9 Access control / Pääsynhallinta**
  Pääsynhallinnan politiikat. Käyttäjien, järjestelmien ja sovellusten pääsynhallinta ja käyttäjien vastuut.

- **A.10 Cryptography / Salaus**
  Kryptauksen ja avainten hallinnan määräykset

- **A.11 Physical and environmental security / Fyysinen turvallisuus ja ympäristön turvallisuus**
  Määräykset turva-alueille, uhilta suojautumiselle, laiteturvallisuus, tiedon turvallinen hävittäminen.

- **A.12 Operational security / Käyttöturvallisuus**
  IT toimintaohjeet, velvollisuudet, suojautuminen haittaohjelmilta, kirjaaminen, varmuuskopiointi, seuranta, asennukset, haavoittuvuudet.

- **A.13 Communications security / Viestintäturvallisuus**
  Verkkoturvallisuuteen, eristämiseen, verkkopalveluihin ja tiedonsiirtoon liittyvät määräykset.

- **A.14 System acquisition, development and maintenance / Järjestelmän hankkiminen, kehittäminen ja ylläpito**
  Määräykset tietoturvan vaatimuksille, kehittämiselle ja tukiprosesseille.

- **A.15 Supplier relationships / Suhteet toimittajiin**
  Määritykset mitä sisällyttää sopimuksiin ja kuinka tarkkailla toimittajia.

- **A.16 Information security incident management / Tietoturvallisuuden hallinta**
  Määräykset, kuinka raportoida tapahtumat ja heikkoudet, kuinka määritellä vastuut, tapahtumiin vastaaminen ja todisteaineiston kerääminen.

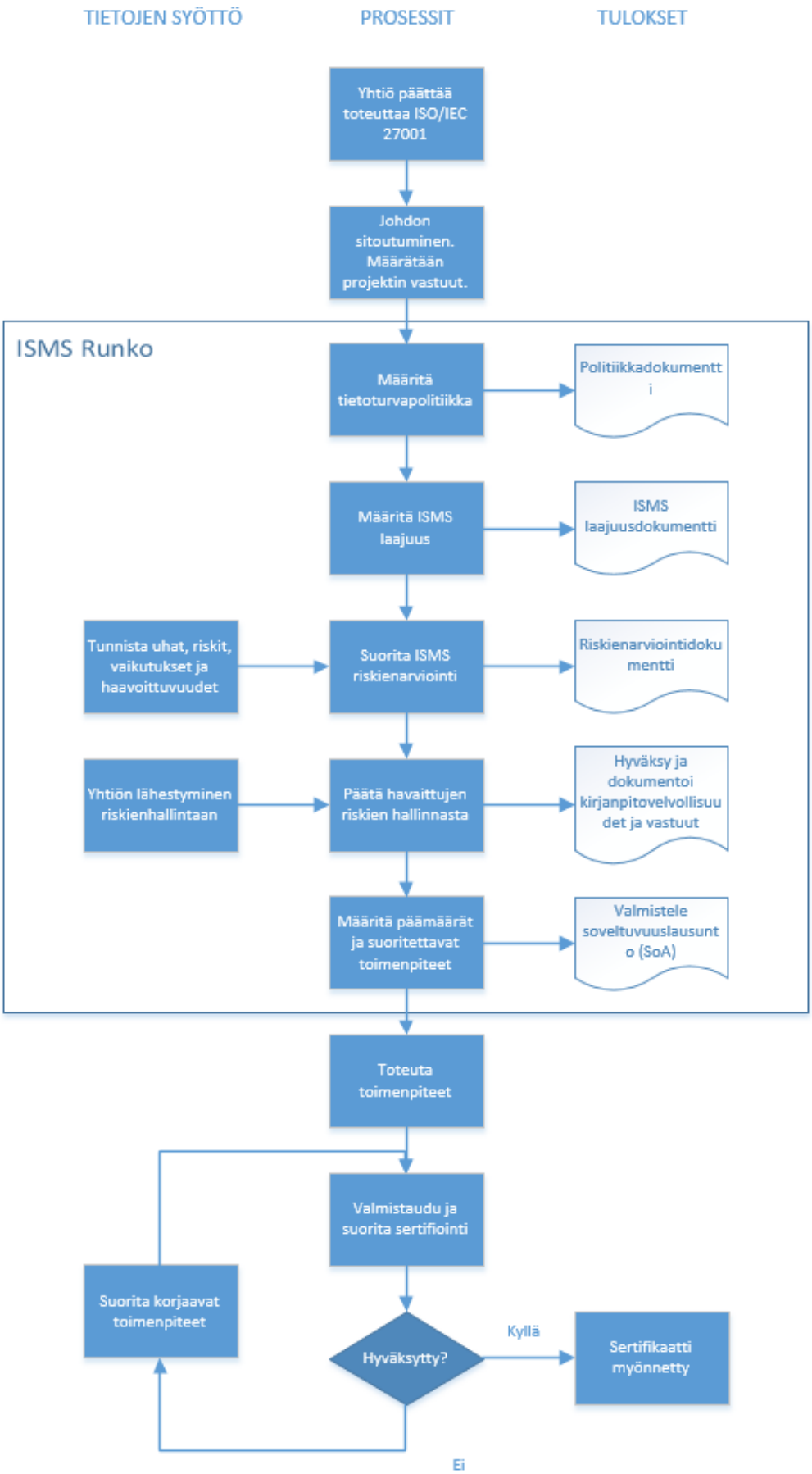
- **A.17 Information security aspects of business continuity management / Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia**
  Määräykset koskien liiketoiminnan jatkuvuutta, toimintatapoja, verifikaatioita, tarkasteluja ja vikasietoisuutta.

