Informaatioteknologian tiedekunnan julkaisuja
No. 55/2018

Jouni Pöyhönen

Standardit, ohjeet ja suositukset osana teollisuusorganisaatioiden kyberturvallisuuden hallintaa

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 55/2018

Editor: Pekka Neittaanmäki
Covers: Petri Vähäkainu ja Matti Savonen

ISBN 978-951-39-7541-8 (verkkoj.)
ISSN 2323-5004

Jyväskylä 2018

Standardit, ohjeet ja suositukset osana teollisuusorganisaatioiden kyberturvallisuuden hallintaa

Standards, instructions and recommendations as part of the keywork instructions and recommendations as part of the keywork management of industrial organizations

Jyväskylän yliopisto
Informaatioteknologian tiedekunta
Tietotekniikan laitos

CIRP-raportti
2.painos
2017

Jouni Pöyhönen

JYVÄSKYLÄN YLIOPISTO

TIIVISTELMÄ

Standardisointi mahdollistaa organisaatiossa yhteisten toimintatapojen hakemisen. Se helpottaa myös organisaation toimintaa sen keskeisten sidosryhmien, kuten viranomaisten, muun elinkeinoelämän ja kuluttajien kanssa. Lisäksi standardisoinnilla edistetään tuotteiden yhteensopivuutta ja turvallisuutta, suojellaan kuluttajaa ja ympäristöä sekä helpotetaan kotimaista ja kansainväistä kauppaa.

Tämä raportti on katsaus standardeihin, ohjeisiin ja suosituksiin, joiden koetaan olevan hyödyllisiä teollisuusyrityksen toiminnassa sen automaatiojärjestelmien (ICS-järjestelmä) kyberturvallisuuden näkökulmasta katsottuna. Katsauksessa pääpaino on dokumenteissa, jotka hyödyntävät teollisuusyrityksen toiminnan kehittämistä verkottuneessa kybertoimintaympäristössä. Raportin keskeinen merkitys ja käyttötarkoitus muodostuvat lyhyistä katsauksista edellä mainituista näkökulmista valittujen dokumenttien sisältöön. Tavoitteena on antaa niistä lukijalle johdantomainen kuvaus luoden pohjan jatkotarkastelun tarpeisiin.

Avainsanat: ICS-järjestelmä, kyberturvallisuus, standardi, ohje, suositus

TAULUKOT

TAULUKKO 1. ICS-alueen standardeja 4
TAULUKKO 2. Suojattavan tiedon attribuutit ja niihin liittyvien uhkien vaikutusluokat 9

KUVIOT

KUVIO 1. Kyberturvallisuutta edistävä verkottunut toimintaympäristö 3
KUVIO 2. ISA-perheen standardien kehityskaaret 6
KUVIO 3. ICS-toimintaympäristön kyberturvallisuuden hallintaan liittyviä keskeisiä standardeja, ohjeita ja suosituksia 7
KUVIO 4. ISO27000-standardin viitekehys 14
KUVIO 5. NIST 800-52 ohjeen sisältö 17
KUVIO 6. Tietoturvariskien hallintaprosessi 18
KUVIO 7. Riskien käsittelytoiminta 19
KUVIO 8. Kyberturvallisuuden riskien hallinta ja tuotteen elinkaaren vaiheet 20
KUVIO 9. Kyberturvallisuuden riskien hallinta ja tuotteen elinkaaren vaiheet yleisellä tasolla 21
KUVIO 10. Organisaation riskien hallinnan prosessi 22
KUVIO 11. Organisaation riskien arviointi osana riskien hallinnan prosessin toteutusta 25
KUVIO 12. Organisaation riskikehyksen peruskomponentit 26
KUVIO 13. Organisaation riskikehyksen tasot 28
KUVIO 14. Järjestelmäsuunnittelun prosessit ja järjestelmien elinkaaret 39
KUVIO 15. Informaatioturvallisuuden arvioinnin kolme pääperiaatetta 40

SISÄLLYSLUETTELO

1. Johdanto 1
2. Kyberturvallisuuden hallinta ja elinkaari 4
3. Kyberturvallisuuden hallintaan liittyviä suosituksia ja standardeja 7
3.1 Kyberturvallisuuden perustermistö 8
3.2 Minimivaatimukset turvallisuudelle 10
3.3 Informaatioturvallisuuden hallinta 13
3.4 Teollisuusautomaation kyberturvallisuus 15
3.5 Riskien hallinta 18
3.6 Turvallisuustekniikat 30
3.7 Muu ohjeisto 34
Lähteet 42

1. Johdanto

Standardi tai normi on organisaation esittämä määritelmä siitä, miten jokin asia tulisi tehdä. Standardeja ja normeja käyttävät niin eri toimialojen laitevalmistajat ja palveluntarjoajat kuin julkisen sektorin toimijat ja tutkimuslaitokset, omista lähtökohdistaan ja globaalissa toimintaympäristössä toimiessaan. Siksi standardeja on vuosikymmenien saatossa kertynyt useisiin eri tarkoituksiin huomattava määrä. Merkittävimmät kansainväliset standardisoimisjärjestöt ovat yleinen kansainvälinen standardisointiorganisaatio ISO (International Organization for Standardization), sähkötekniikkaan ja elektroniikkaan erikoistunut IEC (International Electrotechnical Commission), saksalainen yleisiä keskieurooppalaisia teollisuustavaroiden valmistusta koskeva standardi DIN (Deutsches Institut für Normung), EEC- ja EFTA-maiden perustama eurooppalainen CEN (Comité Européen de Normalisation), eurooppalainen sähköalan standardisoimisjärjestö Cenelec (European Committee For Electrotechnical Standardization), ja eurooppalainen telealan standardisoimisjärjestö ETSI (European Telecommunications Standards Institute). Tietotekniikan alalla ISO ja IEC ovat muodostaneet yhteisen komitean alan standardien kehittämiseksi.

Kansalliset standardointijärjestöt laativat kansallisia standardeja ja osallistuvat kansainvälisten standardien laadintaan. Suomen kansallinen toimija tällä alueella on Suomen standardisoimisliitto ry (SFS). Suomessa on hajautettu standardisointijärjestelmä, jossa SFS toimii keskusjärjestönä ja laatii standardit yhdessä toimialayhteisöjensä kanssa.

SFS toteaa standardien tarkoituksesta seuraavaa: *Standardisointi on yhteisten toimintatapojen laatimista. Sen tarkoitus on helpottaa viranomaisten, elinkeinoelämän ja kuluttajien elämää. Standardisoinnilla lisätään tuotteiden yhteensopivuutta ja turvallisuutta, suojellaan kuluttajaa ja ympäristöä sekä helpotetaan kotimaista ja kansainväistä kauppaa.* (Suomen Standardisoimisliitto SFS ry.)

Usein standardeihin viitataan Euroopan unionin säädöksissä, jotka ovat asetuksia, direktiivejä tai päätöksiä. Asetukset tulevat sellaisenaan voimaan kaikissa EU-maissa, kun direktiivit voidaan puolestaan saattaa voimaan jokaisessa jäsenmaassa parhaaksi katsomalla tavalla. Päätökset koskevat niitä yrityksiä tai jäsenmaita, joille ne on osoitettu. Lisäksi standardit on mainittu myös lukuisissa EU:n asiakirjoissa kuten tiedonannoissa ja päätöslauselmissa. Ne eivät ole kuitenkaan juridisesti sitovia asiakirjoja. (Suomen Standardisoimisliitto SFS ry.)

EU:n uuden lähestymistavan (New Approach) mukaisesti laadittavat direktiivit sisältävät vain tuotteiden olennaisesti terveyttä, turvallisuutta, kuluttajansuojelua ja ympäristöä koskevia vaatimuksia sekä vaatimustenmukaisuuden osoittamisen vaihtoehtoja. Tämän johdosta tekniset yksityiskohdat, spesifikaatiot, joita tarvitaan tuotettaessa ja markkinoitaessa direktiivien mukaisia tuotteita, esitetään Euroopassa niin sanotuissa yhdenmukaistetuissa standardeissa yksittäisten standardien sijaan. Ne ovat eurooppalaisia standardeja, jotka on laadittu Euroopan komission ja/tai EFTA:n toimeksiannosta. Niiden viitetiedot on julkaistu EU:n virallisessa lehdessä. Vanhoissa

direktiiveissä ja kansallisissa säädöksissä sen sijaan viitataan edelleen lukuisiin yksittäisiin eurooppalaisiin standardeihin. Viittauksella standardi voidaan tehdä pakolliseksi tai sitä voidaan pitää esimerkkinä säädöksen vaatimukset täyttävästä ratkaisusta. (Suomen Standardisoimisliitto SFS ry.)

Tekniset spesifikaatiot eivät kuitenkaan ole pakollisia, vaan niillä on vapaaehtoisen standardin status. Kansallisten viranomaisten on kuitenkin tunnustettava, että tuotteet, jotka on valmistettu yhdenmukaistettujen standardien mukaisesti, täyttävät direktiiveissä olevat turvallisuusvaatimukset. Tällaiset tuotteet saavat siten vapaasti liikkua yli kansallisten rajojen. Kansallisissa säädöksissä myös voidaan viitata standardeihin.

Tuotteita voidaan valmistaa myös standardeista poiketen, koska standardit ovat vapaaehtoisia. Tällöin kuitenkin valmistajalla on velvollisuus osoittaa jollain muulla tavoin, että hänen tuotteensa täyttävät direktiivien olennaiset vaatimukset.

Tuotteet, joita uuden lähestymistavan direktiivit koskevat varustetaan CE-merkinnällä. Uuden lähestymistavan direktiivejä on runsaat 20 kappaletta. CE-merkintä on käytössä muun muassa sähkölaitteissa ja muissa koneissa, lääkinnällisissä laitteissa, leluissa, painelaitteissa, henkilönsuojaimissa sekä radio- ja telepäätelaitteissa. (Suomen Standardisoimisliitto SFS ry.)

Kansainvälinen standardisointi organisaatio ISO (International Organization for Standardization) määrittelee standardisoinnin yleiset edut seuraavasti: *“International Standards bring technological, economic and societal benefits. They help to harmonize technical specifications of products and services making industry more efficient and breaking down barriers to international trade. Conformity to International Standards helps reassure consumers that products are safe, efficient and good for the environment.”* (International Organization for Standardization.)

Tavoitteena on vapauttaa kauppaa paitsi poistamalla tulleja, myös karsimalla tarpeetonta sääntelyä, purkamalla investointeihin liittyviä rajoituksia sekä yhdenmukaistamalla käytäntöjä. Suurimmat hyödyt olisivat saatavilla sääntelyn alueella lainsäädäntöä, teknisiä määräyksiä ja standardeja harmonisoimalla tai muutoin yhteen sovittamalla.

Yhdysvalloissa standardien käyttö on yhteisten toimintatapojen noudattamista organisaatioissa sekä niiden välillä ja nämä toimintatavat ovat hyvin yleisiä. Ilmeisesti myös siksi standardit ja erilaiset ohjeet ja suositukset ovat usein maksuttomia.

Ohjeiden ja suositusten tavoitteet liittyvät yleensä toiminnan kehittämiseen. Kybermaailmassa ne avustavat käyttäjäänsä parantaen organisaation toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. Tällöin toiminnot saattavat olla esimerkiksi kyberturvallisuuden johtamisen ja hallinnoinnin tai teknillistä tietojärjestelmien, tietoverkkojen ja ICT-palvelujen kehittämistä, ylläpitoa tai käyttöä.

Huoltovarmuuskeskus on laatinut kyberturvallisuussuosituksia tavoitteena kannustaa ja helpottaa elinkeinoelämän yrityksiä sekä julkishallinnon organisaatioita kehittämään toimintaedellytystensä parantamista ja tuotannontekijöiden varmistamista kyberturvallisuuteen panostamalla. Suosituksissa painotetaan normien käyttö yhtenä perustyökaluna haettaessa organisaatioihin nykyistä parempaa turvallisuustasoa. Organisaatioiden kyberturvallisuus voidaan esittää verkottuneesta toimintaympäristöstä koostuvana viitekehyksenä, jonka yhtenä perusosana ovat normit (KUVIO 1).

KUVIO 1. Kyberturvallisuutta edistävä verkottunut toimintaympäristö (Lehto, Limnéll, Innola, Pöyhönen, Rusi & Salminen, 2017, 41)

Standardit ja usein myös ohjeet ja suositukset ovat osana organisaatioiden vaatimustenmukaisuuden hallintaa. Organisaatioilta voidaan lakien noudattamisen lisäksi edellyttää niitä erilaisissa sopimuksissa, jotka ovat peräisin edellä mainituista lähteistä. Vaatimustenmukaisuuden hallintaan kuuluvat vaatimusten tunnistamisen lisäksi toiminnan nykytilan arvioiminen, sen riskien tunnistaminen ja toimintaa ehkäisevien ja korjaavien toimenpiteiden prosessit. Monissa tapauksissa organisaation kannattaa asettaa vaatimuksia myös omille alihankkijoilleen ja yhteistyökumppaneilleen. (Suomen Standardisoimisliitto SFS ry.)

Tämä raportti on katsaus standardeihin, ohjeisiin ja suosituksiin, joiden voidaan ajatella olevan hyödyllisiä teollisuusyrityksen kyberturvallisuuden osalta. Katsauksessa pääpaino on dokumenteissa, jotka erityisesti auttavat teollisuusyritysten toiminnan kehittämisessä verkottuneessa kybertoimintaympäristössä. Raportti pitää sisällään lyhyen katsauksen hyödyllisiin dokumentteihin ja tavoitteena on antaa niistä johdantomainen kuvaus jatkotarkastelutarpeen pohjaksi. Jokainen raportissa mainittu asiakirja on toiminut katsauksen lähteenä.

2. Kyberturvallisuuden hallinta ja elinkaari

Julkaisu “A survey of cyber security management in industrial control systems” (Knowles, Prince, Hutchison, Ferdinand, Disso, Jones, 2015) käsittelee laajasti ICS-alueen standardeja. Ne ovat pääosin vapaasti saatavilla olevia yhdysvaltalaisia kansallisia standardeja tai suosituksia ja ovat siten käyttökelpoisia kehitettäessä muun muassa teollisuusautomaatiojärjestelmien kyberturvallisuuden hallintaa niiden elinkaaren eri vaiheissa. Taulukko 1 on osa julkaisua ja siitä ilmenee edellä mainitut standardit.

