

Antti Kortelainen

Yhtiön tietoturvallisuuden standardisointi ja standardisoinnista saatavat hyödyt

Opinnäytetyö

Kevät 2019

SeAMK Tekniikka

Konetekniikan tutkinto-ohjelma



SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: SeAMK Tekniikka

Tutkinto-ohjelma: Konetekniikka

Suuntautumisvaihtoehto: Kone- ja tuotantotekniikka

Tekijä: Antti Kortelainen

Työn nimi: Yhtiön tietoturvallisuuden standardisointi ja standardisoinnista saatavat hyödyt.

Ohjaaja: Heikki Heiskanen

Vuosi: 2019

Sivumäärä: 33

Liitteiden lukumäärä: 0

Tietoturvallisuudenhallintajärjestelmällä keskitetään kaikki tietoturvallisuuteen liittyvät asiat ja hallitaan niitä. Hallintajärjestelmä koostuu useasta eri osasta. Näitä osia käsitellään standardisarjassa SFS-EN ISO/IEC 27000. Työn tavoitteena oli valmista yhtiön tietoturvajärjestelmä ulkoista auditointia ja sertifiointia varten. Työssä perehdytään tietoturvallisuudenhallintajärjestelmän standardisointiin, keskittyen tietoturvariskien hallintaan. Riskienhallinnalla pyritään pienentämään riskejä.

Työssä käydään läpi standardien SFS-EN ISO/IEC 27000-27005 mukaista tietoturvariskien hallintaa. Yhtiön tietoturvallisuutta pyrittiin valmistelevaan sisäistä auditointia varten. Työ aloitettiin perehtymällä SFS-EN ISO/IEC 27000 standardisaraan. Niistä saatiin selville tietoturvan hallinnan eri osat ja tämän avulla määritettiin lähtökohta työlle. Tietoturvan riskienhallinnanohjeistus tehtiin standardin SFS-ISO/IEC 27005 mukaisella tavalla.

Standardisarja ohjeistaa jatkuvaan tietoturvalliseen parantamiseen. Ajantasaisella tietoturvallisuuden hallintajärjestelmällä pystytään takamaan tavoiteltu tietoturvasuustaso.

Työssä saavutettiin asetetut tavoitteet. Opinnäytetyön tuloksena yhtiö on paremmin valmistautunut ulkoista auditointia ja sertifiointia varten. Tuloksena syntyi standardien mukaiset ohjeistukset ja dokumentointipohjat tietoturvallisuuden riskienhallintaan.

Avainsanat: tietoturva, tietoturvan riskienhallinta, tietoturvallisuuden hallintajärjestelmä, standardi

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Mechanical Engineering

Specialisation: Mechanical Engineering

Author: Antti Kortelainen

Title of thesis: Standardising and benefits of standardisation of information security for a corporation

Supervisor: Heikki Heiskanen

Year: 2019

Number of pages: 33

Number of appendices: 0

Information security management systems hold all the information security of an organization and they are used to control it. A management system consists of many different parts. Standard series SFS-EN ISO/IEC 27000 deals with all the parts of an information management system. The main point of the thesis was to prepare a company's information security risk management for external audit and certification. In the thesis the standardisation of an information security management system was studied. The focus of the thesis was on the standardisation of information risk management. Information risk management was used to lessen the effects of risks.

The work centered on the SFS-EN ISO/IEC 27000-27005 information security risk management. The main point was to prepare the company's information security for internal audit. The work started by reading up on the SFS-EN ISO/IEC 27000 standard series. The series helped with defining the starting point for the thesis. Information security risk management templates were standardized. This was done according to the SFS-ISO/IEC 27005 which was the information security risk management standard.

The standard series SFS-EN ISO/IEC 27000 guides organizations for continual improvement. Only with an up-to-date information security management system can a target information security level be reached.

This thesis reached its main goals. The company is now better prepared for external audit and certification. The results of the thesis are the standardized guidelines and documentation templates for information security risk management.

Keywords: information security, information risk management, information security management system, standard

SISÄLTÖ

Opinnäytetyön tiivistelmä.....	1
Thesis abstract.....	2
SISÄLTÖ	2
Kuva-, kuvio- ja taulukkoluettelo	5
Käytetyt termit ja lyhenteet	6
1 JOHDANTO	7
1.1 Tausta	7
1.2 Työn tavoitteet.....	7
1.3 Työn rajaukset.....	7
1.4 Yritysesittely	8
2 TEORIA	9
2.1 Tietoturvallisuus	9
2.1.1 Tietoturvapoliittika	9
2.2 Standardi.....	9
2.3 SFS-EN ISO/IEC 27000 standardisarja	10
2.4 Standardisoinnista saatavat hyödyt.....	12
2.5 Tietoturvallisuus ja sen dokumentointi	12
2.6 Työssä käytetyt tietoturvallisuusstandardit	13
2.6.1 SFS-EN ISO/IEC 27000:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto.....	13
2.6.2 SFS-EN ISO/IEC 27001:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.	13
2.6.3 SFS-EN ISO/IEC 27002:2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Ohjeistava. ...	14
2.6.4 SFS-ISO/IEC 27003:2017. Information technology. Security techniques. Information security management systems. Guidance	16

2.6.5	SFS-ISO/IEC 27004:2016 2. painos. Informaatioteknologia. Turvallisuustekniikat. Seuranta, mittaus, analysointi ja arviointi. Ohjeistava.....	17
2.6.6	SFS-EN ISO/IEC 27005 2.painos. Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta. Ohjeistava	17
2.7	Tietoturvallisuuden riskienhallinta	17
2.7.1	Tausta	17
2.7.2	Tietoturvariskien hallintaprosessin yleiskuvaus.....	18
2.7.3	Tietoturvariskien hallinnan perusosien määrittäminen	18
2.7.4	Tietoturvariskien arviointi	19
2.7.5	Riskien tunnistaminen	20
2.7.6	Riskianalyysi	21
2.7.7	Riskien merkityksen arviointi.....	22
2.7.8	Tietoturvariskien käsittely.....	22
2.7.9	Tietoturvariskien hyväksyminen	24
2.7.10	Tietoturvariskejä koskeva viestintä	24
2.7.11	Tietoturvariskien seuranta.....	25
3	TUTKIMUSMENETELMÄT	26
4	TULOKSET JA TULOSTEN TARKASTELU	28
4.1	Ohjeistukset	28
4.2	Dokumentointipohjat	29
5	JOHTOPÄÄTÖKSET JA SUOSITUKSET	30
6	YHTEENVETO.....	31
	LÄHTEET	32

Kuva-, kuvio- ja taulukkoluetelo

Kuvio 1. Tietoturvallisuuden hallintajärjestelmä kokonaisuus. 26

Taulukko 1. ISO/IEC 27000 standardisarja. 10

Käytetyt termit ja lyhenteet

Auditointi	Auditointi on riippumaton ja dokumentoitu prosessi, jossa objektiivisesti määritetään sovittujen auditointikriteerien täyttymistä.
Haavoittuvuus	Heikkous, jota uhka voi käyttää hyväkseen.
Hallintakeino	Riskiä muuttava toimenpide.
Riski	Haitallisen tapahtuman mahdollisuus.
Soveltuvuuslausunto	Soveltuvuuslausunnosta käy selville organisaation tai sen osan kaikki hallintakeinot sekä perustelut miksi ne ovat tai eivät ole käytössä. Tämä sisältää kaikki standardin SFS-EN ISO/IEC 27001 liitteessä A olevat hallintakeinot vähintään.
TTHJ (ISMS)	Tietoturvallisuuden hallintajärjestelmä. (Information security management system.)
Uhka	Mahdollinen syy epätoivottuun tapahtumaan.