- **A.18 Compliance / Vaatimustenmukaisuus**
  Lainsäädäntöön ja sopimuksiin liittyvät määräykset. Tiedon ja henkilökohtaisen datan suojaaminen.

(SFS ISO/IEC 2013, Kosutic 2015.)

4 SERTIFIOINTIPROSESSI

Sertifioinnilla tarkoitetaan yrityksen tai organisaation palvelun, tuotteen, henkilöstöjohtamisen tai johdon arvioimiseen perustuvaa todistusten myöntämistä. Yritys voi sertifikaatillaan osoittaa toimivansa sertifioidun standardin mukaisesti. Yrityksen sertifioinnin suorittaa aina ulkopuolinen puolueeton osapuoli. ISO/IEC 27001 -standardin sertifiointiprosessi alkaa sertifikaattihakemuksella sertifiointeja suorittavalle osapuolelle. Ennen sertifioinnin hakua pitää vaadittavat toimenpiteet olla suoritettuina. Kuviossa 3 on esitetty askel askeleelta koko standardin sertifiointiprosessi, sisältäen tietoturvallisuuden hallintajärjestelmän luomisen ja tuotetut dokumentit. (The ISO Directory 2007, The British Standards Institution 2018, IsecT 2018).



Kuvio 3. ISO/IEC 27001 -standardin sertifiointiprosessi.

Ensimmäiseksi organisaation johto päättää ISO/IEC 27001 -standardin toteuttamisesta yrityksessä. Jos johto sitoutuu toteuttamaan standardin vaatimuksia, jaetaan standardisointiprojektin tehtävät ja vastuut henkilöstölle. (The ISO Directory 2007.)

Seuraavana alkaa tietoturvallisuuden hallintajärjestelmän toteuttaminen. Tietoturvallisuuden hallintajärjestelmän kattavuus ja resurssit mitoitetaan ja dokumentoidaan tarkasti. Tärkeimpinä dokumentteina ovat kattavuusdokumentti, riskianalyysi ja soveltuvuuslausunto. Dokumenttien perusteella kolmannen osapuolen sertifiointitaho pystyy tarkastamaan, että toimenpiteet ovat suoritettu vaatimusten mukaisesti. Jos standardin vaatimukset eivät täyty, sertifikaatti evätään ja organisaatio ryhtyy havaittuja puutteita koskeviin toimenpiteisiin. Puutteet korjattuaan organisaatio voi hakea uutta auditointia. (BSI 2018, The ISO Directory 2007.)