Information security publications by industry and country.			
Industry	Country	Publication	Paid or public
Cross-industry	International	ISO/IEC27000 Series	Paid
	United States	DoDDirective8500.1: Information Assurance	Public
		DoD Instruction8500.2: Information Assurance Implementation	Public
		DoD Instruction8510.01:DIACAP	Public
		FIPS 199	Public
		FIPS 200	Public
		NIST 800 Series	Public

TAULUKKO 1. ICS-alueen standardeja (Knowles ym., 2015, 60)

Taulukossa esiintyvän ISO/IEC 27000-perheen tärkeimmiksi kotimaisten organisaatioiden kyberturvallisuuden hallinnan apuvälineiksi voidaan nähdä kuuluvan alastandardit, joissa kuvataan tietoturvallisuuden hallintajärjestelmän vaatimukset (27001:2005) ja riskienhallinnan toteutus (27005:2011). Lisäksi tärkeä alastandardi ICS:n osalta on ISO/IEC27019:2013, joka sisältää suhteellisen uudet ohjeet ja suositukset energia-alan sovellusten kyberturvallisuudesta.

Edellä mainitussa julkaisussa on todettu ISO/IEC 27000- standardisarjan tietoturvallisuuden hallintaa koskevan menettelyohjeen ISO/IEC27002 olevan laajimmin käytetty standardi ICS-järjestelmien operoinnissa, vaikka tarjolla on myös ICS-specifisiä standardeja (Knowles ym., 2015, 58).

Huoltovarmuuskeskuksen, VTT:n ja teollisuuden kyberturvallisuuden KYBER-TEO-tutkimushankkeen eräässä yrityskohtaisessa case-tutkimuksessa on kehitetty toimenpiteitä tietoturvan ohjeistamiseksi yrityksen automaatiojärjestelmän hankintaa varten. Siinä on referensseinä käytetty muun muassa seuraavia standardeja tai standardin luontoisia julkaisuja (selityksineen): (Huoltovarmuuskeskus, 2015, 13 - 14).

- Department of Homeland Security: Cyber Security Procurement Language for Control Systems (julkinen)
- IEC-61511: Turva-automaation tietoturvan riskianalyysi
- ISA/IEC 62443-sarjassa tietoturvariskien identifiointi ja analysointi
- ISA-62443-1-1 & 1-2: Termit, lyhenteet, käsitteet, mallit
- ISA-62443-2-1: Tietoturvaohjelman perustaminen
- ISA-62443-2-4: Vaatimukset ICS-järjestelmätoimittajille
- ISA-62443-3-1: Tietoturvateknologiat
- ISA-TR84.00.09-2013 Security Countermeasures Related to Safety Instrumented Systems (SIS)
- ISO/IEC 27001: Hallintavaatimukset
- ISO/IEC 27002: Hallinnan menettelyohjeet
- NIST 800-sarja: Erilaisia kyberturvallisuuden erityisjulkaisuja (julkisia)
- SFS Käsikirja 631-3: Automaatio. Osa 3: Tietoturvallisuus
- WIB: Process Control Domain - Security Requirements for Vendors

SFS-käsikirjaan 631-3 vuodelta 2013 on koottu joukko automaatiojärjestelmien tietoturvallisuuden parantamiseen pyrkiviä standardijulkaisuja. Mukana ovat suomennokset standardisarjojen IEC 62443 ja ISO/IEC 27000 keskeisistä osista. Niissä kuvatun järjestelmällisen lähestymistavan avulla saadaan monimutkaisenkin automaatiojärjestelmän tietoturvallisuus hallintaan. The International Society of Automation (ISA) vuodelta 2007 julkaisemat standardit ovat eri vaiheiden jälkeen päivittyneet nykyiseen muotoonsa. Kuviosta 2 selviää niiden kehityskulku. (Suomen Standardisoimisliitto SFS ry, 2013, 9 - 10.)

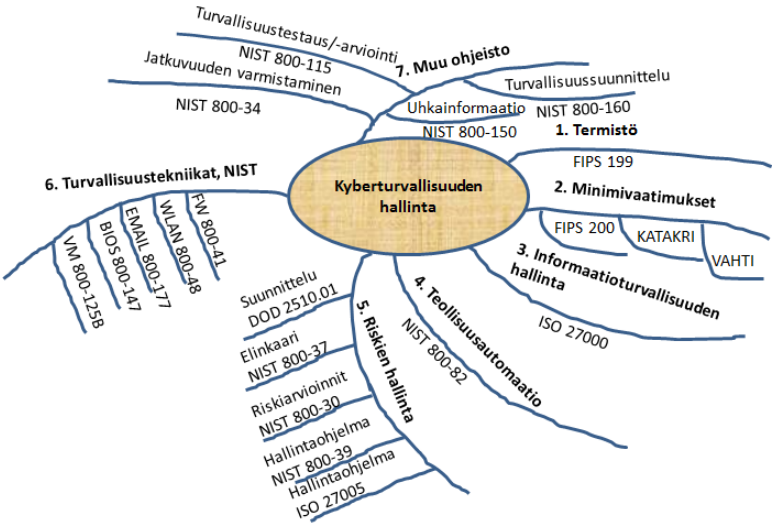
Restructuring of ISA99 Standards

Work Group	Content Description	Previous ISA Number	Year	Revised ISA Number	Currently-approved IEC number	Proposed IEC Renumbering
WG1	Technical report on security technologies	ISA–TR99.00.01	2007	ISA–99.01.02	IEC/TR 62443–5	IEC/TR 62443–1–2
WG3	Terminology, Concepts, and Models	ISA–99.00.01	2007	ISA–99.01.01	IEC/TS 62443–1	IEC 62443–1–1
WG2	Establishing an Industrial Automation and Control Systems Security Program	ISA–99.00.02	2008 (Est)	ISA–99.02.01	IEC 62443–2	IEC 62443–2–1
TBD	Operating an Industrial Automation and Control Systems Security Program	ISA–99.00.03	TBD	ISA–99.02.02	IEC 62443–3	IEC 62443–2–2
WG4	Technical Security Requirements for Industrial Automation and Control Systems: Target Security Levels	part of ISA–99.00.04	TBD	ISA–99.03.01 - ISA–99.03.xx	part of IEC 62443–4	IEC 62443–3–1 - IEC 62443–3–x

KUVIO 2. ISA-perheen standardien kehityskaaret (Gilsinn, 2008, 3)

3. Kyberturvallisuuden hallintaan liittyviä suosituksia ja standardeja

Kuviossa 3 on esitetty taulukkoon 1 luetteloiduista standardista eräitä keskeisimpiä kyberturvallisuuden hallintaan liittyviä suosituksia, ohjeita ja standardeja, joiden avulla organisaatio voi kehittää ICS-toimintaympäristöönsä liittyviä hallinnollisia ja teknillisiä kykyjään toimintansa parantamiseksi kyberympäristöissä toimintaa varten. Lisäksi kuva sisältää merkittävimmät kansalliset KATAKRI- ja VAHTI-ohjeet. Tässä raportissa on lyhyet kuvaukset kuvassa esiintyvistä dokumenteista.



KUVIO 3. ICS-toimintaympäristön kyberturvallisuuden hallintaan liittyviä keskeisiä standardeja, ohjeita ja suosituksia

3.1 Kyberturvallisuuden perustermistö

Kyberturvallisuuden luokitteluun liittyvistä perustermistä on julkaistu oheinen standardi, jonka mukaan yhdysvaltalaisissa hallinnon IT-verkoissa, -järjestelmissä ja –tiedoissa toimitaan. Sen sisältö vastaa yleisesti alalla käytettyä termistöä, joten standardia on yleiskäyttöinen ja sopii sovellettavaksi vastaavaan tarkoitukseen myös muualla.

Federal Information Processing Standards, FIPS PUB 199 (2004)
Standards for Security Categorization of Federal Information and Information Systems

Standardi tiedon luokittelemiseksi ja suojaamiseksi siihen liittyvien attribuuttien mukaan jaoteltuna tarkoittaa seuraavaa:

- Standardia voidaan käyttää tiedon ja tietojärjestelmien luokitteluun määritettäessä niiden riskitasoja. Luokittelu on ensimmäinen askel riskienhallinnan prosessissa.
- Tieto tai tietojärjestelmä voidaan sisällyttää eri riskitasoille kunkin suojattavan attribuutin mukaan.
- Ohje sisältää tietoturvallisuuden minimivaatimukset jokaisessa attribuuttiluokassa.

Suojattavan tiedon kolme attribuuttia ovat:

- TIEDON LUOTETTAVUUS (CONFIDENTIALITY)
- TIEDON EHEYS (INTEGRITY)
- TIEDON SAATAVUUS (AVAILABILITY)

Oheisessa taulukko 2:ssa on attribuutit ja niihin kohdistuvat uhkavaikutukset kuvattu sanallisesti. (Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, 2004, 6)

TURVALLISUUSTASO	MATALATASO	KESKITASO	KORKEATASO
Luottamuksellisuus Sisältää rajoituksia tietojen saantiin ja tietojen paljastumiseen. Mukaan lukien keinot yksityisyyden ja omistusoikeuden suojaamiseksi.	Tietojen luvattomalla paljastumisella voidaan olettaa olevan **rajallisen kielteinen vaikutus** organisaation toimintaan, varallisuuteen tai yksilöihin.	Tietojen luvattomalla paljastamisella voidaan olettaa olevan **vakava haitallinen vaikutus** organisaation toimintaan, varallisuuteen tai yksilöihin.	Tietojen luvattomalla paljastamisella voidaan olettaa olevan **vakava tai katastrofaalisen haitallinen** vaikutus organisaation toimintaan, varallisuuteen tai yksilöihin.
Eheys Informaation muuttamisen tai tuhoamisen estäminen. Informaation aitouden varmistaminen.	Tietojen luvattomalla muokkauksella tai tuhoamisella voidaan olettaa olevan **rajallisen kielteinen vaikutu**s organisaation toimintaan, varallisuuteen tai yksilöihin.	Tietojen luvattomalla muokkauksella tai tuhoamisella voidaan olettaa olevan **vakava haitallinen vaikutus** organisaation toimintaan, varallisuuteen tai yksilöihin.	Tietojen luvattomalla muokkauksella tai tuhoamisella voidaan olettaa olevan **vakava tai katastrofaalisen kielteinen** vaikutus organisaation toimintaan, varallisuuteen tai yksilöihin.
Saatavuus Ajankohtaisen ja luotettavan tiedonsaannin ja käytön varmistus.	Tietojen tai tietojärjestelmän käytöllä tai käyttötietojen häiriintymisellä odotetaan olevan **rajallisesti haitallisia vaikutuksia** organisaation toimintaan, varallisuuteen tai yksilöihin.	Tietojen tai tietojärjestelmän käyttöoikeuksien katoamisella tai käytön estymisellä voi odottaa olevan **vakava kielteinen vaikutus** organisaation toimintaan, varallisuuteen tai yksilöihin.	Tietojen tai tietojärjestelmän käytön tai käytön katoamisella voi odottaa olevan **vakava tai katastrofaalisen kielteinen** vaikutus organisaation toimintaan, varallisuuteen tai yksilöihin.

TAULUKKO 2. Suojattavan tiedon attribuutit ja niihin liittyvien uhkien vaikutusluokat (Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, 2004, 6)

3.2 Minimivaatimukset turvallisuudelle

Kyberturvallisuuden turvallisuusluokittelun mukaisista minimivaatimuksista yhdysvaltalaisissa hallinnon IT-verkoissa, -järjestelmissä ja -tiedostoissa on julkaistu alla oleva standardi. Se muodostaa peruslähtökohdan kyberturvallisuusprosessien valinnoille. Sitä on mahdollista käyttää myös muualla vastaavaan tarkoitukseen.

Federal Information Processing Standards, FIPS 200 (2006)
Minimum Security Requirements for Federal Information and Information Systems

Tämä standardi edistää tietoturvallisten tietojärjestelmien kehittämistä, käyttöönottoa ja toimintaa määrittämällä tietoturvallisuuden vähimmäisvaatimukset sekä helpottamalla johdonmukaisempaa, vertailukelpoista ja toistuvaa lähestymistapaa määritettäessä tietojärjestelmien turvatarkastusten valintaa niille asetettavissa olevia minimivaatimuksia vasten. (Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, 2006, 1.)

Standardi antaa ohjeita yhdysvaltalaisen julkisen hallinnon, sen verkosto-organisaatioiden ja yksityisen sektorin yritysten, tiedon ja tietojärjestelmien turvallisuuden minimitasojen määrittämiseksi seuraavasti:

- Standardi perustuu riskitasojen mukaan määritetyille tarkoituksenmukaisille turvallisuustasoille.
- Ohjeistaa tiedon ja tietojärjestelmän sisällyttämisen jokaiseen luokitteluryhmään.
- Antaa turvallisuusluokittelun minimivaatimukset tiedolle ja tietojärjestelmälle jokaisessa luokitteluryhmässä.

Tiedon turvallisuuden luokittelussa sen luotettavuus, eheys tai saatavuus vaihtelevat tietojärjestelmästä toiseen järjestelmään asetetun turvallisuusvaatimuksen mukaisesti. Tällöin uhkan matala vaikutustaso toteutuu, kun sen tiedon jokaiseen attribuuttiin kohdistuvan uhkan vaikutus arvioidaan matalaksi. Järjestelmän keskimmäinen vaikutustaso määrittyy silloin, kun vähintään yksi sen tiedon attribuuteista arvioidaan tälle tasolle eikä yksikään attribuuteista saavuta keskimmäistä tasoa korkeampaa statusta. Korkein taso määrittyy silloin, kun yksikin sen attribuuteista arvioidaan tälle tasolle. (Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, 2006, 2 - 4.)

Ohjeessa tietoturvallisuuden minimivaatimukset edellytetään seuraavilta osa-alueilta: pääsynhallinta, tilannetietoisuus ja koulutus, tarkastustoiminta ja eri vastuut, sertifiointi, akkreditointi ja turvallisuusarvioinnit, kokoonpanonhallinta, valmiussuunnittelu, tunnistaminen ja todentaminen, tapahtumavastuut, ylläpito, laitesuojaus, fyysinen- ja ympäristösuojaus, suunnittelu, henkilöstöturvallisuus, riskiarviointi, järjestelmä- ja palveluhankinta, järjestelmä- ja laitesuojaus sekä tietoturva. (Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, 2006, 2 - 4.)

Kansallinen turvallisuusauditointikriteeristö, KATAKRI (2015)

Kriteeristön tavoitteena on yhtenäistää viranomaistoimintoja silloin, kun viranomainen toteuttaa yrityksessä tai muussa organisaatiossa kohteen turvallisuustason todentavan tarkastuksen eli turvallisuusauditoinnin. Kriteeristö toimii kansallisesti velvoittavana asiakirjana silloin, kun suomalaisten yritysten turvallisuustaso varmennetaan kansallisen turvallisuusviranomaisen toimesta kansalliseen tarpeeseen tai kansainväliseen viranomaispyyntöön pohjautuen tai yritysturvallisuustodistuksen myöntämiseen pyrkien. (Puolustusministeriö, 2015, 4.)