1 JOHDANTO

1.1 Tausta

Työssä keskitytään enimmäkseen tietoturvallisuudenriskin hallintaan. Työn tarkoituksena oli luoda ohjeistus ja pohjat yhtiön tietoturvanriskin hallintaan. Yhtiöllä oli valmiiksi tietoturvajärjestelmä, mutta se ei ollut standardien mukainen. Tietoturvajärjestelmän standardisoinnilla tarkoitetaan, että tietoturvajärjestelmä on tiettyjen standardien mukainen. Tässä tapauksessa standardien SFS-EN ISO/IEC 27000-27005 mukainen. Riskienhallintaan keskittyvä standardi SFS-EN ISO/IEC 27005 on keskeisessä osassa tietoturvan standardisoinnissa.

Yhtiön tietoturvajärjestelmän standardisointi täyttää vaaditun tason vasta ulkopuolisen auditoinnin jälkeen. Työssä pyrittiin valmistelemaan tietoturvajärjestelmä sisäistä auditointia varten, joka suoritetaan ennen ulkoista auditointia kustannussyistä. Sisäisen ja ulkoisen auditoinnin eroina on taho, joka suorittaa auditoinnin. Sisäisessä auditoinnissa yhtiö itse tekee sen ja ulkoisessa auditoinnissa ulkopuolinen riippumaton taho suorittaa sen.

1.2 Työn tavoitteet

Tavoitteena oli valmistella yhtiön tietoturvajärjestelmä ulkoista auditointia ja sertifiointia varten. Auditointia varten tietoturvajärjestelmä piti standardisoida. Standardisoinnilla tavoiteltiin lisäksi läpinäkyvyyttä yhtiön tietoturvaan.

1.3 Työn rajaukset

Työssä käytetty standardisarja on SFS-EN ISO/IEC 27000. Standardisarjasta käytettiin standardeja 27000-27005. Työ rajattiin näihin standardeihin, koska ne ovat keskeisimmät tietoturvallisuusstandardit yhtiölle. Tässä vaiheessa yhtiö keskittyy standardisoimaan oleelliset kokonaisuudet. ISO/IEC 27007 otetaan käyttöön, kun yhtiö valmistautuu tiedonhallintajärjestelmän ulkoiseen auditointiin.

1.4 Yritysesittely

Salassapitosopimuksen mukaan mitään yhtiön tietoja ei tule näkymään julkisissa dokumenteissa.

2 TEORIA

2.1 Tietoturvallisuus

Tietoturvallisuudella pyritään suojaamaan tieto-omaisuutta. Tämä voi olla henkilö-tietoja, aineetonta omaisuutta, taloudellista tietoa jne. Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, käytettävyydestä, eheydestä, kiistämättömyydestä ja pääsynvalvonnasta. Tiedon luottamuksellisuudella tarkoitetaan, että tieto on vain sitä oikeutettujen henkilöiden käytettävissä. Käytettävyydellä tarkoitetaan, että tieto on saatavissa ja se löytyy nopeasti. Tiedon eheydellä varmistetaan, että tiedot pitävät paikkaansa. Kiistämättömyydellä tarkoitetaan, että tiedon käyttäjät tunnistetaan ja heidän tietonsa tallennetaan. Pääsynvalvonnalla estetään luvottomien käyttäjien pääsy tietoihin. (Hakala, Vainio & Vuorinen 2006, 4-5.)

2.2 Tietoturvapoliitiikka

Tietoturvapoliitiikan, vanhemmalta nimeltä atk-poliitiikan, tulee olla osa organisaation kokonaisturvapoliitiikka. Näiden politiikoiden laatiminen on organisaation johdon vastuulla. Poliitiikat tehdään kirjallisena ja niiden tarkoitus on ohjeistaa turvallisuuden suunnittelemisessa. Poliitiikat tulee kirjoittaa sellaisen muotoon, että muutkin kuin turvallisuushenkilöt ymmärtävät sen. Kirjoitetut politiikat eivät saa sisältää tietoa, jota voidaan käyttää hyödyksi hyökkäyksen suunnittelussa. Poliitiikkoja tarkentava ohjeistus tulee olla luettelona kirjoitetussa politiikassa. Tietoturvasuunnitelmalla pyritään pääsemään tietoturvapoliitiikan määrittämälle tasolle. Suunnitelmassa määritetään yksityiskohtaisesti, miten tämä saavutetaan. Tietoturvaohjeet jatkapäiväiseen toimintaan voidaan luoda karsimalla yksityiskohtia pois tietoturvasuunnitelmasta. (Hakala, Vainio & Vuorinen 2006, 7-10.)

2.3 Standardi

Standardi on asiakirja, joka on laadittu yhteisten toimintatapojen pohjalta. Standardisoidulla varmistetaan tuotteiden ja järjestelmien toimivuus sekä yhteensopivuus.

Standardit tarjoavat säännöt, ohjeistuksen ja ominaisuudet tuotteille. (Standardit tutuksi 2019.)

Kirjainyhdistelmät standardin nimen alussa kertovat, missä standardi on laadittu sekä missä se on voimassa. Standardien rakenne muodostuu alustavista, velvoittavista ja opastavista osioista. Standardin soveltamisala osoittaa sen käyttökohteen. (Standardit tutuksi 2019.)

Kansainvälisiä standardeja suositellaan käytettäväksi mieluummin kuin kansallisia, jos se on mahdollista. Tällä saavutetaan suuremmat markkinat. Vain standardien mukainen tuote hyväksytään markkinoille. (Developing International Standards 2019.)

2.4 SFS-EN ISO/IEC 27000 -standardisarja

ISO/IEC tietoturvallisuuden hallintajärjestelmästandardisarjaa pidetään alansa uusimman kehityksen mukaisena. Standardisarja esittää mallin hallintajärjestelmien luomiseen ja käyttöönottoon. Sitä noudattamalla voidaan saavuttaa tietoturvallisuuden perusedellytykset ja valmistautua auditointiin. Se on kansainvälinen ja kaikki organisaatiot voivat soveltaa sitä toiminnoissaan. Se koostuu toisiinsa liittyvistä standardeista. Taulukosta 1 näkee kaikki standardisarjan standardit. Vihreällä värillä on korostettu työssä käytetyt standardit. Tummennettuja standardeja ei käsitellä tässä työssä ollenkaan. (SFS-EN ISO/IEC 27000 2017, 5.)

Taulukko 1. ISO/IEC 27000 standardisarja.

Sanasto	27000					
Vaatimukset	27001	27006	27009			
Ohjeistukset	27002	27003	27004	27005	27007	
	TR 27008	27013	27014	TR 27016		
Toimialakohtaiset	27010	27011	27015	27017	27018	27019
Hallintakeino- kohtaiset	2703X	2704X				

Työssä käytettyjä standardeja käsitellään enemmän kohdassa kolme. Standardi ISO/IEC:

- 27000 sisältää standardisarjan yleiskuvauksen ja sanaston.
- 27001 käsittelee tietoturvallisuuden hallintajärjestelmän luomista sekä käyttöä koskevien standardien asettamia vaatimuksia. Standardi esittelee myös hallintakeinoja. Tämän standardin vaatimukset suorittamalla organisaatio voi saada sertifiointin auditoinnin jälkeen.
- 27006 sisältää tietoturvallisuuden hallintajärjestelmien auditointi- ja sertifiointia koskevat vaatimukset. Standardi täydentää standardia ISO/IEC 17021, joka on johtamisjärjestelmien auditointiin ja sertifiointiin tarkoitettu. (SFS-EN ISO/IEC 17021-1 2015.)
- 27002 esittää menettelyohjeet standardin ISO/IEC 27001 liitteen A hallintakeinojen toteuttamiseen.
- 27003 sisältää prosessin standardin ISO/IEC 27001 vaatimusten toteuttamiseksi.
- 27004 käsittelee tietoturvallisuuden hallintajärjestelmän vaikuttavuuden mittausta.
- 27005 ohjeistaa riskienhallintaa ja riskienhallintajärjestelmän luontiin.
- 27007 esittää auditointiohjeet organisaatiolle, jotka suorittavat ISO/IEC 27001:n auditointeja.
- TR 27008 on standardisoitu tekninen raportti (TR). Raportti käsittelee hallintakeinojen katselmointia. Tämä raportti on tarkoitettu hallintakeinojen auditoiduille, mutta ei hallintajärjestelmien auditointiin.
- 27013 sisältää ohjeistusta standardien ISO/IEC 27001 ja ISO/IEC 20000 hallintajärjestelmien suunnitteluun. ISO/IEC 20000 käsittelee palvelunhallintajärjestelmiä. (SFS-ISO/IEC 20000-1 2018.)
- 27014 ohjeistaa organisaatioita tietoturvallisuuden hallinnoinnissa.
- TR 27016 käsittelee ja ohjeistaa tietoturvallisuuden taloudellisuutta. (SFS-EN ISO/IEC 27000 2017, 27-30.)

2.5 Standardisoinnista saatavat hyödyt

Käyttämällä standardisarjaa SFS-EN ISO/IEC 27000 saavutetaan pienempi riskien toteutumistodennäköisyys ja pienennetään riskien vaikutuksia. Standardisarja opastaa käyttämään maailmanlaajuisesti hyväksyttyjä tietoturvallisuuskäytäntöjä ja parantamaan tietoturvallisuutta jatkuvasti. Toteuttamalla vaatimusstandardin SFS-EN ISO/IEC 27001 ja hankkimalla sertifiointin yritys pystyy todistamaan tietoturvallisuustasonsa. Laillisista sekä sopimuksellisista syistä organisaatiolla voi olla tarve pystyä todistamaan tietoturvallisuustasonsa. (SFS-EN ISO/IEC 27000 2017, 25-26.)

Standardisarja opastaa kokonaisvaltaiseen tietoturvallisuuden toteutukseen ja käyttöönnottoon sekä ylläpitoon. Tämä tapahtuu kattavalla ja kustannustehokkaalla tavalla. Standardisarja auttaa pitämään yrityksen johdon ajan tasalla ja opastamaan alaisiaan tietoturvallisuudessa. Standardeja noudattamalla voidaan tehdä tehokkaita tietoturvainvestointeja. (SFS-EN ISO/IEC 27000 2017, 25-26.)

2.6 Tietoturvallisuus ja sen dokumentointi

Kaikki mahdollisesti tarvittava tieto tietoturvallisuuteen liittyen tulee olla dokumentoituna organisaation käytettävissä. Kaikki versiot eri dokumenteista tulee säilyttää. Dokumentoimalla kaikki tietoturvallisuuteen liittyvä tieto pystytään tarkistelemaan organisaation tietoturvallisuuden kehitystä ja tiedetään varmasti sen nykytilanne. Dokumentteihin tulee olla pääsy ainoastaan henkilöillä, joilla on lupa katselmoida tai muokata niitä. (SFS-EN ISO/IEC 27001 2017, 11.)

Tietoturvallisuuden luonnissa, päivityksessä ja käytössä syntyy paljon erilaisia dokumentteja. Nämä dokumentit on hyvä luetteloida ja ryhmitellä. Tämä nopeuttaa niiden löytämistä sekä tarkastelua. Dokumentit voidaan ryhmitellä esimerkiksi toimintaa ohjaaviksi ja toiminnan raporteiksi. Nämä ryhmät on hyvä vielä jakaa tarkemmin pienemmiksi kokonaisuuksiksi. (Hakala, Vainio & Vuorinen 2006, 32-35.)

Dokumenttien rakenne tulee olla samanlainen. Kaikista dokumenteista tulee löytyä tekijä, päivämäärä ja muut yleiset tiedot. Tämä saavutetaan helpoiten käyttämällä

organisaatioiden itse suunnittelemaa dokumentointipohjia, joista ilmenee kaikki organisaatiolle tarpeelliset tiedot. Kaikki dokumentit tulee olla tallennettuna organisaation hyväksymään muotoon, esimerkiksi doc-, xlsx- tai pdf-muotoon. (Hakala, Vainio & Vuorinen 2006, 32-35.)

2.7 Työssä käytetyt tietoturvallisuusstandardit

2.7.1 SFS-EN ISO/IEC 27000:2017. Informaatioteknologia.

Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät.

Yleiskuvaus ja sanasto.

Standardi sisältää tietoturvallisuuden hallintajärjestelmän yleiskuvauksen, aiheeseen liittyvät termit sekä TTHJ-standardisarjan esittelyn. Standardisarja on paljon laajempi kokonaisuus kuin tässä opinnäytetyössä käytetyt standardit.

2.7.2 SFS-EN ISO/IEC 27001:2017. Informaatioteknologia.

Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät.

Vaatimukset.

Opinnäytetyön tarkoituksena oli toteuttaa tämän standardin vaatimukset kyseisen standardisarjan avulla. Tässä standardissa käsitellään TTHJ:n luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista.

TTHJ:n luonnissa ja toteutuksessa tulee huomioida organisaation

- tarpeet
- tavoitteet
- turvallisuusvaatimukset
- käytettävät organisaation prosessit
- organisaation koko
- organisaation rakenne.

Nämä tekijät voivat muuttua organisaation kehittyessä ja ajan kuluessa. TTHJ:n tavoitteena on suojata tietoa ja hallita tietoturvariskejä. Tietoturvan tulee olla osa organisaation prosesseja ja suunnittelua.

2.7.3 SFS-EN ISO/IEC 27002:2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Ohjeistava.

Tässä ohjeistavassa standardissa keskitytään tietoturvan hallintakeinoin ja niiden toteuttamiseen. Ennen kuin voidaan valita ja toteuttaa hallintakeinoja täytyy ymmärtää

- mitä pyritään suojaamaan
- organisaation toimintaympäristö
- tietoturvavaatimukset
- hallintakeinojen valinta
- organisaation oman ohjeistuksen kehittäminen
- elinkaarta koskevat näkökohdat.

Kaikki organisaatiot keräävät, käsittelevät ja tallentavat tietoa. Tieto ja kaikki tiedon suojaamiseen liittyvät asiat ovat suojattavaa omaisuutta. Tämä omaisuus on tärkeää liiketoiminnalle ja sitä tulee suojata kaikkia uhkia vastaan. Uhat voivat olla tahattomia tai tahallisia. Tietoturvariskeiltä ei voi kokonaan välttyä. Tietoturvallisuudella pyritään pienentämään tietoturvariskejä ja riskien vaikutuksia.

Tietoturvallisuus saavutetaan TTHJ:n avulla. TTHJ koostuu seuraavista hallintakeinokokonaisuuksista:

- politiikoista
- prosesseista
- menettelyistä
- organisaation rakenteista
- ohjelmistoista
- laitteistoista.

Hallintakeinoille on laadittava ohjeistus ja ne on otettava käyttöön. Hallintakeinojen jatkuvalla parantamisella pidetään tietoturva ajan tasalla. TTHJ:n avulla pystytään hallitsemaan tietoturvakokonaisuutta.

Teknisillä tietoturvakeinoilla on rajansa. Kokonaisvaltaisen tietoturvan saavuttamiseen tarvitaan organisaation kaikkien jäsenten tuki. TTHJ vakuuttaa organisaation johdon sekä sidosryhmät siitä, että tieto ja täten liiketoiminta on suojattu.