ISO/IEC 27001 -standardin vaatimusten täytyttyä organisaatio saa ISO/IEC 27001 -sertifikaatin, joka on voimassa kolme vuotta kerrallaan. Tämän jälkeen organisaatio voi hakea halutessaan uutta auditointia. Sertifikaatin voimassaolon aikana suoritetaan säännöllisiä tarkastuksia, jotta vaatimusten mukaisen tietoturvallisuuden hallintajärjestelmän ylläpito ja parantaminen varmistuvat. (Bureau Veritas Finland 2018.)

Sertifiointeja myöntävät sertifiointilaitokset, jotka ovat sitoutuneet puolueettomuuteen. Suomessa ISO/IEC 27001 -standardin sertifikaatin voi auditoida muun muassa Kiwa Inspecta Oy, Nixu Certification Oy ja Bureau Veritas Finland. (Kiwa Inspecta 2018, Nixu Certification 2018, Bureau Veritas Finland 2018.)

5 PROJEKTI

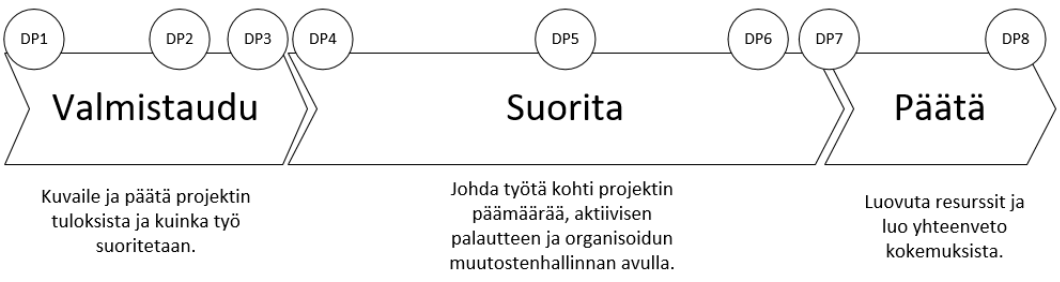
Projektin tavoitteena on selvittää Boliden Harjavalta Oy:ltä ISO/IEC 27001-standardin vaatimuksiin nähden puuttuvat dokumentit. Boliden-konsernilla on oma jo vanhentunut tietoturvallisuuden hallintajärjestelmä, joka on luotu 2006, ja jota on

täydennetty 2012. Konsernin tietoturvan hallintajärjestelmä olisi syytä päivittää vastaamaan uusia vaatimuksia, tai vastaamaan ISO/IEC 27001-standardin vaatimuksia. Tutustuin kyseiseen dokumentaatioon ja päätimme projektiryhmän kesken käyttää sitä toiminnan pohjana alkavassa projektissa. Projektin aikatauluna oli kesä 2018 ja tulos viimeisteltiin elokuun lopussa. Tulos ilmenee listana puuttuvia dokumentteja. Projektin kustannuksiin sisältyy ISO/IEC 27001-standardin vaatimusten suomennettu PDF Suomen Standardisoimisliitto SFS ry:ltä.

Projekti aloitettiin valitsemalla sopiva projektimalli Boliden Harjavallan projektimalleista. Projektimalli on yrityksessä sovittu tapa ohjata organisaation projekteja ja niiden muodostamia kokonaisuuksia. Mallissa on oltava kuvaus projektin prosessien johtamisesta. Projektimallin avulla projektijohtaminen yhtenäistyy, turha työ vähenee, päätöksenteko paranee ja pystytään parantamaan resurssien hallintaa. Boliden Harjavalta Oy:llä on käytössä Tieto Oyj:n esirakennettu projektimalli. (Projekti-instituutti 2016.)

5.1 Boliden Harjavalta projektimalli

Boliden Harjavalta Oy käyttää Tieto Oyj:n kansainvälistä, ja etenkin pohjoismaissa käytettyä, Practical Project Steering (PPS) –projektimallia. PPS ottaa huomioon tunnettuja kansainvälisiä projektihallinnan standardeja kuten IPMA, PMI ja PRINCE2, sekä tukee valmistautumista standardien sertifiointiin. Projektimalli on toimialariippumaton, ja soveltuu näin yksinkertaisesta projektista suureen ja moniasteiseen. PPS-projektimalleja on kolmea eri kokoa; Mini, Medium ja Mega. Käytämme tähän projektiin alla olevan kuvan mukaista Medium-mallia. Mahdollinen sertifiointiprosessi-projekti käyttäisi myös samaa mallia (Tieto 2018.)