KATAKRI on siten viranomaisten auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. KATAKRI:a voidaan käyttää auditointityökaluna erityisesti arvioitaessa yrityksen turvallisuusjärjestelyjen toteutumista yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Sitä voidaan käyttää myös apuna yrityksien, yhteisöjen sekä viranomaisten muussa turvallisuustyössä ja työn kehittämisessä. (Puolustusministeriö, 2015, 4.)

Mikäli suomalainen yritys tarvitsee yritysturvallisuustodistuksen esimerkiksi valtionhallinnon salassa pidettävää tietoa sisältäviin hankkeisiin liittyen tai osallistuakseen kansainväliseen tarjouskilpailuun, niin toimivaltaiset viranomaiset toteuttavat yritysten turvallisuustason tarkastamisen. Vaatimukset täyttävälle yritykselle toimivaltainen viranomainen voi myöntää tästä erillisen todistuksen (kansainvälisessä yhteydessä Facility Security Clearance, FSC). Ohjeistoa sovelletaan myös alihankintaketjuun siten, kuin organisaatiolla on mahdollisuus toimeksiantonsa perusteella siirtää työtä alihankintaan. Organisaatio vastaa samojen periaatteiden mukaisesta auditoinnista alihankintayrityksissä. (Puolustusministeriö, 2015, 5.)

KATAKRI:iin kirjatut vaatimukset on jaettu kolmeen osa-alueeseen. Turvallisuusjohtamista koskevassa osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on riittävät turvallisuusjohtamisen valmiudet sekä kyvykkyys siihen. Turvallisuusjohtamisen osa-alueessa on kuvattu perustaso, jonka vaatimukset kohdeorganisaation tulee täyttää. Fyysistä turvallisuutta koskevassa osa-alueessa kuvataan salassa pidettävien tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset. Organisaation tilat voidaan salassa pidettävien tietojen käsittely- ja säilyttämistarpeen perusteella jakaa kolmeen alueeseen: hallinnollinen alue, turva-alue ja tekninen turva-alue. Teknistä tietoturvallisuutta koskevassa osa-alueessa kuvataan puolestaan tekniselle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset. Ohjeen osa-alueet on laadittu erillisiksi kokonaisuuksiksi, jolloin jokaista osa-alueita voidaan käyttää myös erikseen. (Puolustusministeriö, 2015, 3.)

Kansallinen valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä, VAHTI-ohjeet

Valtiovarainministeriön asettama Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä (VAHTI) toimii julkisen hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä. (Valtionvarainministeriö.) Sen tavoitteena on erityisesti VAHTI-ohjeiston avulla kehittää tieto- ja kyberturvallisuutta, valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. Tavoite pitää sisällään tieto- ja kyberturvallisuuden sekä ICT-varautumisen saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta sekä tietojärjestelmien, tietoverkkojen ja ICT-palvelujen kehittämistä, ylläpitoa ja käyttöä. (Valtionvarainministeriö.)

Valtionhallinnon näkökulmasta katsottuna siihen liittyy kansallista ja kansainvälistä tietoturvallisuutta kehittävien yhteistyöryhmien toiminta sekä mahdollisesti valtionhallinnolle annettavien linjausten valmistelu. Suomen kyberturvallisuusstrategian mukaisesti VAHTI käsittelee ja sovittaa yhteen valtionhallinnon keskeiset tieto- ja kyberturvallisuuden linjaukset. (Valtionvarainministeriö.)

VAHTI-ohjeita käytetään valtionhallinnon lisäksi laajasti hyväksi myös kansainvälisessä tietoturva- ja yhteistyössä, elinkeinoelämässä, yrityksissä ja kunnissa sekä opetus- ja kansalaistoiminnassa. (Valtionvarainministeriö.)

3.3 Informaatioturvallisuuden hallinta

Kansainvälinen ISO/IEC 27000- standardisarja ohjeistaa organisaatioiden informaatioturvallisuuden kokonaishallintaa. Se on laadittu malliksi hallinnan kehittämiselle, toteuttamiselle, käyttämiselle, valvonnalle, katselmoinnille, ylläpitämiselle ja parantamiselle. Standardi on maksullinen, mutta sitä on vapaasti saatavana opetusmateriaalina SFS:n verkkosivuilla. (Suomen Standardisoimisliitto SFS ry, 2015, 10.)

ISO/IEC 27000- standardisarjan koulutusmateriaalissa on todettu informaatioturvallisuuden hallintajärjestelmän tarpeesta ja luonteesta seuraavasti: (SFS 2012.)

1. Tietoturvallisuuden hallintajärjestelmä tukee eri kokoisia ja tyyppisiä organisaatioita silloin, kun ne:

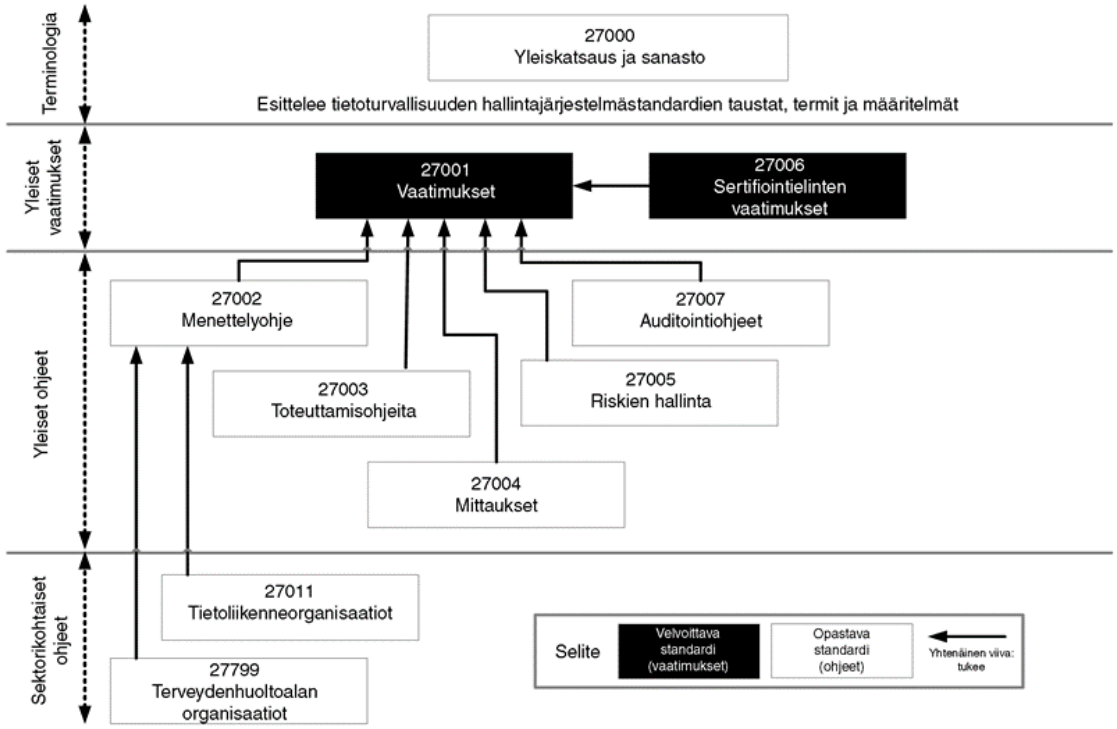
- keräävät, käsittelevät, säilyttävät ja välittävät suuria määriä informaatiota,
- pitävät informaatiota sekä siihen liittyviä prosesseja, järjestelmiä, verkkoja ja ihmisiä tärkeinä turvattavina kohteina, joiden avulla organisaation tavoitteet saavutetaan,
- kohtaavat monia erilaisia riskejä, jotka voivat vaikuttaa turvattavien kohteiden toimintaan, ja
- muokkaavat riskejä toteuttamalla tietoturvamekanismeja. (Suomen Standardisoimisliitto SFS ry, 2015, 8.)

2. Tietoturvallisuuden hallintajärjestelmää voidaan kuvata siten, että:

- se on osa yleistä hallintajärjestelmää, joka liiketoimintariskien arviointiin perustuen luodaan ja toteutetaan ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyvä tietoturvallisuus,
- se on tarkoitettu yritysjohdon tietoturvatyön organisoimiseksi ja helpottamiseksi,
- sen tulisi kattaa kaikki tietoturvan johtamisessa, hallinnoimisessa ja valvonnassa tarvittavat menettelyt ja toimenpiteet,
- se ei ole yksittäinen dokumentti, vaan moniosainen prosessi, jota on kehitettävä jatkuvasti, sen osia ovat muun muassa riskianalyysi, tietoturvapolitiikka, tietoturva-, jatkuvuus- ja toipumissuunnitelmat. (Suomen Standardisoimisliitto SFS ry, 2015, 9.)

Kuviossa 4 esitetään tietoturvallisuuden hallintajärjestelmästandardien väliset suhteet. Tietoturvallisuuden hallintajärjestelmästandardien sarja koostuu toisiinsa liittyvistä standardeista (osa vielä valmisteilla). Tietoturvallisuuden hallintajärjestelmästandardien sarja liittyy moniin muihin ISO- ja ISO/IEC -standardeihin. Standardit luokitellaan tarkemmin johonkin seuraavista tyypeistä:

- yleiskatsauksen ja termit sisältävät standardit (27000)
- vaatimuksia määrittelevät standardit (27001, 27006)
- yleisiä ohjeita antavat standardit (27002, 27003, 27004, 27005, 27007) ja
- sektorikohtaisia ohjeita antavat standardit (27011, 27799).



KUVIO 4. ISO27000-standardin viitekehys (Suomen Standardisoimisliitto SFS ry, 2015, 21)

3.4 Teollisuusautomaation kyberturvallisuus

Teollisuusautomaatiojärjestelmät (ICS-järjestelmät) toimivat fyysisen toimintaympäristön digitaalisena ohjausjärjestelmänä, kun IT-järjestelmät puolestaan hallitsevat pääosin dataa. ICS-järjestelmät pitävät sisällään huomattavia riskejä, jotka voivat toteutuessaan johtaa ihmisten terveyden vaarantumiseen, vakaviin ympäristövaurioihin, yritysten tai yhteiskunnan taloudellisiin menetyksiin. Sen vuoksi niille asetetaan käytettävyysvaatimuksia, jotka voivat poiketa huomattavasti perinteisistä IT-ratkaisuihin kohdistuvista vaatimuksista. Kyberturvallisuuden huomioiminen onkin erityisen oleellista ICS-järjestelmien kokonaisriskien hallitsemiseksi.

NIST Special Publication 800-82 Revision 2, (2015)
Guide to Industrial Control Systems (ICS) Security

Teollisuusautomaatiojärjestelmien (Industrial Control Systems, ICS) kyberturvallisuuden ohjeistamiseksi on käytettävissä NIST-ohjeperheen julkaisu 800-82 Revision 2, joka käsittelee laajasti koko tekniikka-alueen turvallisuusratkaisuja, kuten SCADA-käytönvalvontajärjestelmät (Supervisory Control and Data Acquisition Systems), hajautetut automaatiojärjestelmät (Distributed Control Systems, DCS) ja ohjelmoitavat logiikkajärjestelmät (Programmable Logic Control, PLC). Se sisältää järjestelmien tyypilliset rakenteet keskinäisine riippuvuuksineen, niiden haavoittuvuudet tyypillisine uhkineen ja suositukset toimenpiteistä uhkien aiheuttamien riskien pienentämiseksi. Julkaisu linkittää myös muita NIST-perheen ohjeita alueen turvallisuuden hallitsemiseksi. (Stouffer, Pillitteri, Lightman, Abrams & Hahn, 2015, 1.)

Ohjeen alkuosassa on myös selostettu eri teollisuusautomaatiojärjestelmien rakenteita ja esitetty niistä tyypillisimpiä esimerkkejä. Teollisuusautomaatiojärjestelmät on jaettu niiden ohjausjärjestelmien ja verkkorakenteen perusteella seuraaviin ryhmiin:

1. SCADA-käytönvalvontajärjestelmät (Supervisory Cotrol and Data Acquisition Systems)
2. Hajautetut automaatiojärjestelmät (Distributed Control Systems, DCS)
3. Ohjelmoitavat logiikkajärjestelmät (Programmable Logic Control, PLC)

Ohje painottaa riskitarkastelun tärkeyttä läpi organisaation kolmitasoisena tarkasteluna. Tasot ovat organisaatiotason tarkastelu, liiketoimintaprosessitaso ja IT-/ICS- järjestelmätasot (tietojärjestelmät). Tavoitteena tulee olla jatkuvan parantamisen periaate riskiriippuvaisissa toimenpiteissä läpi organisaatioketjun, jossa on sen ulkoisia omistajia ja sisäisiä toimijoita. Riskien arviointiprosessiin kuuluu neljä komponenttia. Ne ovat rajaaminen, arvioiminen, reagointi ja valvonta. Ne ovat keskenään riippuvuussuhteessa siten, että esimerkiksi valvonta voi johtaa muutokseen riskien rajaamisessa ja sitä kautta koko prosessiketjussa. (Stouffer ym., 2015, 2 - 4.)

Ohjeen mukainen toiminta pitää sisällään informaatioturvallisuuden kokemusten, ohjelmien ja toimintatapojen yhdistämisen ICS-järjestelmien tekniikoiden ja toimintaympäristön vaatimiin erityispiirteisiin. ICS-järjestelmiä käyttävien organisaatioiden on jatkuvasti päivitettävä turvallisuussuunnitelmiaan vastaamaan muutoksia teknologioissa, toimintatavoissa, toimintaa ohjaavissa standardeissa ja säädöksissä yhtä hyvin kuin muissakin turvavaatimuksissa. Onnistunut turvallisuusohjelman laadinta perustuu turvattavan liiketoiminnan huomioimiseen, organisaatiorajat ylittävien ohjelman laadintatiimien kokoamiseen, ICS-spesifiseen politiikkaan ja toimintatapoihin, riskienhallinnan toteuttamiseen ja henkilöstön kouluttamiseen. Henkilöstön sitouttaminen ohjelman laadintaan ja toteutukseen tulee lähteä organisaation johdosta ja sen tulee ulottua koko henkilöstöön läpi organisaation. (Stouffer ym., 2015, 2 - 4.)