Organisaation tietoturvavaatimukset koostuvat kolmesta kokonaisuudesta. Nämä ovat

- riskien arviointi
- lait, asetukset sekä sopimukset
- organisaation periaatteet ja tavoitteet.

Hallintakeinot voivat olla suoraan standardista otettuja, mutta yleensä niitä joutuu muuttamaan organisaatiolle sopiviksi. Täysin uusia hallintakeinoja voidaan kehittää tarpeen vaatiessa. Hallintakeinojen valinta tulee suhteuttaa siihen tarvittaviin resursseihin ja hallintakeinojen puutteeseen. Tämä tarkoittaa riskitapahtuman toteutumista ja siitä aiheutuvia kustannuksia. Riskien arviointia voidaan käyttää hallintakeinojen valinnan apuna ja samalla saadaan tärkeysjärjestys hallintakeinoille. Valinnassa tulee huomioida lait ja asetukset.

Tietoturvaohjeistuksen lähtökohtana tulisi olla tämä standardi. Lisäksi saattaa olla tarve hallintakeinoille ja ohjeistukselle, jota ei ole tässä standardissa.

Tiedon elinkaari koostuu sen

- luomisesta
- varastoinnista
- käsittelystä
- viestimisestä
- hävittämisestä tai tuhoutumisesta.

Tiedon elinkaaren eri kohdissa sen arvot ja riskit voivat vaihdella. Tietojärjestelmän elinkaari koostuu sen

- perustamisesta
- määrittelystä

- suunnittelusta
- kehittämisestä
- testauksesta
- toteutuksesta
- käytöstä
- ylläpidosta
- käytön poistamisesta
- hävittämisestä.

Tietoturvallisuus tulisi huomioida tietojärjestelmän kaikissa vaiheissa. Jatkuva parantaminen on tärkeä osa TTHJ:ä.

2.7.4 SFS-ISO/IEC 27003:2017. Information technology. Security techniques. Information security management systems. Guidance

Tässä englanninkielisessä ohjeistavassa standardissa keskitytään TTHJ:n ja sen soveltamiseen yleisellä tasolla. TTHJ koostuu seuraavista vaiheista:

- organisaation tarpeiden ja tietoturvan ymmärtämisestä
- riskien arvioinnista
- tietoturvaprosessin käyttöönotosta ja käyttämisestä
- TTHJ:n seuraamisesta ja arvioinnista
- TTHJ:n jatkuvasta parantamisesta.

TTHJ koostuu seuraavista osista

- politiikoista
- henkilöiden vastuista
- hallintaprosesseista
- dokumentoidusta tiedosta
- riskien arvioinnista
- riskien käsittelystä.

Kaikki tämän standardin kohdat eivät sovellu kaikille organisaatioille. Osa ohjeistuksesta soveltuu paremmin suurille kuin pienille organisaatioille.

2.7.5 SFS-ISO/IEC 27004:2016 2. painos. Informaatioteknologia.

Turvallisuustekniikat. Seuranta, mittaus, analysointi ja arviointi.

Ohjeistava.

Tämä ohjeistava standardi keskittyy TTHJ:n (ISO/IEC 27001) seurantaan, mittaukseen, analysointiin ja arviointiin. Seurannan ja mittausten tulokset tukevat tietoturvacyklin tekoa. Standardin ohjeistus tulee mukauttaa organisaation tarpeisiin.

2.7.6 SFS-EN ISO/IEC 27005 2.painos. Informaatioteknologia. Turvallisuus.

Tietoturvariskien hallinta. Ohjeistava

Tämä ohjeistava standardi keskittyy tietoturvariskien hallintaan, joka on tärkeä osa TTHJ:ä (ISO/IEC 27001). Standardissa ei ole tiettyä tietoturvariskien käsittelytapaa. Organisaatioiden tulee laatia standardin pohjalta itselleen sopiva menetelmä.

2.8 Tietoturvallisuuden riskienhallinta

2.8.1 Tausta

Järjestelmällisellä tietoturvariskien hallinnalla voidaan saavuttaa organisaation tietoturvavaatimukset. Tietoturvariskien hallinnan tulee olla linjassa organisaation yleisen riskienhallinnan kanssa. Tietoturvariskien hallinta on jatkuva prosessi, jonka tulee vastata riskeihin vaikuttavasti ja nopeasti. Tällä hallintaprosessilla pyritään pienentämään riskit hyväksyttävälle tasolle. Prosessia voidaan soveltaa koko organisaatioon tai johonkin sen osaan. (SFS ISO/IEC 27005 2013,18-20.)

Organisaatiot muuttuvat ja samoin niiden toimintaympäristö voi muuttua. Tämä voi vaikuttaa organisaation riskiprofiiliin, liiketoiminnan päämääriin, strategioihin, toimintaan tai markkinoihin, joilla organisaatio toimii. Riskien hallinnalla pyritään pienentämään epävarmojen muutoksien vaikutuksia sekä varautumaan niihin. Muutosten tapahtuessa organisaatioiden tulee arvioida uudelleen riskit ja mahdollisuudet,

joita muutokset aiheuttavat. Näiden muutosten arviointi tulee olla osa TTHJ:n jatkuvaa parantamista. (Humphreys 2016, 44.)

2.8.2 Tietoturvariskien hallintaprosessin yleiskuvaus

Tietoturvariskien hallintaprosessi koostuu tietoturvariskien

- hallinnan perusosien määrittämisestä
- arvioinnista
- käsittelystä
- hyväksymisestä
- viestinnästä
- seurannasta.

Nämä prosessin vaiheet voivat toistua useamman kerran prosessin läpikäynnin aikana. Toistoilla voidaan saavuttaa yksityiskohtaisempi riskinhallinta. Riskinhallintaprosessi käydään yleensä yllä olevan luettelon mukaisessa järjestyksessä pois lukien viestintä ja seuranta. Nämä kaksi kohtaa voidaan suorittaa kaikissa prosessin vaiheissa. Organisaation tulee varmistaa tarvittavien resurssien varaaminen tietoturvariskien hallintaprosessia varten. (SFS ISO/IEC 27005 2013, 22.)

2.8.3 Tietoturvariskien hallinnan perusosien määrittäminen

Riskienhallintajärjestelmän suunnittelu alkaa toimintaympäristön määrittämisellä. Toimintaympäristön määrittämiseen tarvitaan kaikki olennaiset tiedot organisaation tietoturvallisuuteen liittyen. Ulkoinen ja sisäinen toimintaympäristö tulee määrittää. Tietoturvariskien hallinnan päämäärä täytyy määrittää eli mitä pyritään saavuttamaan riskien hallinnalla. Päämäärien määrittämiseen vaikuttavat lait, pyritty laatu-taso, liiketoiminnan jatkuminen ja tietoturvahäiriöiden vähentäminen. (SFS ISO/IEC 27005 2013, 26.)

Tietoturvariskien hallintaprosessi koostuu

- arviointikriteereistä
- vaikutuskriteereistä

- riskien hyväksymiskriteereistä
- tietoturvariskien hallinnan rajoista
- organisoinnista. (SFS ISO/IEC 27005 2013, 26-30.)