Kuvio 4. Tieto PPS Medium-projektimalli.

Projektimallin asetanta koostuu kahdeksasta päätöksentekopisteestä (Decision Point, DP). Päätöksentekopisteet ovat esitelty alla:

DP 1 – Päätös projektin aloittamisesta

- Ohjausryhmä tekee päätöksen aloittaa projekti ja määrittää valmisteluvaiheen töiden laajuuden.

DP 2 – Päätös jatkosta, keskeyttämisestä, tai valmisteluiden muuttamisesta

- Päätetään valmisteluvaiheessa töiden suorittamisesta, sillä oletuksella, että projekti-idea on kelpaava ja meneillään oleva työ näyttää lupaavalta.

DP 3 – Päätös projektisuunnitelman hyväksymisestä

- Hyväksytään valmisteluvaiheessa aikaansaatu suunnitelma.

DP 4 – Päätös toiminnan aloittamisesta

- Tehdään päätös aloittaa projektin suorittaminen projektisuunnitelman mukaan. Tässä vaiheessa pitää päästä yhteisymmärrykseen ja hyväksyä toimintamenetelmät, kustannukset, aikataulut ja riskit. Lisäksi tarkistetaan, että kaikki tarvittavat sopimukset ovat allekirjoitettu.

DP 5 – Päätös jatkosta, muutoksista, tai keskeytyksestä

- Tarkistetaan onko tapahtunut muutoksia, jotka vaikuttavat projektin etenemiseen. Onko tullut esille uusia riskejä tai mahdollisia parannuksia suunnitelmaan. Katsotaan tarvitaanko projektiorganisaatioon muutoksia.

DP 6 – Projektin tuloksen lopullinen hyväksyntä

- Hyväksytään projektin toimitus, toimitus jäljelle jääneillä ongelmilla, tai toimituksen uudelleenteko.

DP 7 – Projektin tuloksen vastuiden siirtäminen

- Projektin tuloksen vastuut jaetaan projektiorganisaatiolta muille osapuolille.

DP 8 – Päätös projektin päättämisestä

- Kattaa projektin ja sen ohjausryhmän lopettamisen ja projektitilien sulkemisen.
- Alkaa pöytäkirjojen, loppuraportin ja arkistoitujen dokumenttien toimittamisella ja siirrolla.

5.2 Projektin kulku

Aloituspalaveriin osallistui Boliden Harjavalta Oy:n tietohallinnon henkilöstöä. Palaverissa käytiin läpi ISO/IEC 27001-standardin sisällön ja Boliden-konsernin laatimat tietoturvadokumentaatiot ja laaditun dokumentaation puutteita. Vertasimme olemassa olevaa Bolidenin tietoturvadokumentaatiota standardin vaatimuksiin ja totesimme konsernin tietoturvadokumentaation vastaavan jo valmiiksi suurelta osalta standardin vaatimuksia. Määräsimme tietoturvallisuuden hallintajärjestelmän kattamaan Boliden Harjavalta Oy:n tuotanto- ja talousorganisaatiot, jotta toisen ei tarvitsisi kohdella toista organisaatiota ulkoisena sidosryhmänä hankaloittaen dokumentaatiota ja tuoden ylimääräistä ja turhaa työkuormaa.

Opiskelin ja laadin ennen seuraavaa palaveria Bolidenin virallisen Tieto PPS-projektimallinmukaisen projektisuunnitelman, jonka luimme tarkkaan ja hyväksyimme palaverissä. Määrättiin projektiorganisaation ohjausryhmä, joka koostui tietohallinnon henkilöstöstä. Ohjausryhmän toimintaa ohjasi tietohallintopäällikkö. Riskienarvioinnissa totesimme väärien havaintojen voivan johtaa ylimääräiseen työhön jatkoprojektissa ja pahimmassa tapauksessa tietoturvariskiin. Projektin eteneminen aikataulutettiin ja sovittiin, että viikoittain tullaan pitämään palaveri. Projektin aikataulun takarajaksi asetettiin elokuun loppu.