ICS:n turvallisuusarkkitehtuuri on sidoksissa yrityksen yleiseen IT-arkkitehtuuriin. ICS:n kyberturvallisuuteen kohdistuu kuitenkin omia erityisvaatimuksia. Esimerkiksi yrityksen tiedonsiirron verkkoarkkitehtuuria suunniteltaessa on suositeltavaa erottaa ICS-verkko sen yleisestä verkosta - yritysverkosta. Internet, sähköposti ja muu vastaava liikenne ovat yritysverkon liikennettä, mutta ne eivät ole sallittuja ICS-verkossa. Verkkolaitteisiin, niiden konfiguraatioihin ja ohjelmistopäivityksiin kohdistuvat ICS-järjestelmissä tiukat kontrollit. Yritysverkoissa tilanne ei saata aina olla näin. Mikäli ICS-verkkoliikenne sallittaisiin yritysverkossa, niin se olisi siepattavissa tai siihen kohdistuisivat yleiset DoS- ja ”Man-in-the-Middle” hyökkäykset. Toisin sanoen verkkojen erottamisella estetään yritysverkojen turvallisuus- ja toimintaongelmien siirtymiset ICS-verkkoihin. Erottamistekniikkoina ovat palomuurit ja DNZ-tekniikan avulla suoritettava verkon segmentointi. (Stouffer ym., 2015, 2 - 4.)

Tiedonsiirtoverkon segmentointi ja erottaminen tulee perustua ICS-järjestelmien operatiivisten riskein analysointiin. Ison ICS-tiedonsiirtoverkon osittaminen myös pienempiin osaverkkoihin voi olla tarkoituksenmukaista. Tarkoituksenmukaisuus riippuu sellaisista tekijöitä, kuin hallinnan valtuutuksista, luottamustekijöistä, toiminnan kriittisyydestä (Stouffer ym., 2015, 4) ja siirrettävän liikenteen määrästä erotettuun verkkoon. Nämä tietoverkkoon kohdistettavat toimenpiteet ovat organisaation näkökulmasta katsottuna kaikista tehokkaimpia ICS:n suojaustoimenpiteitä kyberuhkia vastaan.

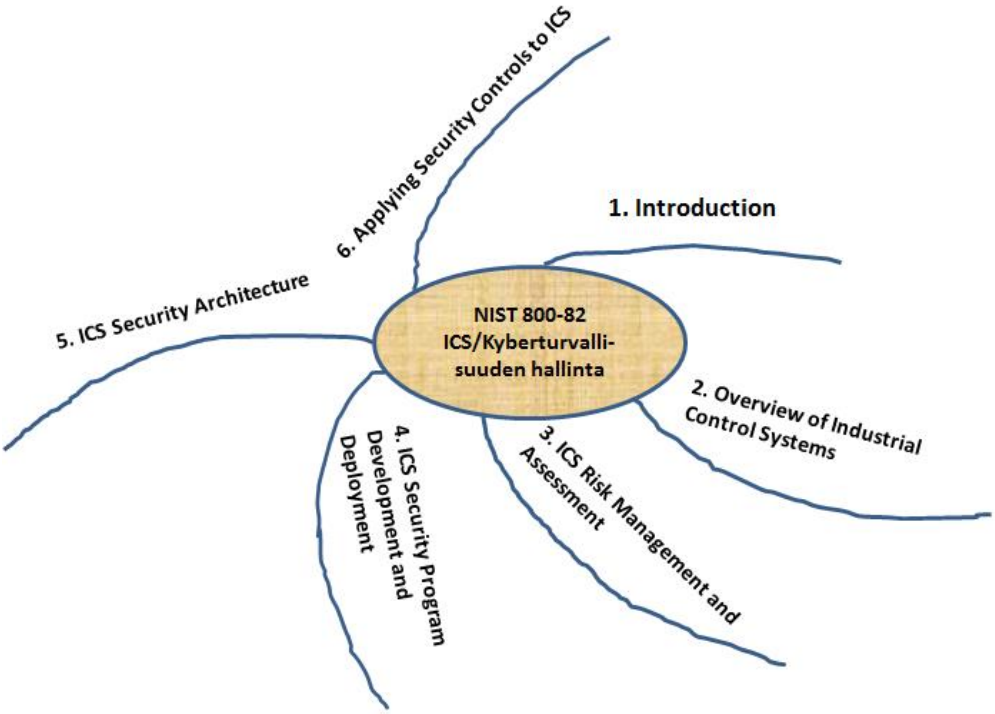
Ohjeen mukaan tiedonsiirtoverkon segmentointi- ja erottamistekniikoista riippumatta toimenpiteisiin pätee seuraavat teemat:

- Jokainen järjestelmä ja verkko tulee segmentoida ja erottaa aina datalinkkitasolta sovellustasolle asti.
- Käyttöoikeudet myönnetään ainoastaan tarvittavilta osilta.
- Erota informaatioon ja infrastruktuuriin liittyvät turvallisuusjärjestelyt toisistaan.
- Sovella käyttöoikeuksissa niin sanottuja white-listoja; ne sopivat ICS-järjestelmiin, koska niiden sovellukset ovat vakioituja. Toimenpide helpottaa myös järjestelmien loki-analyysejä.

Ohjeen viimeisessä luvussa, joka käsittelee tietoturvamenettelyjen soveltamista ICS-järjestelmiin, on viittauksia alueen muihin standardeihin, ohjeisiin ja suosituksiin. Muun muassa riskienhallinnasta

ohjeistuksen mukaiset vaiheet ovat kuvattuina ICS-järjestelmiin sovellettuna. Vaiheet ovat järjestelmäluokittelu, tietoturva-asetusten valinta, tietoturvavalvontatoimenpiteet, suojausasetusten arviointi, järjestelmähyväksyntä ja valvontatoimenpiteiden seuranta. Lisäksi luku käsittää laajasti eri turvatoimenpiteiden soveltamisia ICS-ympäristöön. Niihin liittyen yksi ohjeen liitteistä pitää sisällään selvitykset uhkalähteistä, haavoittuvuuksista ja tavanomaisimmista haitallisista tapahtumista. (Stouffer ym., 2015, 6-1 - 6-41.)

Kuvio 5 havainnollistaa koko ohjeen sisältöä. Siihen on poimittu ohjeen pääotsikoita.



KUVIO 5. NIST 800-52 ohjeen sisältö (Stouffer ym., 2015, 1-6 - 41)

3.5 Riskien hallinta

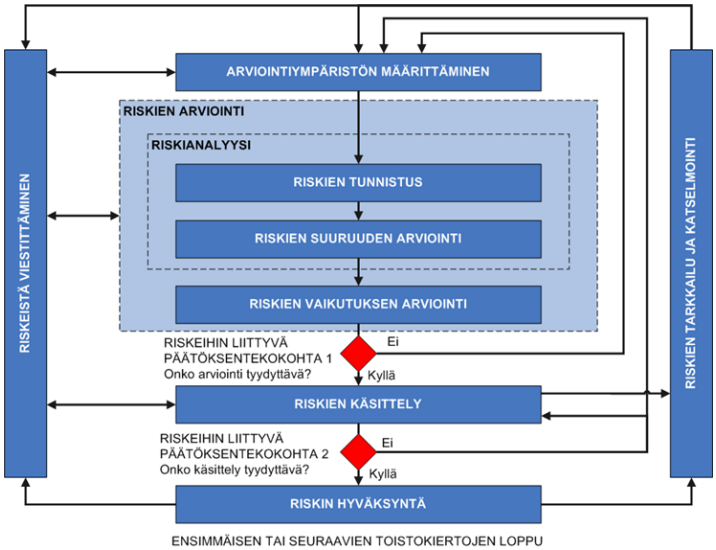
ISO/IEC 27005 Riskien hallinta

Tämä ohje käsittelee organisaation tietoturvallisuusriskien hallintaa. Sen ohjeisto tukee standardin ISO/IEC 27001 mukaisia tietoturvallisuuden hallintajärjestelmän vaatimuksia, mutta se ei pidä sisällään mitään tiettyä riskien hallinnan menettelytapaa. Organisaatio itse määrittelee riskien hallintaan liittyvät toimintatapansa. Toimintatavan valintaan vaikuttavat esimerkiksi hallintajärjestelmän kattavuusvaatimukset, arviointiympäristö ja toimiala. Standardin menettelyjä voidaan soveltaa kaiken tyyppisissä organisaatioissa. (Suomen Standardisoimisliitto SFS ry, 2015, 49.)

Ohjeen ISO/IEC 27005 mukaiset riskeihin liittyvät menettelyt voidaan kiteyttää seuraaviin kuvioihin. Kuviossa 6 on esitetty tämän standardin mukainen tietoturvallisuuden hallintaprosessi, joka koostuu seuraavista vaiheista:

- arviointiympäristön määrittämisestä
- riskien arvioinnista
- riskien käsittelystä
- riskin hyväksynnästä
- riskeistä viestimisestä ja
- riskien tarkkailusta ja katselmoinnista

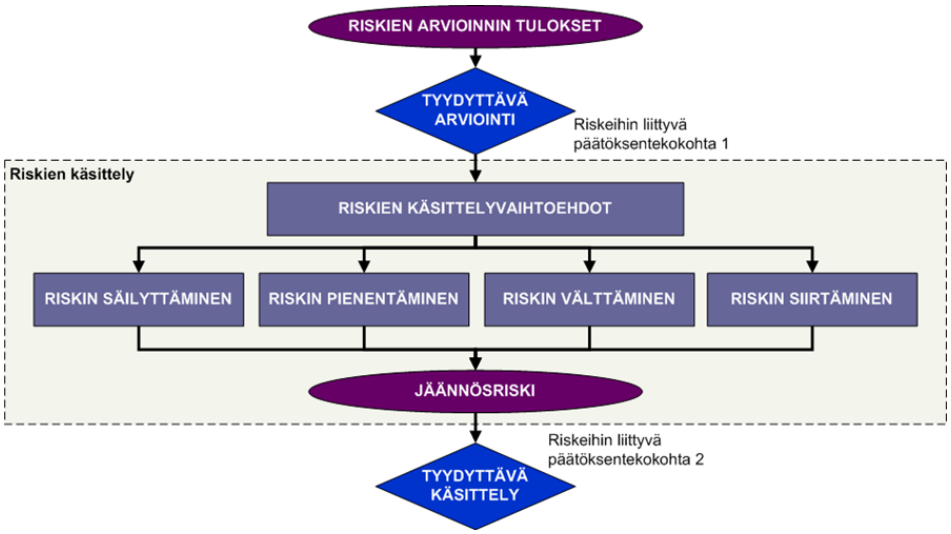
Kuviosta 6 ilmenee kuinka riskien arviointi- ja käsittelytoiminnot voivat olla iteratiivisia tietoturvariskien hallintaprosessissa. Riskien iteratiivinen toimintamalli auttaa saavuttamaan tasapainon siten, että turvamekanismien tunnistaminen suoritetaan tehokkaasti ja samalla varmistetaan erityisesti suurten riskien asianmukainen arviointi. (Suomen Standardisoimisliitto SFS ry, 2015, 49.)



KUVIO 6. Tietoturvariskien hallintaprosessi (Suomen Standardisoimisliitto SFS ry, 2015, 49)

Arviointiympäristön määrittämisen jälkeen tehdään riskien arviointi, jonka jälkeen voidaan siirtyä riskien käsittelyyn (KUVIO 7). Riskien käsittelyvaihtoehdot tulisi valita riskien arvioinnin tulosten, vaihtoehtojen toteuttamisen odotettavissa olevien kustannusten ja näistä vaihtoehdoista odotettavissa olevien hyötyjen perusteella. Vaihtoehdot, joilla on mahdollista pienentää riskejä merkittävästi suhteellisen alhaisin kustannuksin, tulisi toteuttaa ja erityisesti riskien haitalliset seuraukset tulisi saada niin vähäisiksi kuin on käytännössä mahdollista. Organisaation tulisi tarkastella myös harvinaisia, mutta vakavia riskejä, jolloin saatetaan joutua toteuttamaan turvamekanismeja, jotka eivät ole perusteltuja pelkästään taloudellisin perustein. (Suomen Standardisoimisliitto SFS ry, 2015, 50.)

Ohje painottaa, että riskien käsittelyn tehokkuus riippuu riskien arvioinnin tuloksista. Esimerkiksi on mahdollista, ettei jäännösriskiä saada välttämättä heti hyväksyttävälle tasolle, jolloin sen vaatimia toimenpiteitä on edelleen tehostettava. Koko tietoturvariskien hallintaprosessin ajan on tärkeää viestiä riskeistä ja niiden käsittelystä organisaatiossa tarkoituksenmukaisella tavalla. (Suomen Standardisoimisliitto SFS ry, 2015, 50.)



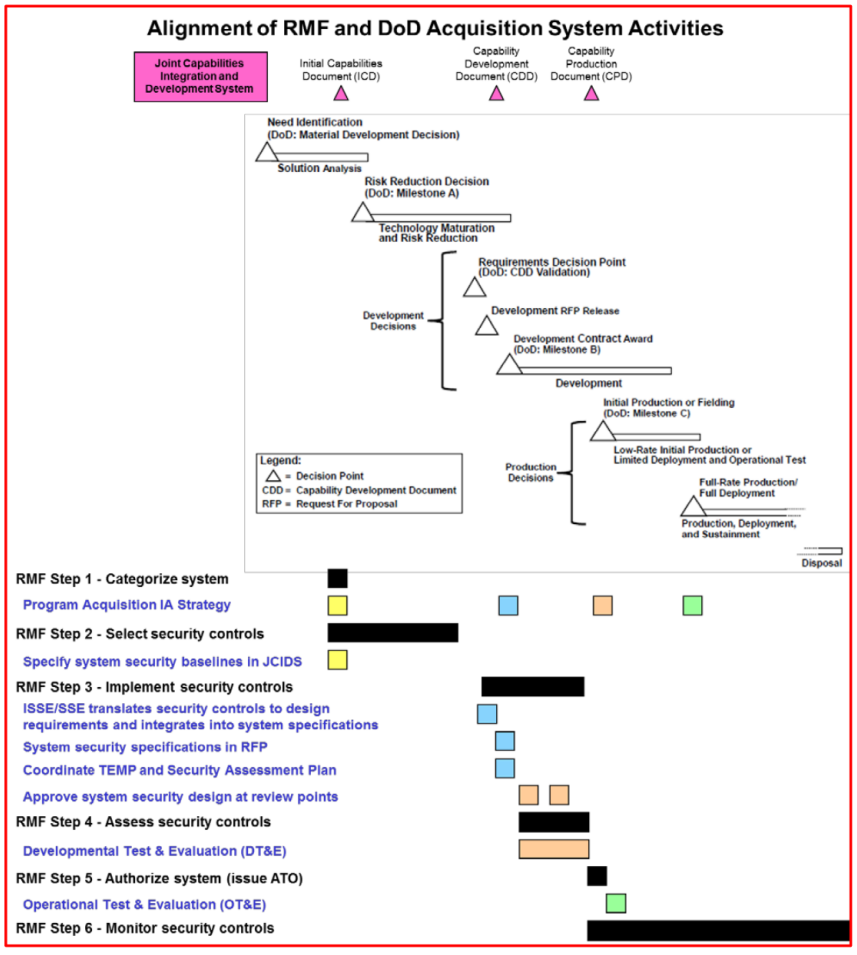
KUVIO 7. Riskien käsittelytoiminta (Suomen Standardisoimisliitto SFS ry, 2015, 50)

Department of Defense, INSTRUCTION NUMBER 8510.01 (2017)
Risk Management Framework (RMF) for DoD Information Technology (IT)

ICS-järjestelmien elinkaaret ovat pitkiä ja niitä jatketaan yleensä kustannustehokkaasti eritasoisilla elinkaaripäivityksillä. Kyberturvallisuuden riskien hallitseminen ja turvallisuutta parantavat toimenpiteet onkin suoritettava huomioiden tarkasteltavan järjestelmän koko elinkaari. Niiden liittäminen elinkaaren alkuvaiheen järjestelmäsuunnitteluun, jatkossa tapahtuviin elinkaaripäivitysten suunnitteluun ja käytännön implementointeihin sopii ICS-järjestelmien elinkaarien eri vaiheissa suoritettaviin toimenpiteisiin kehitetyt standardit ja ohjeet. Yhdysvalloissa on puolustusvälineteollisuus ohjeistettu dokumentilla “The U.S. Department of Defense (DoD), DoD Instruction 8510.01:DIACAP” toteuttamaan järjestelmähankintojen riskiperusteista hallintaa.