Yllä olevan luettelon kolmea kriteeriä kutsutaan tietoturvariskien hallintaprosessin peruskriteereiksi. Arviointikriteerillä arvioidaan, mitä riski merkitsee organisaatiolle. Mihin riski vaikuttaa? Vaikutuskriteerillä arvioidaan riskin vahingot ja kustannukset. Miten riski vaikuttaa? Hyväksymiskriteerillä arvioidaan riskin hyväksyttävyyttä. Mikä on tavoite riskitaso ja millä perusteilla voidaan hyväksyä korkeampi riskitaso? Tietoturvariskien hallinnan rajat ja laajuus täytyy määrittää. Mikä kuuluu hallinnan piiriin? Tällä varmistetaan, että riskien arvioinnissa huomioidaan kaikki oleellinen. Tietoturvariskien hallinnan rajaamisessa täytyy perustella, miksi jotkin asiat ovat jätetty rajojen ulkopuolelle. Organisoinnilla määritetään vastuut ja säilytettävät tallenteet. Kuka on vastuussa mistäkin ja mitä säilytetään? (SFS ISO/IEC 27005 2013, 26-30.)

2.8.4 Tietoturvariskien arviointi

Tietoturvariskien arvioinnilla tunnistetaan ja määritetään riskejä. Riski kuvaillaan määrällisesti tai laadullisesti. Arvioinnilla saadaan määritettyä riskeille tärkeysjärjestys. Riskin arviointi koostuu riskien tunnistamisesta, riskianalyysistä ja riskin merkityksen arvioinnista. Riskin arvioinnissa määritetään. (SFS ISO/IEC 27005 2013, 32.)

- suojattavien kohteiden arvo
- kohdistuvat uhat
- haavoittuvuudet
- nykyiset hallintakeinot
- hallintakeinojen vaikutus riskeihin
- mahdolliset seuraukset
- riskien priorisointi. (SFS ISO/IEC 27005 2013, 32.)

Riskin arviointia voidaan toistaa useamman kerran tietoturvan hallintaprosessin aikana, jotta pystytään perehtymään kaikkiin riskeihin tarpeeksi syvällisesti. Riskien

arviointi tulee olla aina räätälöity kyseiselle organisaatiolle. (SFS ISO/IEC 27005 2013, 32.)

2.8.5 Riskien tunnistaminen

Riskien tunnistamisella määritetään mahdolliset tappiot ja tappioiden syntyperä. Riskien tunnistamisen tulee kattaa kaikki mahdolliset riskit. Organisaation tulee tunnistaa suojattavat kohteet ja niiden osat. Suojattava kohde on asia, jolla on arvoa organisaatiolle. Tietoturvallisuuden hallintaprosessissa suojattavien kohteiden tunnistamista voidaan toistaa useamman kerran, jotta saadaan kaikki mahdollinen tieto kohteista. Tämä ei välttämättä luo lisäarvoa, mutta varmistetaan kaikkien suojattavien kohteiden osienkin läpikäynti. Suojattavalle kohteelle määritetään omistaja, joka huolehtii kohteen elinkaaresta ja suojauksesta. Suojattaville kohteille voidaan antaa erilaisia arvoja, joilla pyritään kuvaamaan niiden arvoa organisaatiolle. (SFS ISO/IEC 27005 2013, 32-34.)

Organisaation tulee tunnistaa uhat ja niiden aiheuttajat. Uhka on asia, joka saattaa vahingoittaa suojattavaa kohdetta. Uhan aiheuttaja voi olla luonnollinen, ihmisten aiheuttama, tahaton tai tahallinen. Kaikki uhat ja uhkien aiheuttajat tulee tunnistaa. Uhkien arvioinnissa on hyvä käyttää aiempaa tietoa tietoturvatapahtumista sekä uhka-arvioinneista. (SFS ISO/IEC 27005 2013, 34-36.)

Organisaation tulee tunnistaa käytössä olevat hallintakeinot sekä niiden toimivuus. Tällä pyritään vähentämään kustannuksia (hallintakeinojen toimintaa ja vaikutusta käsitellään laajemmin standardissa ISO/IEC 27004). Suunniteltuja hallintakeinoja tulisi arvioida kuin ne olisivat jo käytössä. Toimimattomat hallintakeinot tulee poistaa käytöstä tai korvata kustannusten sekä mahdollisten riskien vuoksi. Kaikkien organisaation hallintakeinojen tulisi löytyä dokumentoituna tietona, kuten esimerkiksi organisaation soveltuvuuslausunnosta. (Soveltuvuuslausuntoa käsitellään standardissa ISO/IEC 27003.) (SFS ISO/IEC 27005 2013, 36.)

Haavoittuvuus ei itsessään aiheuta vahinkoa. Vahinko tapahtuu uhan käyttäessä haavoittuvuutta hyväkseen. Kaikki haavoittuvuudet tulee määrittää ja niitä tulee seu-

rata muutosten varalta. Haavoittuvuuksia voi ilmetä kaikkialla organisaatiossa. Haavoittuvuus yleensä liittyy suojattavan kohteen ominaisuuksiin. (SFS ISO/IEC 27005 2013, 38.)

Tietoturvahäiriöskenaarioriskien toteutuminen on yhden tai useamman riskin toteutuminen kuvaava tapahtumasarja. Tietoturvahäiriöskenaarion avulla voidaan määrittää mahdollisia seurauksia ja vahinkoja. Tietoturvahäiriöskenaarion vaikutuksia arvioidaan vaikutuskriteerin avulla. Suojattavien kohteiden arvojen avulla voidaan määrittää useampaan suojattavaan kohteeseen vaikuttavia tietoturvahäiriöskenarioita. Syvässä skenaarioiden arvioinnissa tulee huomioida riskin vaikutukset pidemmällä aikavälillä. Tästä esimerkkinä voidaan ottaa tuotantolaitteen hajoaminen, jonka seurauksena kuluu resursseja vahingon tutkimiseen, vahingon huoltoon, tuotannon pysähtymiseen, vaikutukset tuotteiden tilauksiin, mahdollisten tulevien tilausten peruuntuminen sekä vaikutukset työturvallisuuteen. (SFS ISO/IEC 27005 2013, 38-40.)

2.8.6 Riskianalyysi

Riskianalyysillä arvioidaan riskin seurauksia, häiriöiden todennäköisyyttä ja riskitasoa. Riskianalyysi voi olla laadullinen tai määrällinen. Laadullisella analyysillä saadaan nopeasti suurpiirteisesti analysoitua riski, ja määrällisellä saadaan analyysiin tarkkuutta. Määrällisessä analyysissä kuvataan riskiä numeroin ja laadullisessa sanoin. (SFS ISO/IEC 27005 2013, 40.)

Riskin seurauksia on helpoin arvioida rahallisena arvona. Tämä antaa tarvittavaa tietoa päätöksentekoa varten. Vahingoittuneiden suojattavien kohteiden yhteen lasketulla arvolla voidaan kuvata riskin seurauksia. Tämä ei anna kokonaiskuvaa riskin seurauksista, mutta sitä voidaan käyttää lähtökohtana. Mallintamalla tietoturvahäiriöskenaarioriskien pystytään määrittämään kaikki vahingoittuneet suojattavat kohteet sekä vahingon vaikutukset niihin. Riskin seurauksia voidaan kuvata useammalla arvolla. Tästä esimerkkinä rahallinen arvo, organisaation maineen arvo ja työturvallisuusarvo. Tämä tulee huomioida vaikutuskriteerin määrittelyssä. (SFS ISO/IEC 27005 2013, 42.)

Häiriöskenaarioiden todennäköisyys tulee määrittää, kun häiriöskenaariot on määritetty. Todennäköisyyksien määrittämisen tukena voidaan käyttää erilaisia tilastoja tai organisaation omaa kokemusta niistä. Haavoittuvuudet lisäävät todennäköisyyttä ja etenkin monen haavoittuvuuden yhteisvaikutus voi olla suuri. (SFS ISO/IEC 27005 2013, 44.)