Seuraavien viikkojen aikana laadimme listaa standardin vaatimuksiin nähden puuttuvista dokumenteista, joita kukin projektiorganisaation jäsen oli havainnut itsenäisesti. Havaittiin muutosten seurauksena mahdollisesti muutoksia työsopimuksessa työntekijälle eriteltäviin tietoturvavastuisiin. Määrittelimme palavereissä puutteellisen dokumentaation vastaamaan standardin vaatimuksia. Jos nykyisessä tietoturvadokumentoinnissa tapahtuu kesken projektin muutoksia, arvioidaan uudestaan standardiin nähden vaadittava dokumentaatio.

Tuotettu tietoturvan ehostamisdokumentti käytiin tietohallintopäällikön ja projektin ohjausryhmän kanssa lävitse verraten sitä standardin vaatimuksiin. Selvitettyämme vaatimuksiin nähden puuttuvan dokumentaation, totesimme suorittaneemme vaadittavat valmistelut. Boliden Harjavalta Oy on nyt valmis aloittamaan halutessaan

dokumenttien laatimisprojektin ja dokumentaation täyttäessä standardin vaatimukset, sertifiointiprosessin.

6 LOPPUSANAT

ISO/IEC 27001 -standardin sertifiointi Suomessa on hitaassa kasvussa. Näkisin, että tietoisuus ja kiinnostus standardia kohtaan tulee kasvamaan huomattavasti seuraavan vuosikymmenen aikana, kun katsoo, kuinka suureksi puheenaiheeksi tietoturva on noussut viime vuosina. Kansainvälisesti standardi on paljon suuremmassa huomiossa. Vuonna 2016 Suomessa oli myönnetty 54 ISO/IEC 27001-sertifikaattia. Samaan aikaan Euroopan maiden keskiarvo oli 266. Huippua piti Iso-Britannia 3367:llä myönnetyllä sertifikaatilla. (Charlet 2016.)

On ymmärrettävää, miksi monet organisaatiot, varsinkaan pienet, eivät rupea noudattamaan standardin vaatimuksia. On haasteellista löytää sopiva kultainen keskiviiva, jossa yrityksen tietoturva kasvaa tuomatta valtavaa määrää vain turhaa raportointia. Seuraavana tulee houkutus rajata tietoturvallisuuden hallintajärjestelmä vain tiettyyn organisaation osaan, kuten vaikka tietohallintoon. Tämä tuo ongelmaksi sen, että organisaation muita osia olisi tämän jälkeen kohdeltava ulkoisena sidosryhmänä, eikä esimerkiksi voisi olla samassa aliverkossa, ja tällöin hallinta sekavoituu.

Boliden Harjavalta Oy:lle ISO/IEC 27001-standardin sertifiointi toisi mahdollisesti positiivista näkymää Boliden Harjavallasta uusille ja vanhoille liikekumppaneille. Tietomurrot voivat näin isossa yrityksessä pahimmassa tapauksessa johtaa toiminnan keskeyttämiseen ja näin suuriin tappioihin. Kääntöpuolena standardi tuo ylimääräistä työtä yksittäiselle työntekijälle ja enemmän asioita huomioitavaksi eri työtehtävissä. Henkilökunnalle pitäisi kouluttaa standardin sisältö sekä sen alla toimiminen ja konsernin muiden toimipaikkojen kanssa toimiminen monimutkaistuisi.

LÄHTEET

Boliden. 2018. Boliden Harjavalta. Viitattu: 14.6.2018. Saatavissa: https://www.boliden.com/fi/operations/smelters/boliden-harjavalta#

Boliden. 2018. Organisaatio. Bolidenin henkilöstön intranet. Viitattu: 28.6.2018.