Yritystasolla ohjeiston toimivuuden todentaminen käytännössä on edellytyksenä järjestelmätoimittajan hyväksynnälle puolustusvälinetoimittajaksi, joten sitä voidaan pitää käyttökelpoisena ohjeena myös muihin kohteisiin. Sen avulla voi muodostaa suuntaa antava käsitys kyberturvallisuuden suunnitteluun tarvittavista eri toimenpiteistä ja niiden vaiheista. (Department of Defense, 2017, 1 - 2.)

Ohje viittaa riskienhallinnan kolmiportaiseen lähestymistapaan (organisaatio, liiketoimintaprosessi, tietojärjestelmä), joka on kuvattu julkaisussa NIST SP 800-39. Ohje synkronoi ja integroi edellä mainittujen tasojen toimenpiteet riskienhallintaan kaikissa IT-järjestelmän elinkaaren vaiheissa ja muodostaa niistä loogisen kokonaisuuden. Kuviossa 8 on esitetty järjestelmähankinnan elinkaaren turvallisuussuunnittelun vaiheet. (Department of Defense, 2017, 14.)

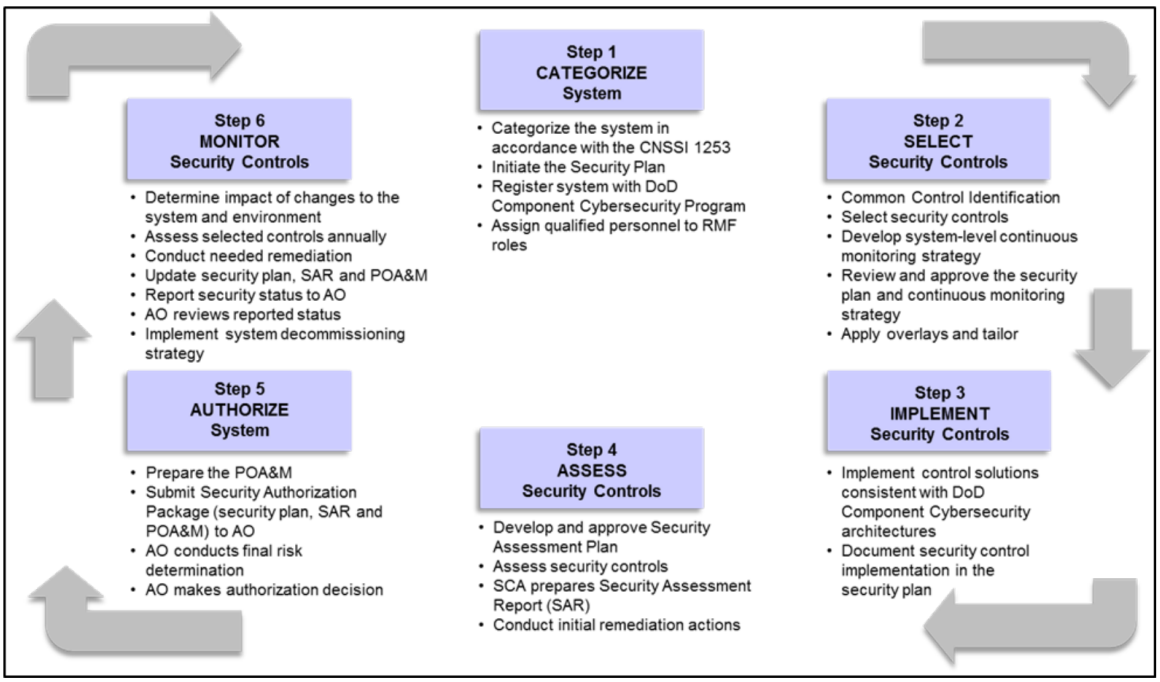


KUVIO 8. Kyberturvallisuuden riskien hallinta ja tuotteen elinkaaren vaiheet (Department of Defense, 2017, 39)

IT-järjestelmän elinkaaren eri vaiheisiin sidotut toimenpideaskeleet ovat seuraavat:

1. Järjestelmäluokittelu
2. Tietoturva-asetusten valinta
3. Tietoturvavalvontatoimenpiteet
4. Suojausasetusten arviointi
5. Järjestelmähyväksyntä
6. Valvontatoimenpiteiden seuranta

Kuviossa 9 IT-järjestelmän elinkaaren mukaiset riskien hallinnan vaiheet ovat avattu yleisellä tasolla.



KUVIO 9. Kyberturvallisuuden riskien hallinta ja tuotteen elinkaaren vaiheet yleisellä tasolla (Department of Defense, 2017, 28)

Seuraavassa ohjeessa NIST Special Publication 800-37 edellä mainittujen vaiheiden toimenpiteet ovat kuvattuina kuvioon 9 tarkemmin.

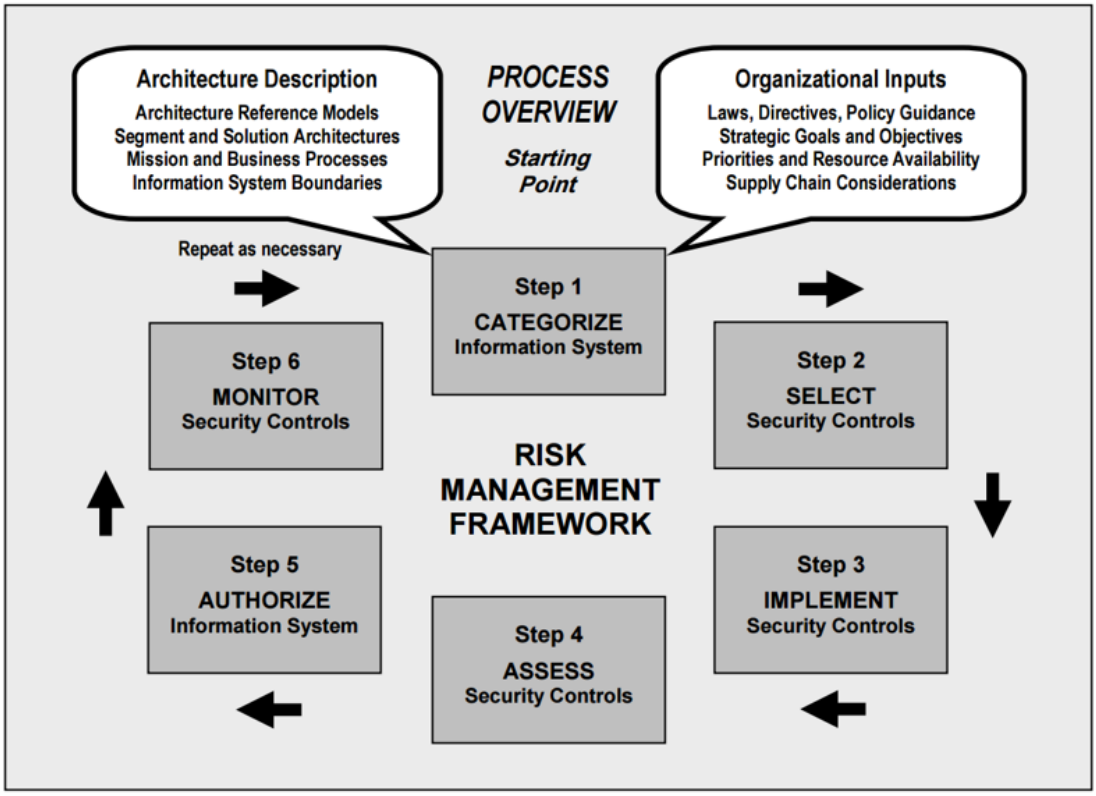
NIST Special Publication 800-37 Revision 1, (2010)
Guide for Applying the Risk Management Framework to Federal Information Systems Security Life Cycle Approach

Tämän ohjeen mukaisen riskienhallinnan viitekehyksen (Risk Management Framework, RMF) soveltaminen on tarkoitettu IT-järjestelmien elinkaarien aikaiseen riskien tarkasteluun. Viitekehyksen mukainen toiminta korostaa riskien hallintatyön merkitystä osana yrityksen johtamista ja kokonaisvaltaista riskien hallintaa. Se painottaa riskien hallinnan toimenpiteistä saatujen kokemuksen ja organisaation kaikkien kyberturvallisuuskykyjen hyödyntämistä sovellettaessa toimenpiteitä IT-toimintaan, alueen tilannetietoisuuden ylläpitämiseen ja johdon päätöksenteon pohjaksi. Ohjeet tarkoitus on kohdistaa käytännön riskien arviointitoimenpiteet IT-järjestelmien

turvallisuusluokitteluun, ohjaustoimenpiteiden valintaa, käyttöönottoon ja valvontaan. (National Institute of Standards and Technology, 2010, 1.)

Ohjeen mukaan koko organisaation osallistumista riskien arviointityöhön pidetään ensiarvoisen tärkeänä, koska tällöin riskit tulee huomioitua kaikilta osilta ja laaja-alaisesti koko organisaation toimintakentässä. Se tarkoittaa operatiivisten IT-järjestelmätason riskien lisäksi sitä, että mukaan tulevat myös taktisen tason ja strategisen tason riskitarkastelut. Näin toteutettuna operaatioympäristöön ja liiketoimintaympäristöön kohdistettuna riskitarkastelu kattaa niin prosessitason toteutusvastuut kuin organisaation kokonaisvastuut. Toimenpiteiden tulee olla johdonmukaisia, hyvin informoituja ja jatkuvasti ylläpidettäviä. Riskien hallinnan viitekehyksen mukaiset vaiheet ja vastuut on lueteltu ohjeessa. (National Institute of Standards and Technology, 2010, 1 - 2.)

Ohjeen merkittävin anti on edellä mainitun kuusivaiheisen riskienhallinnan prosessin kuvaaminen. Kuviossa 10 on vaiheet kuvattu yleisellä tasolla.



KUVIO 10. Organisaation riskien hallinnan prosessi (National Institute of Standards and Technology, 2010, 8)

Jokaiseen hallintaprosessin vaiheeseen on ohjeessa kuvattu sen eri osavaiheet ja niiden vaatimat toimenpiteet, ensisijaiset vastuut, toiminnan edellyttämät tukevat roolit, valtuutukset, toimenpiteet järjestelmän eri elinkaarivaiheissa ja tehtävän suorittamiseen liittyvät täydentävät ohjeet. Siihen on myös luetteloitu jokaiseen vaiheeseen liittyvät muut ohjeet ja tietolähteet. (National Institute of Standards and Technology, 2010, 8 - 9.)

Ohjeen loppuosan liitteissä on muun muassa lueteltu ja kuvattu toimintaan liittyvät organisaatiolliset vastuut ja esitetty taulukkomuodossa jokaisen vaiheen tehtävät ja niihin liittyvät vastuutahot rooleineen. Lisäksi liitteissä on kuvaukset turvallisuuteen liittyvistä valtuutuksista, niiden jatkuvan

valvonnan toteutuksesta ja kuvaukset riskien hallintaan liittyvistä mahdollisista toimintaympäristöistä. (National Institute of Standards and Technology, 2010, A-1 - I-3.)

Vaiheessa 1 IT-järjestelmät luokitellaan tiedon attribuuttien mukaan eli luokittelu tapahtuu tiedon luotettavuuden, eheyden ja saatavuuden mukaisesti. Oheiset attribuutit ovat ohjeen FISP 199 mukaisia. Tiedon saatavuuden varmistaminen ja siten järjestelmätason korkean käytettävyyden ylläpitäminen on merkittävin ICS-järjestelmien tapauksessa. SCADA-järjestelmään annetut suositukset ja ohjaukset liittyvät järjestelmän jokaiseen tehtävään, mutta esimerkiksi sähkön jakelun ja tuotannon ohjauksessa vaatimustasot ovat seuraavat: luotettavuusvaatimus on keskitasoa, eheysvaatimus on korkea ja käytettävyysvaatimus on korkea. Lisäksi ohje antaa esimerkkejä erilaisten haittavaikutusten luokittelusta asteikolla matala, keskinkertainen ja korkea sovellettuna taloudellisiin menetyksiin, ympäristövaikutuksiin, häiriön kestoon ja julkisuuskuvaan. (National Institute of Standards and Technology, 2010, 25.)

Vaiheessa 2 suoritetaan varmenteiden valintatoimenpiteet vaiheessa 1 suoritetun luokittelun mukaisesti. Ohje FISP 200 määrittää minimivaatimukset kahdeksalletoista turvallisuusalueelle tiedon luotettavuuden, eheyden ja satavuuden näkökulmista, kun tietoa käsitellään, varastoidaan tai välitetään IT-järjestelmissä. Varmenteen tulee olla koko työyhteisöä käsittävä, tarkoituksenmukainen, organisaatiota ja IT-järjestelmiä päällekkäisesti kattava lajitelma niitä. Näin varmenteet voidaan kohdistaa parhaiten vastaamaan kunkin kohteen tarpeita. Niiden ”räätälöinnillä” saavutetaan organisaation sisällä olevat erillistarpeet ja -vaatimukset. Esimerkiksi ICS-järjestelmissä varmenteiden ”räätälöinti” on suoritettava kohdassa 1 esitettyjen haittavaikutusten luokittelun mukaisesti. (National Institute of Standards and Technology, 2010, 25.)