Häiriöskenaarioiden riskitaso tulee määrittää. Tämä tapahtuu riskien seurauksille sekä häiriöskenaarioiden todennäköisyyksille annettujen arvojen avulla. (SFS ISO/IEC 27005 2013, 44.)

2.8.7 Riskien merkityksen arviointi

Häiriöskenaarioiden riskitasoa verrataan riskien arviointikriteeriin. Näin pystytään arvioimaan riskin merkitystä organisaatiolle. Riskien merkityksen arvioinnin jälkeen riskit listataan tärkeysjärjestykseen. Tätä listaa käytetään apuna riskien käsittelyn päätöksenteossa. (SFS ISO/IEC 27005 2013, 46.)

2.8.8 Tietoturvariskien käsittely

Tietoturvariskien käsittelyllä pyritään pienentämään tietoturvariskejä. Jäljelle jäävää riskiä kutsutaan jäännösriskiksi. Kaikkia riskejä ei pystytä koskaan poistamaan kokonaan. Riskin käsittely kattaa neljä eri vaihtoehtoa. Nämä vaihtoehdot eivät ole toisiaan poissulkevia. Riskin käsittelyn vaihtoehdoista parhaita ovat halvat hallintakeinot, jotka vähentävät riskiä huomattavasti. Yhden riskin käsittelyllä saatetaan vaikuttaa useampaan riskiin. (SFS ISO/IEC 27005 2013, 46-50.)

Riskin käsittelysuunnitelmalla kuvataan riskin pienentämiseen suunniteltuja toimia ja mitä hallintakeinoja käytetään. Suunnitelmassa määritetään riskin käsittelytoimenpiteiden tärkeysjärjestys sekä aikataulu. Suunnitelmaan on myös hyvä sisällyttää tarvittavat resurssit. Organisaation johtajien tehtävänä on hyväksyä tai hylätä ehdotetut riskien käsittelysuunnitelmat. (SFS ISO/IEC 27005 2013, 50.)

Organisaatioon kohdistuvat rajoitukset tulee tunnistaa ja selvittää. Ne saattavat vaikuttaa riskien käsittelyvaihtoihin. Rajoitukset voivat johtua esimerkiksi organisaation

toiminta ympäristöstä, laista tai organisaation rakenteesta. (SFS ISO/IEC 27005 2013, 50.)

Jäännösriski tulee määrittää. Tämä tapahtuu toistamalla riskinhallinta prosessi kuin riskin käsittelysuunnitelma olisi jo toteutettu. Jäännösriskin riskitaso saattaa olla liian korkea, ja riskin käsittelysuunnitelma joudutaan tämän takia uusimaan tai jäännös-riski vain hyväksytään. (SFS ISO/IEC 27005 2013, 50.)

Riskinkäsittelyn neljä vaihtoehtoa ovat riskin muokkaaminen, säilyttäminen, välttäminen ja jakaminen. Riskin muokkaamisella alennetaan riskitaso hallintakeinojen avulla hyväksyttäväksi. Hallintakeinojen valinta tulee aina olla perusteltu. Sen kokonaiskustannuksia kannattaa verrata suojattavan kohteen arvoon. Jotkin hallintakeinot voivat tarjota organisaatiolle uusia liiketoimintamahdollisuuksia. Tästä esimerkkinä hallintakeinon erityisosaaminen. Hallintakeino saattaa vaikuttaa organisaation tuottavuuteen. Huono hallintakeino saattaa jopa lisätä riskiä. Mahdolliset vaikuttavat hallintakeinot tulee luetteloida. Luettelossa voidaan ottaa kantaa niiden kustannuksiin, hyötyihin tai tärkeysjärjestykseen. Luetteloa voidaan käyttää hyödyksi riskinkäsittelyn päätöksenteossa. (SFS ISO/IEC 27005 2013, 50.)

Riski voidaan säilyttää, jos riskitaso on valmiiksi hyväksyttävällä tasolla, tai jos hyväksymällä se saavutetaan uusia liiketoimintamahdollisuuksia. Riskin säilyttämisen tulee aina olla perusteltua. (SFS ISO/IEC 27005 2013, 52.)

Riskin välttäminen ei aina ole mahdollista. Joitain riskejä aiheuttavia toimintoja tai olosuhteita voidaan välttää, mutta tämä saattaa vaikuttaa liiketoimintamahdollisuuksiin. Riskin välttäminen voi olla tarpeen, kun muut riskin käsittelyvaihtoehdot eivät pienennä sitä tarpeeksi tai niiden kustannukset ovat liian suuret. (SFS ISO/IEC 27005 2013, 52.)

Jotkin riskit voidaan jakaa muiden osapuolien kanssa. Muut osapuolet saattavat pystyä vaikuttamaan siihen enemmän kuin organisaation sisäiset hallintakeinot. Tämä saattaa itsessään aiheuttaa uusia riskejä. Riskin jakaminen ei välttämättä jaa vastuuta. (SFS ISO/IEC 27005 2013, 52.)

2.8.9 Tietoturvariskien hyväksyminen

Riskien ja jäännösriskien hyväksymisen tulee aina olla perusteltua. Perustelussa tulee ilmoittaa, ylittääkö riskitaso riskien hyväksymiskriteerit. Nämä kriteerit voivat muodostua useammasta hyväksymistasosta. Näitä kriteerejä on hyvä käyttää apuna riskien hyväksymisessä, mutta ne eivät saa yksinään määrätä sitä. (SFS ISO/IEC 27005 2013, 54.)

Vaikka hyväksymiskriteeri ei täyty, riskin hyväksymistä voidaan perustella sillä, että vallitsevia olosuhteita ei huomioitu hyväksymiskriteerin luonnissa. Tässä tapauksessa riski voidaan hyväksyä tai hylätä. Riskin hyväksymiskriteereihin tulee tässä tapauksessa lisätä uusi kohta tai niitä tulee muuttaa päätöksen perusteella. (SFS ISO/IEC 27005 2013, 54.)

Kaikissa tapauksissa ei ole tarpeeksi aikaa tarkistaa riskien hyväksymiskriteereitä. Tällaisia tapauksia varten tulee olla menettely, jossa todetaan riskit ja perustellaan, miksi riskien hyväksymiskriteerit ohitettiin. (SFS ISO/IEC 27005 2013, 54.)

2.8.10 Tietoturvariskejä koskeva viestintä

Riskeistä tulee tiedottaa yrityksen sisällä sekä olennaisille sidosryhmille. Viestinnällä pyritään saavuttamaan yksimielisyys riskienhallinnasta. Sidosryhmien kanssa viestimällä pyritään saamaan heidän näkemyksensä riskeistä ja niiden vaikutuksista. Sidosryhmien käsitykset samoista riskeistä voi poiketa suuresti organisaation näkemyksestä. Sidosryhmien näkemykset sekä tietoturvatavoitteet tulee tunnistaa ja dokumentoida. Näin voidaan käsitellä organisaatioiden välistä tietoturvallisuutta. Riskeistä tulee viestiä jatkuvasti muutosten tapahtuessa. (SFS ISO/IEC 27005 2013, 54.)

Riskin viestintäsuunnitelmia tulee laatia useammanlaisia. Näitä laaditaan tavallisia riskejä varten sekä kriisiviestintää varten. Erilaisia työryhmiä voidaan muodostaa riskiviestinnän laatimista varten yhteistyössä sidosryhmien kanssa. (SFS ISO/IEC 27005 2013, 56.)