Bureau Veritas Finland. 2018. ISO 27001 sertifiointi. Viitattu 22.2.2018. Saatavissa: http://www.bureauveritas.fi/services+sheet/iso_27001_sertifiointi

Harjavallan Suurteollisuuspuisto. 2010. Historian vuosikymmenet. Viitattu: 28.6.2018. Saatavissa: http://www.suurteollisuuspuisto.com/Tiedostot/HistorianVuosikymmenet_20072010_A4_small.pdf

IEC. 2018. About the IEC. Viitattu 13.2.2018. Saatavissa: http://www.iec.ch/about/

ISO 27000 Directory. 2013. An Introduction to ISO 27001. Viitattu 13.2.2018. Saatavissa: http://www.27000.org/iso-27001.htm

ISO. 2016. ISO/IEC 27001 - data per country and sector 2006 to 2016. Viitattu 14.2.2018. Saatavissa: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

ISO. 2018. About ISO. Viitattu 13.2.2018. Saatavissa: https://www.iso.org/about-us.html

ISO. 2018. ISO/IEC 27000 family - Information security management systems. Viitattu 13.2.2018. Saatavissa: https://www.iso.org/isoiec-27001-information-security.html

ISO. 2018. ISO/IEC JTC 1. Viitattu 13.2.2018. Saatavissa: https://www.iso.org/isoiec-jtc-1.html

Kiwa Inspecta Oy. 2018. Viitattu 4.3.2018. Saatavissa: https://www.inspecta.fi/

Kosutic, D. 2013. A first look at the new ISO 27001. Viitattu 14.2.2018. Saatavissa: https://advisera.com/27001academy/blog/2013/01/28/a-first-look-at-the-new-iso-27001-2013-draft-version/

Kosutic, D. 2015. Overview of ISO 27001:2013 Annex A. Viitattu: 21.2.2018. Saatavissa: https://advisera.com/27001academy/knowledgebase/overview-of-iso-270012013-annex-a/

Lahnalahti, J. 2013. Uusi SFS-ISO/IEC 27001:2013. Viitattu: 15.2.2018. Saatavissa: https://www.sfs.fi/files/4224/27001-julkaisu_2013-12-05_Lahnalahti.pdf

Laurent Charlet. 2016. The ISO Survey. Viitattu: 20.08.2018. Saatavissa: https://www.iso.org/the-iso-survey.html

Netgrowth Ltd 2014. Implementing ISO 27001:2013. Viitattu: 14.2.2018. Saatavissa: http://www.netgrowthltd.co.uk/ISO27001.aspx

Nixu Certification Oy. 2018. Viitattu 4.3.2018. Saatavissa: https://www.nixu.com/fi/nixu-certification-oy

Projekti-instituutti. 2016. Pitäisikö meidänkin kehittää projektimalli? Viitattu: 27.08.2018. Saatavissa: https://www.projekti-instituutti.fi/blogi/pitaisiko_meidankin_kehittaa_projektimalli.2544.blog

SFS ISO/IEC 27001:2013. 2013. Tietoturvallisuuden hallintajärjestelmän vaatimukset. Viitattu 21.2.2018

Suomen Standardisoimisliitto SFS ry. Mihin standardeja tarvitaan? Viitattu 13.2.2018. Saatavissa: https://www.sfs.fi/julkaisut_ja_palvelut/standardi_tutuksi/mihin_standardeja_tarvitaan

The British Standards Institution. 2018. Certification for ISO 27001. Viitattu: 22.2.2018. Saatavissa: https://www.bsigroup.com/en-GB/iso-27001-information-security/Certification-for-ISO-27001/

The ISO 27000 Directory. 2007. The ISO27001 Certification Process. Viitattu: 21.2.2018 Saatavissa: http://www.27000.org/ismsprocess.htm

Tieto. 2018. Miksi sinun kannattaa valita PPS? Viitattu: 23.7.2018. Saatavissa: https://www.tieto.fi/palvelut/konsultointipalvelut/muutos-ja-transformaatiopalvelut/pps-kaytannonlaheista-projektinhallintaa/tervetuloa-pps-perheeseen/miksi-pps

IsecT. 2018. ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements (second edition) Viitattu: 30.08.2018. Saatavissa: http://www.iso27001security.com/html/27001.html