Prosessin vaiheessa 3 suoritettavilla toimenpiteillä huolehditaan, että varmenteet tulevat käyttöön niin vanhoissa kuin uusissakin kohteissa. Kun varmenteita otetaan käyttöön, niin samalla on syytä tarkistaa, että niiden kattavuus on riittävä eikä turvallisuuteen jää aukkoja miltään osin. (National Institute of Standards and Technology, 2010, 25.)

Prosessin vaihe 4 pitää sisällään varmenteiden arviointimenettelyn, joka tarkoituksena on varmistaa niiden käyttöönotto, toiminta ja vaikuttavuus niin, että asetetut vaatimukset täyttyvät. (National Institute of Standards and Technology, 2010, 25.)

Prosessin vaihe 5 liittyy IT-järjestelmään siten, että sen tuloksena on hallinnollinen päätös auktorisoida IT-järjestelmän toiminta ja hyväksyttää siihen liittyvät toiminnat, laitteet tai henkilöt valtuutuksineen ja riskeineen. (National Institute of Standards and Technology, 2010, 25.)

Prosessin viimeisen vaiheen (kohta 6) toimenpiteiden tarkoituksena on pitää yllä jatkuvaa IT-järjestelmien muutosseurantaa, jotta niistä aiheutuvia vaikutuksia varmenteisiin voidaan hallita tehokkaasti. (National Institute of Standards and Technology, 2010, 25.)

NIST Special Publication 800-30 Revision 1, (2012)
Guide for Conducting Risk Assessments

Riskien arviointi on yksi organisaation riskienhallinnan peruskomponenteista, josta on laadittu julkaisu nimeltä ”Guide for Conducting Risk Assessments” NIST-sarjaan tunnuksella 800-39. Toimenpiteitä käytetään organisaation toiminnallisten riskien tunnistamiseen, arviointiin ja priorisointiin huomioiden organisaation järjestelmät, henkilöstö, sidosryhmät ja yhteiskunnalliset velvoitteen. Arvioinnin tarkoituksena on tunnistaa ja kartoittaa päätöksentekijöille riskit seuraavasti: organisaatioille aiheutuvat merkittävät uhat, toimintaverkoston välityksellä uhkaavat toimet omaan ja muihin organisaatioihin nähden, sisäiset haavoittuvuudet organisaation ulkopuolelle ja organisaatioiden keskinäisvaikutuksiin. Lisäksi toimenpiteisiin kuluu riskien toteutumisen todennäköisyyksien ja niistä aiheutuvien vahinkojen arviointi. Lopputuloksena tulee olla riskien määrittämisen kuvaus. Tyypillisesti se esitetään riskien haitta-asteena ja tapahtumatodennäköisyytenä, josta lopullinen luokittelu esitetään näiden matemaattisena tulona. (National Institute of Standards and Technology, 2012, 17.)

Ohjeen mukaan riskienhallinnassa toimenpiteet tulee suorittaa kolmella hierarkiatasolla:

- Taso 1, organisaation taso
- Taso 2, tehtävä / liiketoimintaprosessitaso
- Taso 3, tietojärjestelmätaso

Tasoilla 1 ja 2 organisaatiot käyttävät riskinarviointeja arvioidakseen kartoittaa sellaisia järjestelmällisiä tietoturvaan liittyviä riskejä, jotka liittyvät organisaation hallintoon ja johtamiseen, liiketoimintaprosesseihin, yritysarkkitehtuuriin tai rahoitukseen. Tasolla 3 organisaatiot käyttävät riskinarviointeja kartoittaakseen riskejä, jota kohdistuvat tehokkaammin tietoturvaluokitukseen sekä tietoturvallisuuden valvonnan valinta-, toteutus- ja arviointitoimenpiteisiin.

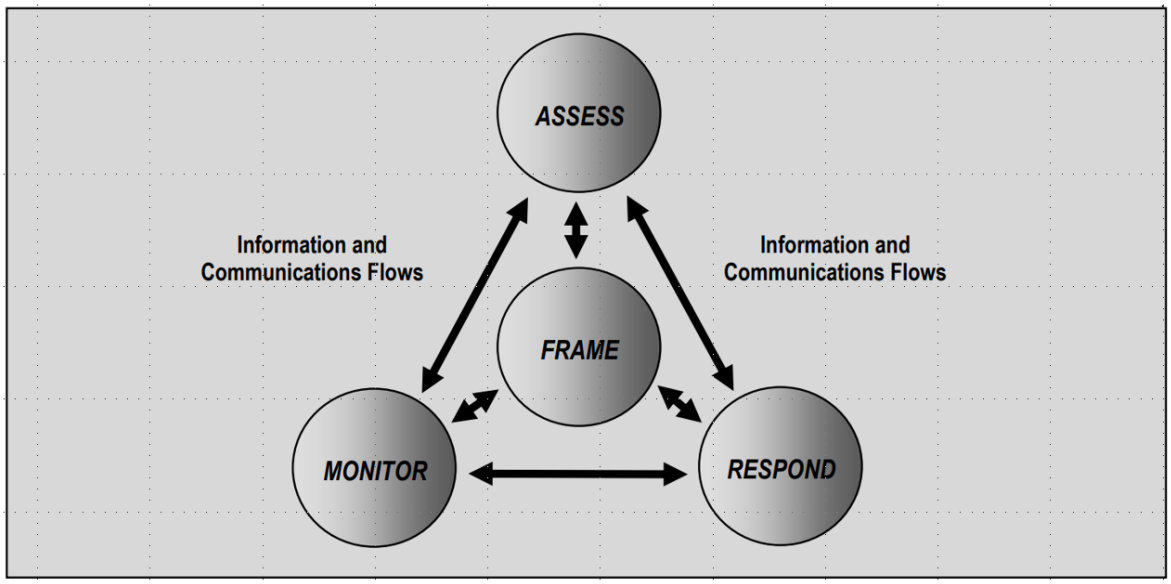
Tämä julkaisu keskittyy riskienhallintaan, joka pitää sisällään seuraavat vaiheet:

- miten valmistaudutaan riskinarviointeihin,
- miten suoritetaan riskinarviointeja,
- miten riskinarviointitulokset voidaan kommunikoida tärkeimpien organisaatioiden kanssa, henkilöstö mukaan lukien,
- miten riskinarviointien pitäminen ajan tasalla tapahtuu ja miten sitä mitataan.

Riskinarvioinnit eivät voi olla kertaluonteisia toimintoja, jotka tarjoisivat pysyviä ja lopullisia tietoja päätöksentekijöille. Pikemminkin organisaatioiden tulee arvioida riskejään jatkuvasti huomioiden järjestelmiensä elinkaaret ja edellä mainitut hierarkiatasot. Organisaatioiden tulee arvioida riskiarviointien tarpeellinen tiheys ja riskiarviointityöhön sitoutuvat resurssit, jotka ovat suhteessa nimenomaisesti määriteltyyn tarkoituksenmukaisuuteen ja laajuuteen. (National Institute of Standards and Technology, 2012, 17 - 18.)

Riskien arviointi on olennainen osa kokonaisvaltaista, koko organisaation laajuista riskienhallintaprosessia, joka on määritelty NIST:n erikoisjulkaisussa 800-39; Tietoturvariskin hallinta: organisaatio, toiminta ja tietojärjestelmä. Riskienhallintaprosesseihin kuuluvat: riskien määrittäminen, riskien arviointi, riskiin vastaaminen ja seuranta. Kuvio 11 havainnollistaa näitä neljää

vaihetta riskienhallintaprosessissa - mukaan lukien riskien arviointivaihe ja riskitiedot sekä kommunikaatio tuloksista. (National Institute of Standards and Technology, 2012, 17.)

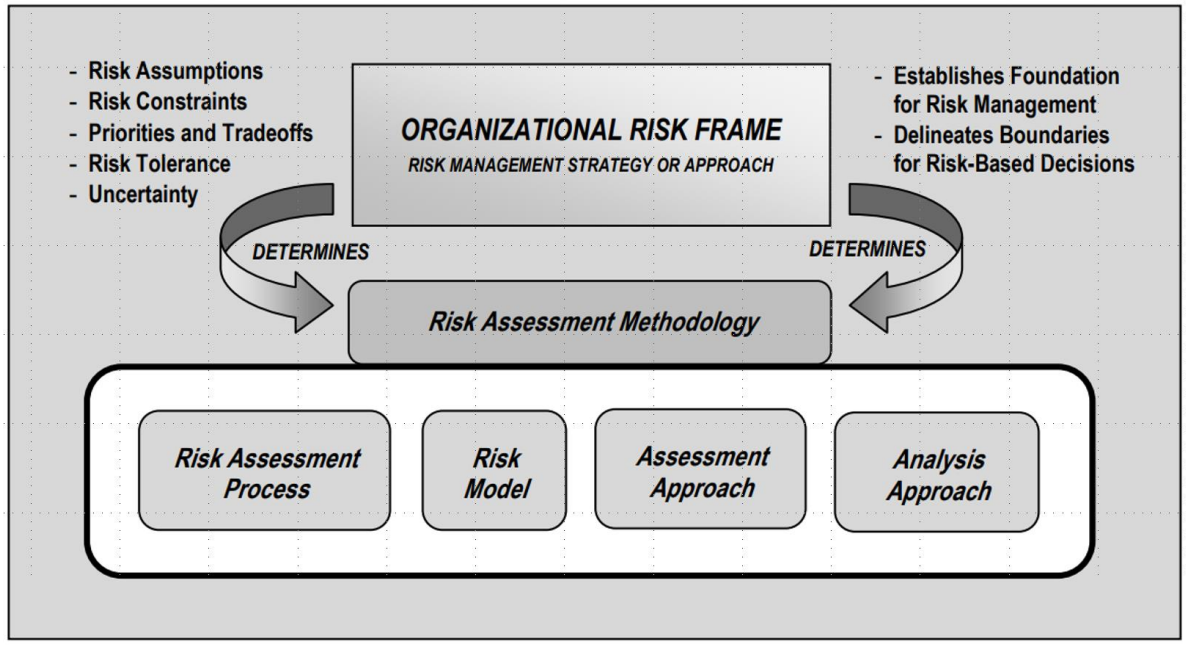


KUVIO 11. Organisaation riskien arviointi osana riskien hallinnan prosessin toteutusta (National Institute of Standards and Technology, 2012, 4)

Riskienarviointimenetelmään kuuluvat tyypillisesti:

- riskienarviointiprosessi, selkeä riskimalli, jossa määritellään keskeiset käsitteet ja arvioitavat riskitekijät ja niiden suhteet,
- arviointimenetelmä, jossa määritellään ne riskitekijät, jotka voivat olettaa toteutuvan,
- miten riskitekijöiden yhdistelmät tunnistetaan / analysoidaan ja arvioidaan (julkaisu NIST 800-30 opas arvioinnin suorittamiseksi) ja
- analysointimenetelmä (esimerkiksi vaikutus tai haavoittuvuus), jossa kuvataan riskien yhdistelmiä ja eri tekijät tunnistetaan/analysoidaan ongelmatilan riittävän kattavuuden varmistamiseksi.

Organisaatiot määrittelevät riskinarviointimenetelmät, jotka ovat osa niiden riskienhallintastrategiaa. Kuviossa 12 on esitetty organisatoristen riskikehysten peruskomponentit ja niiden osien väliset suhteet. Ohjeessa peruskomponenttien sisällöt ovat selvitetty perusteellisesti.



KUVIO 12. Organisaation riskikehyksen peruskomponentit (National Institute of Standards and Technology, 2012, 7)

Ohjeessa on myös kuvattu omana kokonaisuutenaan tietoturvariskien arviointimenettely, mukaan lukien:

- korkean tason yleiskuva riskinarviointiprosessista,
- valmisteluun tarvittavat toimet riskinarviointiin,
- tehokkaat riskinarviointiin tarvittavat toimet,
- tiedot, jotka ovat tarpeen arviointitulosten ilmoittamiseksi ja
- riskien toiminnot, joita tarvitaan riskinarviointien tulosten jatkuvaan ylläpitoon.

Ohjeen keskeisin anti on nelivaiheisessa riskien käsittelyn prosessiohjeistuksessa. Vaiheet ovat aiemmin esillä olleet valmistautuminen, arvioinnin suorittaminen, tulosten ilmoittaminen ja ylläpitäminen. Jokainen vaihe on jaettu joukkoon tehtäviä, jotka ovat kuvattu. Jokaista tehtävää varten on käytössä täydentävät ohjeet. Riskitaulut ja esimerkinomaiset arviointiasteikot luetellaan asiakohtaisissa tehtävissä. (National Institute of Standards and Technology, 2012, 7 - 8.)

Ohjeen liitteinä ovat sanasto tietoturvatermeille, lyhenteiden kuvaus, luettelot tyypillisistä uhkalähteistä ja tapahtumista sekä taulukot tyypillisistä haavoittuvuuksista ja niiden todennäköisyyksistä. (National Institute of Standards and Technology, 2012, A-1 - L-2.)

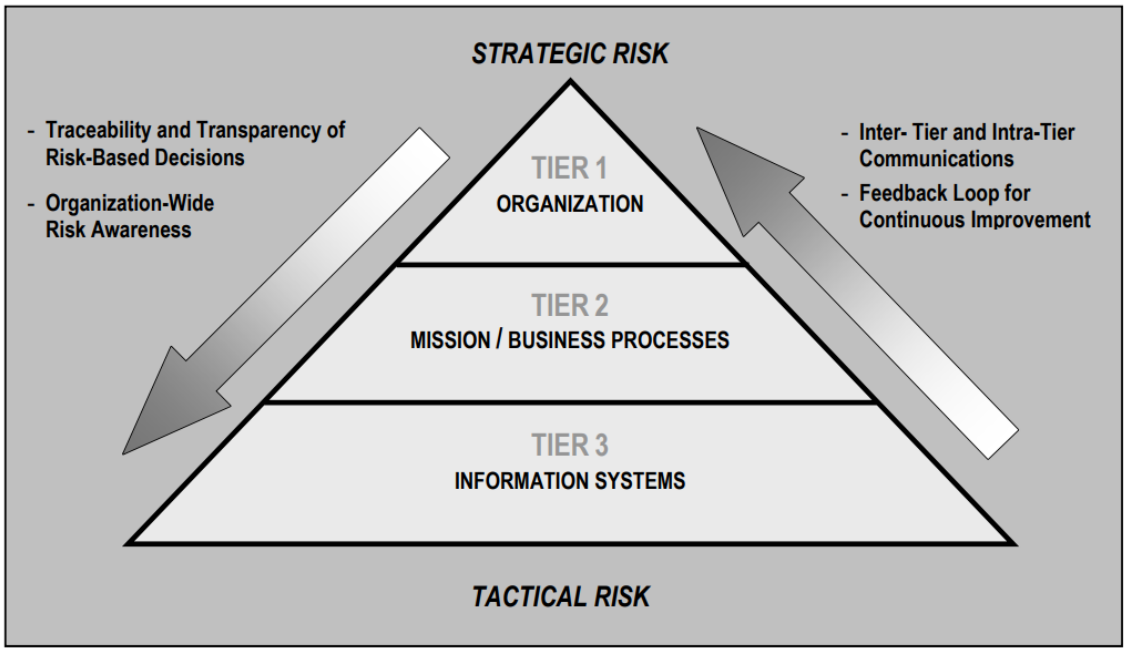
NIST Special Publication 800-39, (2011)
Managing Information Security Risk, Organization, Mission, and Information System View

Organisaation toiminta voi sisältää monenlaisia riskejä. Tietojärjestelmien käyttöön liittyvät turvallisuusriskit ovat vain yksi monista organisaation riskeistä, joita johtajien on syytä käsitellä osana kokonaisvastuutaan. Tehokas riskienhallinta edellyttää, että organisaatiot tunnistavat toimivansa monimutkaisissa, toisiinsa yhteydessä olevissa tietotekniikkaympäristöissä, joissa käytetään huipputeknisiä, mutta myös vanhoja tietojärjestelmiä. (National Institute of Standards and Technology, 2011, 1.)