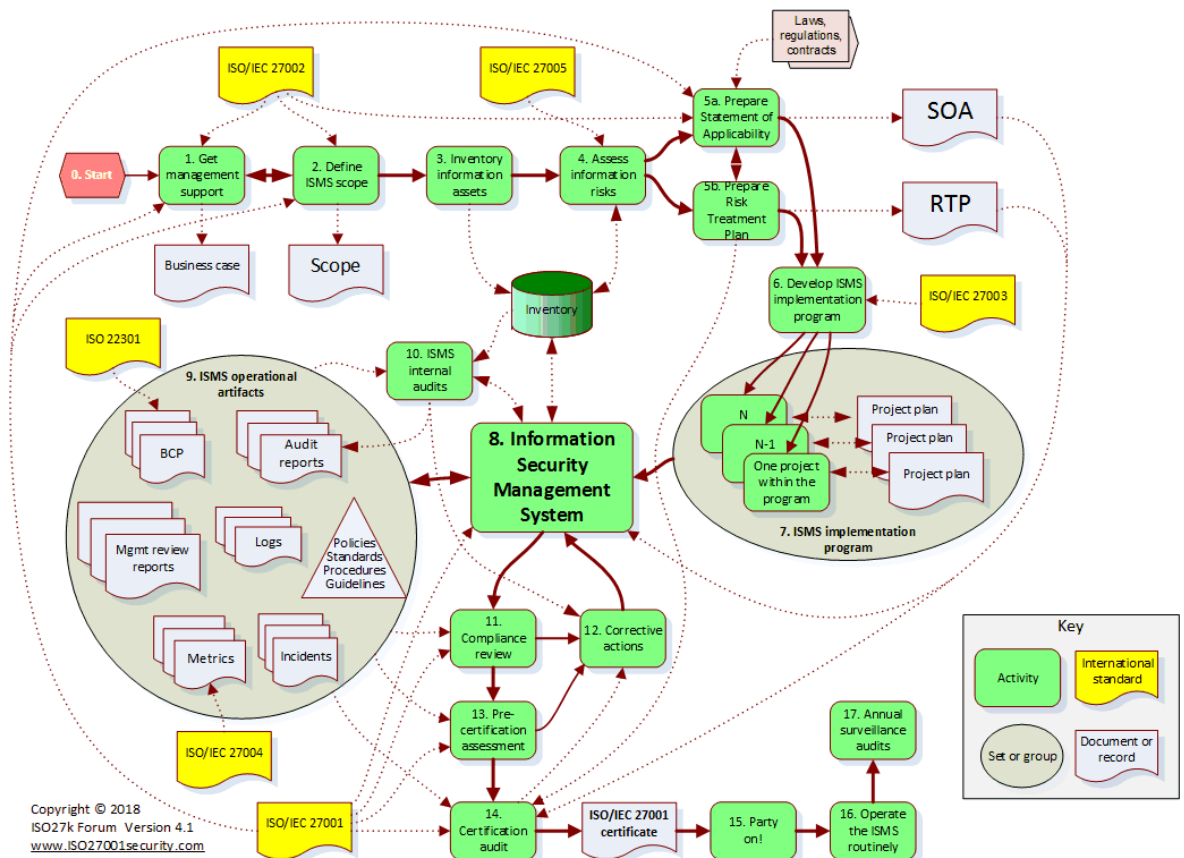
2.8.11 Tietoturvariskien seuranta

Riskit ja niiden osatekijät muuttuvat ajan kuluessa. Riskien seurannalla pyritään pitämään riskienhallinta ajan tasalla. Se voidaan suorittaa seuraamalla muutoksia ja tietoturvahäiriöitä. Riskejä tulee seurata sekä erikseen että yhdessä kertymävaikutuksen vuoksi. Riskit yleensä vaikuttavat muihin riskeihin ja niiden yhteisvaikutus tulee arvioida. Riskien seurannan tulee olla jatkuva prosessi. (SFS ISO/IEC 27005 2013, 56.)

Riskienhallintaa tulee seurata sekä parantaa. Tällä varmistutaan, että se on varmasti vaikuttavaa. Kaikista siihen tehdyistä muutoksista tulee tiedottaa kaikille osapuolille, joiden tulee tietää niistä. Riskienhallinnan kriteerejä tulee katselmoida säännöllisesti ja muuttaa tarpeen vaatiessa. Organisaatioiden tulee varmistaa tarpeellisten resurssien jatkuva saatavuus riskienhallintaa varten. (SFS ISO/IEC 27005 2013, 58.)

3 TUTKIMUSMENETELMÄT

Työ aloitettiin perehtymällä standardisarjaan SFS-EN ISO/IEC 27000. Standardista saatiin selville, mitä tulee tehdä ja miten. Standardista SFS-EN ISO/IEC 27000 saatiin selville tietoturvan hallinnan eri osat ja tämän avulla määritettiin lähtökohta työlle.



Kuvio 1. Tietoturvallisuuden hallintajärjestelmä kokonaisuus. (Salah & Hinson, [viitattu 8.4.2019].)

Kuviosta 1 nähdään TTHJ:n käyttöönotto ja operointi. Työ ei edennyt kuvion mukaisessa järjestyksessä, koska yhtiöllä oli jo valmiiksi standardisoimaton TTHJ ja koska työ rajattiin standardeihin 27000-27005. Kuviota käytettiin apuna järjestelmällisessä standardisoinnissa. Samalla käytiin läpi, että kaikki oleelliset asiat oli sisällytetty nykyiseen hallintajärjestelmään.

Yhtiön tietoturva-ympäristöstä löytyi nykyinen hallintajärjestelmä. Tietoturva-ympäristöön luotiin standardin mukaiset hallintajärjestelmäpohjat. Pohjien luonti aloitettiin soveltuvuuslausunnosta, jolloin saatiin selville mitä kaikkia standardin mukaisia ja

standardisoimattomia hallintakeinoja yhtiöllä oli käytössä. Standardien mukaiset tietoturvariskien hallintapohjat luotiin seuraavaksi. Samalla käytiin läpi ja standardisointiin riskienhallinnan peruskriteerit.

4 TULOKSET JA TULOSTEN TARKASTELU

Yhtiön tietoturvan riskienhallinnanohjeistus kirjoitettiin standardien mukaiseksi. Samalla standardisoitiin riskienhallintajärjestelmän dokumentointipohjat. Nämä tehtiin standardin SFS-ISO/IEC 27005 ohjeistamalla tavalla. Samalla standardisointiin muitakin tietoturvallisuuden riskienhallintaan liittyviä ohjeistuksia ja dokumentteja standardisarjan perusteella.

Standardisoinnin tuloksena syntyi aluksi 34 dokumentointipohjaa. Näitä pohjia myöhemmin muutettiin ja yhdistettiin yhtiölle sopiviksi. Ensimmäiset versiot dokumentointipohjista olivat kankeita käyttää, joten muutoksilla haettiin myös virtaviivaisuutta niiden käyttöön. Ohjeistuksia syntyi yhteensä 7 kappaletta tietoturvallisuuden riskienhallintaa varten. Ohjeistuksia ja dokumentointipohjia tulee jatkuvasti parantaa ja tämä voi vaikuttaa niiden määrään.

4.1 Ohjeistukset

Standardi SFS-ISO/IEC 27005 sisältää ohjeet organisaatioiden tietoturvan riskienhallinnan luomiseksi. Sen pohjalta luotiin standardisoitu ohjeistus yhtiön riskienhallintajärjestelmälle. Standardi ohjeistaa luomaan vähintään ohjeistukset tietoturvariskien

- hallintaprosessille
- toimintaympäristölle
- arvioinnille
- käsittelylle
- hyväksymiselle
- viestinnälle
- seurannalle.

Yhtiön tietoturvariskien ohjeistukset standardisointiin aluksi näiksi kokonaisuuksiksi. Standardisoituja ohjeistuksia muutettiin yhtiön haluamalla tavalla. Salassapitosopimuksen vuoksi ohjeistuksien muutoksia ei käsitellä tässä julkisessa dokumentissa.