Tämä julkaisu sijoittaa tietoturvan ja sen riskitarkastelun laajempaan organisaatiokehykseen, jossa yrityksen tavoitteena on pitää yllä hyvää mainettaan ja saavuttaa menestystä liiketoiminnassaan. Ohjeen tavoitteena on:

- varmistaa, että johtajat tunnustavat tietoturvariskit ja luovat asianmukaiset hallintorakenteet tällaisen riskin tunnistamiseksi ja hallitsemiseksi,
- varmistaa, että organisaation riskienhallintaprosessi toteutetaan tehokkaasti kaikkialla kolmella hierarkiatasolla; organisaatio (taso 1), liiketoimintaprosessit (taso 2) ja tietojärjestelmät (taso 3),
- edistää organisaation ilmapiiriä, jossa tietoturvariskit otetaan huomioon koko toiminnassa, liiketoimintaprosessien suunnittelussa, yrityksen tietojärjestelmien arkkitehtuurissa ja järjestelmäkehityksessä, ja
- auttaa henkilöstöä vastaamaan tietojärjestelmien käytöstä tai toiminnasta ja ymmärtämään aiempaa paremmin mistä tietojärjestelmien turvallisuusriskit muodostuvat.

Jotta riskienhallintaprosessi voidaan integroida koko organisaatiossa, on ohjeessa kuvattu kolmiportainen lähestymistapa. Toimenpiteet tulee kohdentua riskeihin organisaatiotasolla, operaatio-/ liiketoimintaprosessitasolla ja tietojärjestelmätasolla. Ohjeessa riskienhallintaprosessi toteutetaan saumattomasti kaikille kolmelle tasolle, jolloin toimenpiteiden yleistavoitteena on organisaation toiminnan jatkuva parantaminen organisaation tietoturvaan liittyvissä riskeissä. Tarkoituksenmukaiset toimenpiteet ja niiden viestintä kaikkien sidosryhmien kesken ovat merkittävä osa koko prosessia. Niillä on merkitystä eri tahojen sitoutumisessa organisaation toimintaan ja liiketoiminnan menestyksessä. Kuvio 13 havainnollistaa kolmitasoista lähestymistapaa riskienhallintaan yhdessä sen keskeisten ominaispiirteiden kanssa. Se muodostaa linkityksen strategisen tason ja taktisen tason riskien välille. (National Institute of Standards and Technology, 2011, 2 - 3.)



KUVIO 13. Organisaation riskikehyksen tasot (National Institute of Standards and Technology, 2011, 9)

Taso 1 (TIER 1) käsittelee riskejä organisaation näkökulmasta katsottuna. Se muodostaa ensimmäisen riskienhallinnan osa-alueen, joka tarjoaa perussisällön kaikille muillekin riskienhallintatoimille. Organisaatiotasolla toteutettavat ensisijaiset riskienhallinnan toimenpiteet vaikuttavat suoraan toimenpiteisiin tasoilla 2 ja 3. Esimerkiksi tasolla 1 määritellyt tehtävät vaatimuksineen vaikuttavat tasolla 2 suoritettavien liiketoimintaprosessien suunnitteluun, kehittämiseen ja niiden toteuttamiseen. Taso 1 asettaa etusijan tehtäviin ja liiketoimintamalleihin, jotka puolestaan ohjaavat muun muassa sijoitusstrategioita ja rahoituspäätöksiä, ja siten vaikuttavat koko yrityksen tietotekniseen arkkitehtuuriin (mukaan lukien sulautettu tietojärjestelmät). Näistä seuraavat järjestelmien käyttöönotot ja operatiiviset ja tekniset turvatarkastukset tasolla 3. Muita esimerkkejä tason 1 toiminnoista, jotka vaikuttavat seuraaville tasoilla tehtäviin toimenpiteisiin, ovat muun muassa yhteinen tietoturvavalvonta, ohjauksen antaminen riskinhallinnassa, lupajärjestelyt eri toimijoille tietojärjestelmissä ja varautumiseen liittyvät toimenpiteet, kuten järjestelmien palauttamisjärjestyksen määrittäminen ja toteuttamiseen liiketoiminnan kriittisissä tehtävissä. (National Institute of Standards and Technology, 2011, 9 - 10.)

Määrittämistaso 2 (TIER 2) käsittelee riskejä liiketoimintaprosessin näkökulmasta katsottuna. Tason riskienhallintaan kuuluvat toimenpiteet, joilla:

- määritellään liiketoimintaprosessit, joita tarvitaan organisaatiossa koko toiminnan tukemiseen,
- priorisoidaan liiketoimintaprosessit strategisten tavoitteiden suhteen,
- määritellään tarvittavat tiedot menestyksekkääseen toimintaan ja määritellään tietojen kriittisyys/herkkyys sekä sisäiset ja ulkoiset tiedotusorganisaatiot,
- määritetään tietojen sisällyttäminen turvaluokitusvaatimusten mukaisesti ja luodaan tietotekninen yritysarkkitehtuuri, jossa on mukana sulautettu tietoturva-arkkitehtuuri ja joka edistää kustannustehokaita tietotekniikkaratkaisuja ja on johdonmukainen organisaation strategisten tavoitteiden ja suorituskyvyn kanssa.

Tason 2 toimenpiteet vaikuttavat suoraan tasolla 3 toteutettaviin toimintoihin, joista esimerkkinä on yrityksen tietoturva-arkkitehtuuri, joka ohjaa tietosuojatarpeita, jotka vuorostaan vaikuttavat ja

ohjaavat turvatarkastuksiin ja tietojärjestelmien osiin. Taso 2 vaikuttaa myös tietojärjestelmien suunnitteluun mukaan lukien spesifikaatiot, jotka ovat hyväksyttäviä näiden järjestelmien kehittämiseen. Taso 2:n toimet voivat myös tarjota hyödyllistä palautetta tasolle 1, mistä saattaa aiheutua riskitarkasteluun muutoksia tai, jotka vaikuttavat suoranaisesti meneillään oleviin riskienhallintatoimiin. (National Institute of Standards and Technology, 2011, 10.)

Taso 3 (TIER 3) käsittelee riskiä tietojärjestelmien näkökulmista tarkasteltuna ja ohjaa riskien ja riskialttiiden toimintojen liittymiset tasoille 1 ja 2. Tason riskienhallintatoimiin kuuluvat:

- tietojärjestelmien luokittelu,
- tietoturvatarkastukset tietojärjestelmittäin ja niiden toimintaympäristön suhteet huomioiden niin, että kyseiset järjestelmät toimivat yhdenmukaisesti organisaation tietoarkkitehtuurin kanssa ja
- tietoturvatarkastusten valinta, toteutus, arviointi, hyväksyntä, joka on jatkuvaa toimintaa osana järjestelmien elinkaariprosessin toteutusta koko organisaatiossa.

Tasolla 3 tietojärjestelmien omistajat, tietoturvatarkastajat ja järjestelmä- ja turvallisuusinsinöörit tekevät riskiin perustuvia päätöksiä tarvittavien turvatoimenpiteiden toteuttamisesta ja valvonnasta. Päivittäisten toiminnan riskien perusteella laaditut päätökset mahdollistavat ja valtuuttavat luvan tehdä riskiin perustuvia päätöksiä siitä riippumatta ovatko kyseessä olevat tietojärjestelmät alun perin sallittuja toimimaan tietyissä ympäristöissä tai voivatko ne saada edelleen jatkuvan toimiluvan. Jatkuvat riskiperusteiset toimenpiteet auttavat johdon päätöksen teossa turvatessa toimivat liiketoimintaprosessit. Lisäksi taso 3:n toiminnot tarjoavat olennaisen palautteen tasoille 1 ja 2. Esimerkkinä näistä palautteista ovat tietojärjestelmissä havaitut haavoittuvuudet, jotka ulottuvat koko organisaatioon. Nämä samat haavoittuvuudet voivat laukaista muutoksia yrityksen tietoturva-arkkitehtuuriin tai voivat edellyttää organisaation riskitoleranssin muuttamista. (National Institute of Standards and Technology, 2011, 10 - 11.)

Ohje palvelee monipuolisesti riskienhallinnan johtotehtäviä, organisaatioiden kokonaistehtävien suorittamisesta, tietojärjestelmien, tietotekniikkatuotteiden ja -palveluja hankkijoita sekä tietoturvallisuuden valvonta-, hallinta- ja toteutustahoja. (National Institute of Standards and Technology, 2011, 1 - 49.)

3.6 Turvallisuustekniikat

NIST Special Publication 800-177, (2016) Trustworthy Email, 2. DRAFT

Sähköposti on organisaation viestinnässä erittäin merkittävä kanava. Samalla, kun sähköposti mahdollistaa tehokkaan viestinnän, sen avulla hyvin yleisesti yritetään huijata viestin saajia tai murtautua yrityksen tietovarantoihin ja -järjestelmiin. Tämä luonnosasteella oleva NIST-organisaation dokumentti antaa ohjeita ja suosituksia turvalliseen sähköpostitoimintaan. Toimenpiteillä voidaan pienentää riskejä huijatuksi tulemiseksi, viestien päätymiseksi jakeluun kuulumattomille ja niiden käyttöä tietojärjestelmiin kohdistuvana hyökkäysmuotona. Ohje soveltuu käytettäväksi eri kokoisissa julkisissa ja yksityisissä organisaatioissa niin omin toimin hallituissa kuin ulkoistetuissa sähköpostipalveluissa ja virtuaaliympäristössä. (Chandramouli, Garfinkel, Nightingale & Rose, 2016, 3.)

Ohjeessa on kuvattu sähköpostijärjestelmään kuuluvat osat ja niistä muodostuva tyypillinen järjestelmäkokonaisuus sekä järjestelmän tiedonsiirtoprotokollat ja sanomaformaatit (Chandramouli ym., 2016, 3).

Se sisältää myös kuvaukset sähköpostipalvelujen merkittävimmistä uhkatekijöistä tiedon eheyteen, luotettavuuteen ja saatavuuteen liittyen. Uhkatekijät liittyvät erityisesti luvattomiin pääsyihin organisaation sähköpostijärjestelmään ja sen luottamuksellisiin viesteihin, huijausviesteihin ja sähköpostipalvelujen käytön estämiseen. (Chandramouli ym., 2016, 3 - 4.)

Ohje sisältää turvallisuussuosituksia edellä mainittujen uhkien osalta, joilla vähennetään luvattoman lähettäjän riskiä ja luvattomien vastaanottimien riskiä sekä estetään yrityksen IT-infrastruktuuriin kuulumattomien laitteiden kytkeytymiset sähköpostijärjestelmään. (Chandramouli ym., 2016, 3 - 4.)

Ohje sisältä turvalliseen viestien lähettämiseen ja vastaanottamiseen liittyviä menettelyjä, jota on kuvattu teknillisiä yksityiskohtia myöten. Esimerkiksi liikenteen suodattaminen, salaaminen ja eri todennukset ovat laajasti kuvattuina ohjeessa. Kukin osa-alue sisältää turvallisuussuosituksia. (Chandramouli ym., 2016, 3 - 4.)

NIST Special Publication 800-147, (2011), BIOS Protection Guidelines
NIST Special Publication 800-147B, BIOS Protection Guidelines for Servers (Draft)

Tietokoneiden systeemitason perusohjelmisto on nimeltään Basic Input/Output System (BIOS), joka toimii laitetason prosessien käynnistäjänä ja alustajana käyttöjärjestelmälle. Se on tyypillisesti kehitetty alkuperäisen laitevalmistajan tai alihankkijan toimesta ja otettu käyttöön vasta lopullisessa tietokoneen valmistumisvaiheessa valmistajan toimesta, jolloin BIOS:n sisältämät haavoittuvuudet ovat voineet jäädä korjaamatta. Lisäksi luvaton BIOS:n modifiointi haittaohjelman avulla on merkittävä uhka tietokoneiden toiminalle, koska BIOS ohjaa tietokoneen käynnistysprosesseja ja on siten ainutlaatuinen ja ohittamaton osa tietokonearkkitehtuurissa. BIOS:iin kohdistuvien haittaohjelmahyökkäysten onnistuminen vaatii erikoisosaamista. Onnistuessaan ne ovat vaikeasti havaittavissa ja voivat täten aiheuttaa vakavaa vahinkoa tietojärjestelmissä. (Cooper, Polk, Regenscheid, & Murugiah, 2011, 1-1.)

Ohjeisto pitää sisällään suojaustoimenpiteitä, joilla pyritään ehkäisemään hallitsemattomien ja haitallisten BIOS-ohjelmien päätyminen tietokoneisiin. Ohjeisto käsittää turvallisen BIOS-päivitysprosessin ohjeet tahoille, jotka suunnittelevat, valitsevat tai toteuttavat järjestelmän BIOS-päivityksen ja varmistavat sen aitouden ja eheyden. Lisäksi ohje käsittelee BIOS:n suojausta ulkopuolisilta muutoksilta. Suositusten tarkoituksena on estää luvaton BIOS:n muuttaminen. (Cooper ym., 2011, 1-1.)