4.2 Dokumentointipohjat

Standardi SFS-ISO/IEC 27005 ohjeistaa luomaan luetteloita ja raportteja. Raportteihin dokumentoidaan luetteloiden mahdollisia rajauksia, lähtötietoja jne. Standardin mukaan luetteloita ja/tai raportteja tulee olla

- arvioiduista riskeistä
- suojattavista kohteista
- suojattavien kohteiden omistajista
- suojattaviin kohteisiin liittyvistä liiketoimintaprosesseista
- uhista
- soveltuvuus lausunnosta
- haavoittuvuuksista
- haavoittuvuuksista, jotka eivät liity tunnistettuihin uhkiin
- tietoturvahäiriöskenaarioista
- tietoturvahäiriöskenaarioiden seurauksista
- tietoturvahäiriöskenaarioiden todennäköisyyksistä
- riskeistä
- riskien arvioinnista
- riskienkäsittelysuunnitelmista
- jäännösriskeistä
- hyväksytyistä riskeistä
- riskien viestintäsuunnitelmista
- riskitekijöiden seurannasta
- riskienhallinnan seurannasta.

Standardissa käsitellään myös luetteloiden sisältöjen tärkeysjärjestyksiä. Yhtiön dokumentointipohjat standardisoitiin ja muutettiin yhtiölle paremmin sopiviksi. Salasapitosopimuksen vuoksi dokumentointipohjien muutoksia ei käsitellä tässä julkisessa dokumentissa.

5 JOHTOPÄÄTÖKSET JA SUOSITUKSET

Yhtiön tietoturvan riskinhallinta on nyt valmis sisäistä auditointia varten. Sisäisen auditoinnin perusteella todennäköisesti riskinhallintaan pitää tehdä joitain muutoksia. Vaatimusstandardin SFS-EN ISO/IEC 27001 kaikki kohdat tulee tarkistaa. Tämän jälkeen yhtiön tietoturva on valmis ulkoiseen auditointiin ja sertifiointiin.

Standardisarjassa SFS-EN ISO/IEC 27000 korostetaan tietoturvan jatkuvaa parantamista. Riskien hallintajärjestelmä tulee sovittaa jatkossa jokapäiväistä toimintaa varten. Dokumentointipohjia ja ohjeistusta tulee jatkuvasti parantaa muutosten tapahtuessa. Ajantasaisella tietoturvallisuuden hallintajärjestelmällä pystytään takaamaan tavoiteltu tietoturvallisuustaso.

6 YHTEENVETO

Työssä keskityttiin enimmäkseen tietoturvallisuudenriskin hallintaan. Työssä käytiin läpi standardien SFS-EN ISO/IEC 27000-27005 mukaisten ohjeistuksien ja pohjien standardisointia. Yhtiön tietoturvallisuutta pyrittiin valmistelevaan sisäistä auditointia varten, joka suoritetaan ennen ulkoista auditointia kustannussyistä.

Työ aloitettiin perehtymällä standardisarjaan SFS-EN ISO/IEC 27000. Niistä saatiin selville tietoturvan hallinnan eri osat ja tämän avulla määritettiin lähtökohta työlle. Yhtiön tietoturvan riskienhallinnanohjeistus kirjoitettiin standardien mukaiseksi. Dokumentointipohjien standardisointi aloitettiin soveltuvuuslausunnosta. Tämän avulla saatiin selville, mitä kaikkia standardin mukaisia ja standardisoimattomia hallintakeinoja yhtiöllä oli käytössä. Tietoturvan riskienhallinnanohjeistus tehtiin standardin SFS-ISO/IEC 27005 mukaisella tavalla. Ohjeistuksia ja dokumenttipohjia muutettiin yhtiön haluamalla tavalla. Salassapitosopimuksen vuoksi muutoksia ei käsitellä tässä julkisessa dokumentissa.

Yhtiön tietoturvan riskienhallinta on nyt valmis sisäistä auditointia varten. Sisäisen auditoinnin perusteella todennäköisesti riskinhallintaan pitää tehdä joitain muutoksia. Vaatimusstandardin SFS-EN ISO/IEC 27001 kaikki kohdat tulee tarkistaa. Tämän jälkeen yhtiön tietoturva on valmis ulkoiseen auditointiin ja sertifiointiin.

Dokumentointipohjia ja ohjeistusta tulee jatkuvasti parantaa muutosten tapahtuessa. Ajantasaisella tietoturvallisuuden hallintajärjestelmällä pystytään takamaan tavoiteltu tietoturvallisuustaso.

Opinnäytetyön seurauksena saavutettiin läpinäkyvyys, joka mahdollistaa tietoturvan seurannan ja mittaroinin. Standardisoinnin ansiosta yhtiö on nyt paremmin valmistautunut ulkoiseen auditointiin ja SFS-EN ISO/IEC 27001 sertifiointiin.

LÄHTEET

Developing International Standards. 2019. [Verkkosivu]. Switzerland, Geneva: International Electrotechnical Commission (IEC). [Viitattu 8.2.2019]. Saatavana: <https://www.iec.ch/about/activities/standards.htm>

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

Humphreys, E. 2016. Implementing the ISO/IEC 27001 ISMS Standard. 2. uud. p. [Verkkokirja]. Norwood: Artech House. [Viitattu 8.4.2019]. Saatavana: Ebsco eBook Collection-palvelusta. Vaatii käyttöoikeuden.

Salah, O & Hinson, G. ISMS implementation and certification process flowchart v4.1. [Verkkosivu]. [Viitattu 8.4.2019]. Saatavana: <https://iso27001security.com/ISO27k-ISMS-implementation-and-certification-process-4v1.gif>

SFS-EN ISO/IEC 27000. 2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Helsinki: Suomen Standardoimisliitto. Saatavana SFS Online -palvelusta. Vaatii käyttöoikeuden.

SFS-EN ISO/IEC 27001. 2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardoimisliitto. Saatavana SFS Online -palvelusta. Vaatii käyttöoikeuden.

SFS-EN ISO/IEC 27002. 2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Helsinki: Suomen Standardoimisliitto. Saatavana SFS Online -palvelusta. Vaatii käyttöoikeuden.

SFS ISO/IEC 27003. 2017. Information technology. Security techniques. Information security management systems. Guidance. 2. uud. p. Helsinki: Suomen Standardoimisliitto. Saatavana SFS Online -palvelusta. Vaatii käyttöoikeuden.

SFS ISO/IEC 27004. 2016. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Seuranta, mittaus, analysointi ja arviointi. 2. uud. p. Helsinki: Suomen Standardoimisliitto. Saatavana SFS Online -palvelusta. Vaatii käyttöoikeuden.

SFS ISO/IEC 27005. 2013. Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta. 2. uud. p. Helsinki: Suomen Standardoimisliitto. Saatavana SFS Online -palvelusta. Vaatii käyttöoikeuden.

SFS-EN ISO/IEC 17021-1. 2015. [Verkkosivu]. Helsinki: Suomen Standardoimisliitto. [Viitattu 12.4.2019]. Saatavana: <https://sales.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/1/584068.html.stx>

SFS-ISO/IEC 20000-1. 2018. [Verkkosivu]. Helsinki: Suomen Standardoimisliitto. [Viitattu 12.4.2019]. Saatavana: <https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/727723.html.stx>

Standardit tutuksi. 2019. [Verkkosivu]. Helsinki: Suomen Standardoimisliitto. [Viitattu 8.2.2019]. Saatavana: https://www.sfs.fi/julkaisut_ja_palvelut/standardi_tutuksi