Toinen ohje (NIST-800147B) käsittelee palvelimia. Palvelinjärjestelmän arkkitehtuurin ja toiminnan monimutkaisuus sekä prosessoreiden määrä edellyttävät palvelimien etähallintaa, mistä johtuu se, että niiden BIOS:n suojaustoimenpiteet eroavat muista tietokoneiden vastaavista toimenpiteistä. Tästä johtuen BIOS-päivitykset edellyttävät useiden eri päivitysmenetelmien hallintaa. Palvelinten BIOS:n suojaamiseen tähtäävä ohje sisältää kolme keskeistä periaatetta, joita voidaan soveltaa niin pääteasemiin kuin palvelintason laitteisiinkin. Periaatteet liittyvät hyväksyttyyn ohjelmistopäivitykseen, tiedon eheyden suojaamiseen ja ohittamattomiin suojausmenetelmiin. Ohje sisältää palvelimien BIOS-päivitysten vaatimuksia, joiden avulla pyritään ehkäisemään BIOS-ohjelmien vahingoittuminen tai korruptoituminen. (Regenscheid, 2014, 1-1.)

NIST Special Publication 800-41 (2009)
Guidelines on Firewalls and Firewall Policy

Palomuurit ovat laitteita tai ohjelmia, jotka ohjaavat verkkoliikennettä erilaisia turvallisuusasetuksia hyväksi käyttäen. Ohjeella pyritään auttamaan organisaatioita ymmärtämään palomuuritekniikan ominaisuuksia ja käyttöä ohjaavaa palomuuripolitiikkaa. Se tarjoaa käytännön ohjeita palomuurisääntöjen kehittämiseen ja valintaan, palomuurien testaamiseen, käyttöönottoon ja hallintaan. (Scarfone & Hoffman, 2009, ES-1 - ES-2.)

Ohje sisältää yleiskatsauksen useisiin verkon palomuuritekniikkoihin ja suosituksia niiden toteutukseen. Näitä ovat muun muassa paketti- suodatus-, tilatarkastus-, proxy-yhdyskäytävätekniikat/palvelintekniikat ja VPN-tekniikka sekä henkilökohtaiset palomuuriratkaisut. (Scarfone & Hoffman, 2009, ES-1 - ES-2.)

Lisäksi ohje käsittelee palomuurien sijoittamista verkkoarkkitehtuureihin ja palomuurisääntöjä. Ohje antaa ohjeita toimintapolitiikkaan ja käytettäviin liikennetyyppeihin ja pitää sisällään suosituksia edellä mainittuihin alueisiin. (Scarfone & Hoffman, 2009, ES-1 - ES-2.)

Ohjeessa on yleiskatsaus palomuurin suunnitteluun ja toteutukseen. Siinä on luettelo tekijöistä, jotka on huomioonotettava palomuuriratkaisuja valittaessa ja siinä on suosituksia palomuurien määrittämiseksi, testaamiseksi, käyttöönottamiseksi ja hallitsemiseksi. (Scarfone & Hoffman, 2009, ES-1 - ES-2.)

NIST Special Publication 800-48 Revision 1
Guide to Securing Legacy IEEE 802.11 Wireless Networks

Langattomia paikallisverkkoja (Wireless Local Area Networks, WLAN) käytetään yleensä laajentamaan langallisten verkkojen alueellista kattavuutta rajoitetulla toiminta-alueella. Tyypilliset käyttökohteet ovat rakennukset tai alueelliset toiminnalliset kokonaisuudet, joissa on mahdollista toteuttaa radioyhteyden muodostuminen. Perinteisesti käytetty WLAN-tekniikka perustuu

IEEE802.11 standardiin. Tämä dokumentti kiinnittää huomion perinteisesti käytetyn tekniikan ja uudemman IEEE802.11i turvallisuusstandardin välisiin eroihin. IEE801.11 standardin mukaan toimivat WLAN-yhteydet ovat alttiita tiedon saatavuuden, luotettavuuden ja eheyden menetyksille. Turvallisuuden rajoittuneisuus voi aiheuttaa luvattomiin kirjautumisiin organisaation tietojärjestelmiin ja -varantoihin, josta voi johtua tietojen korruptoituminen, tietoverkon kaistaleveyden pieneneminen ja verkon toiminnan rajoittuminen tai estyminen. Ongelmat voivat heijastua laajalle myös muihin järjestelmien verkkoihin yhteyksien kautta. (Scarfone, Dicoi, Sexton & Tibbs, 2008, ES-1 - ES-2.)

Organisaatioille, joilla on käytössään perinteisen tekniikan langattomia yhteyksiä, standardi suosittelee siirtymistä IEEE801.11i:n mukaisten ratkaisujen käyttöönottamiseen. (Scarfone ym., 2008, ES-1 - ES-2.)

Suositukset pitävät sisällään teknillisiä termejä ja niiden kuvauksia. Robust Security Networks (RSN) ja Robust Security Network Associations (RSNA) ovat keskeisempiä termejä. Kuvaukset käsittelevät termeihin liittyviä teknillisiä ominaisuuksia, kuten sanomarakenteita, sanomakättelymenettelyjä, avaimiston hallintaa sekä salauksen ja todentamisen keinoja. (Scarfone ym., 2008, 2-2 - 2-3.)

Ohjeen lopussa on 57-kohtainen tarkistuslista WLAN-yhteyden elinkaaren eri vaiheissa huomioonotettavista turvallisuusseikoista. Lista on hyödyllinen myös organisaatioille, joilla on jo operatiivisessa käytössä WLAN-yhteyksiä ja joiden tavoitteena on parantaa niiden turvallisuutta RSN:n periaatteiden mukaisesti. (Scarfone ym., 2008, 6-6.)

NIST Special Publication 800-125B
Secure Virtual Network Configuration for Virtual Machine (VM) Protection

Virtualisointi on yleistymässä teollisissa sovelluksissa sen mahdollistavien hyötyjen, kuten kustannussäästöjen, järjestelmän käytettävyyden varmistamisen ja joustavuutta lisäävien vaikutusten vuoksi. Nykytietotekniikka mahdollistaa virtuaalisoinnin käytön myös teollisuuden prosessiohjausjärjestelmissä ainakin osittain. Virtuaaliympäristöistä ja niiden virtuaalikoneista (Virtual Machines, VMs) on siten muodostumassa avainresursseja useisiin eri palveluihin, joten niiden kyberturvallisuuden huomioiminen on ensiarvoisen tärkeää. (Chandramouli, 2016, iii.)

NIST 800-125B ohjeistus kuvaa virtuaaliympäristön tietoteknillisiä ratkaisuja, niiden etuja ja haittoja. Ohjeen keskeisiä termejä ovat verkon segmentointi, verkkoyhteyksien redundanssi, VM:n suojaaminen käyttäen palomuuriliikenteen valvontaa ja VM-liikenteen monitorointi. Näiltä osin dokumentti antaa suosituksia turvallisuuskäytänteiden kehittämiseen. (Chandramouli, 2016, 1.)

Verkon segmentoinnin osalta ohjeessa on käsitelty viittä eri lähestymistapaa toteutuksen aikaansaamiseksi. Ensimmäisenä on eri suojaustason vaatimien virtuaalipalvelimien erottaminen toisistaan kytkimillä ja säätämällä verkkoliikennettä palomuurisäännöillä. Tämän jälkeen ohje pitää sisällään virtuaalikytkimien ja –palomuurien teknilliset ratkaisut. Segmentointia käsittelevässä osiossa on lisäksi kuvattu VLAN (Virtual Local Area Network, VLAN) tekniikkaa ja limittelyä virtuaaliverkkoratkaisuiksi. Ohje sisältää edellä mainittuihin asioihin liittyen viisi toimintasuositusta. (Chandramouli, 2016, 1.)

Verkkoyhteyksien redundanssia voidaan parantaa rakentamalla verkkokorteista ryhmiä, joissa on vähintään kaksi fyysistä liityntää. Tällöin toinen on toiminnassa ja toinen varmistaa yhteyden toimivuuden häiriötilanteessa. Yhteyksien hallintaperiaatteet ja –politiikat antavat lisämahdollisuuksia ryhmien laatimiseen ja sitä kautta suojauksen parantamiseen. Tähän liittyy ohjeessa kolme suositusta. (Chandramouli, 2016, 1 - 2.)

VM:n suojaaminen käyttäen palomuuriliikenteen valvontaa perustuu liikenteen valvontaan eri segmenttien väleillä tai segmenttien sisältämiin aliverkkoihin ja VM:stä sisään ja ulos suuntautuvaan liikenteeseen. Ohje pitää sisällään sekä fyysiset palomuuriratkaisut että virtuaalipalomuuriratkaisut etuineen ja haittoineen. Tähän osioon ohjeessa liittyy neljä suositusta. (Chandramouli, 2016, 1 - 2.)

VM-liikenteen monitorointi on tarkoitettu organisaation tiedon suojaamiseen tunnistamalla vahingollinen tai haitallinen liikenne, joka suuntautuu VM:iin tai sieltä ulos aiheuttaen hälytyksen tai suojaustoimenpiteet. Tarvittaessa monitorointi voi käynnistää liikenteen tallentamisen porttipeilauksella analysointitarpeisiin. Ohje suosittelee liikenteen molempien suuntien monitoroinnin. Toteutuksessa on mukana lisäksi kaksi muuta teknillistä suositusta. (Chandramouli, 2016, 1 - 2.)

3.7 Muu ohjeisto

NIST Special Publication 800-34 Rev. 1 (2010)
Contingency Planning Guide for Federal Information Systems

Tämä tietojärjestelmien valmiussuunnittelua käsittelevä dokumentti antaa ohjeita, suosituksia ja näkökohtia tietojärjestelmän ennakoimattoman toiminnan arviointiin ja siitä johtuvien toimenpiteiden suunnitteluun häiriöalttiissa kybertoimintaympäristössä. Organisaation selviytymiskykyä ennakoimattomissa häiriötilanteissa kutsutaan sen resilienssiksi. Se on nopea ja joustava kyky sopeutua ja toipua kaikista tunnetuista tai tuntemattomista muutoksista toimintaympäristössä. Suunnittelun tavoitteena on toiminta, jonka mahdollistaa keskeisten tehtävien suorittamisen häiriöiden aikana. Resilienssit organisaatiot pyrkivät sopeutumaan muutoksiin ja riskeihin, jotka voivat vaikuttaa heidän kykyynsä jatkaa toimintojaan. Ohje painottaa riskienhallinnan ja jatkuvuussuunnittelun yhteisvaikutusten tarpeellisuutta osana hätätilanteiden hallintaan valmistautumista. (Swanson, Bowen, Wohl, Gallup & Lynes, 2010, ES-1 - ES-2.)

Valmiussuunnitelmassa viitataan väliaikaisiin toimenpiteisiin tietojärjestelmäpalvelujen palauttamiseksi häiriötilanteista. Väliaikaisiin toimenpiteisiin voi sisältyä tietojärjestelmien ja toimintojen siirtäminen johonkin vaihtoehtoiseen sijaintipaikkaan, tietojärjestelmätoimintojen hyödyntäminen vaihtoehtoisella laitteella tai suorituskyvyn ylläpitäminen manuaalisilla menetelmillä. (Swanson ym., 2010, ES-1 - ES-2.)

Ohjeessa käsitellään erityistä varasuunnittelua koskevia suosituksia kolmelle alustatyypille ja ohje tarjoaa näille kaikille järjestelmille yhteiset strategiat ja tekniikat. Näitä ovat serverijärjestelmät, tietoliikennejärjestelmät ja tietokonejärjestelmät. (Swanson ym., 2010, ES-1 - ES-2.)

Ohje määrittää seitsemänvaiheisen valmiussuunnitteluprosessin, jonka avulla organisaatio voi kehittää ja ylläpitää elinkelpoista valmiussuunnitteluohjelmaa toimintaansa ajatellen. Nämä seitsemän vaihetta on tarkoitettu integroitavaksi edellä mainittujen IT-järjestelmien elinkaaren jokaiseen vaiheeseen. Vaiheet ovat:

1. Kehitä valmiussuunnitelmaperiaatteet. Tällöin toimintapolitiikka tarjoaa viranomaisten ohjeet ja muut ohjeet tehokkaan valmiussuunnitelman kehittämiseksi.
2. Suorita liiketoiminnan vaikutusten arviointi. Se auttaa tunnistamaan ja priorisoimaan tietoja, jotka ovat tärkeitä organisaation liiketoimintaprosessien tukemisessa. Toimenpiteet tarjoavat perustan jatkotoimenpiteille.
3. Tunnista häiriöitä ehkäisevä valvonta. Järjestelmähäiriöiden vähentämiseen tähtäävät toimenpiteet lisäävät kohdejärjestelmän toimivuutta ja siten vähentää katkoskustannuksia.
4. Luo varasuunnitelmia. Perusteelliset häiriöitä varten laaditut toipumisstrategiat varmistavat järjestelmän nopean ja tehokkaan toipumisen häiriötapahtuman jälkeen.
5. Kehitä tietojärjestelmän valmiussuunnitelma. Suunnitelmassa olisi oltava yksityiskohtaiset ohjeet ja menettelyt turvallisuuden kannalta ainutlaatuisen tiedon ja järjestelmähäiriön palauttamiseksi.
6. Varmista suunnitelman testaamalla, kouluttamalla ja harjoittelemalla. Testaus vahvistaa palautumisominaisuudet, kun taas koulutus valmistelee henkilöstöä suunnitelman aktivoimiseksi ja suunnitelman käyttämiseksi. Harjoitustoiminta parantaa suunnitelman tehokkuutta ja koko organisaation varautumista.
7. Varmista suunnitelman ylläpito. Suunnitelman tulisi olla jatkuvasti ylläpidettävä asiakirja. Sitä tulee päivittää säännöllisesti huomioiden tapahtuneet järjestelmäkehitykset ja organisaatiomuutokset.

Asiakirja on perusteellinen ja loogisesti etenevä ohje hyödynnettäväksi organisaation valmiussuunnitelman kehittämisessä. Siinä on erityisesti huomioitu organisaation tarpeiden arviointi ja sen resilienssin kehittäminen. Ohjeessa on aluksi taustoitettu valmiussuunnittelua mukaan lukien erilaisten turvallisuus- ja hätätilanteiden hallintaan liittyvien suunnitelmien vaikutus organisaation kokonaisresilienssiin, riskienhallintakehyksen (RMF) hyödyntäminen ja ohjeen FIPS199 vaikutustasojen huomioiminen. Tietojärjestelmän ennakoimattoman toiminnan suunnitteluprosessi pitää sisällään perussuunnitelmat, jotka ovat välttämättömiä tehokkaan valmiusominaisuuden kehittämiseksi. Tällä on vaikutuksia kaikkiin suunnittelujaksoihin, mukaan lukien liiketoiminnan vaikutusten arviointi, vaihtoehtoinen ratkaisujen valinta ja niiden hyödyntämisstrategiat. Suunnitelmassa käsitellään myös henkilökunnan yhteisiä tehtäviä ja vastuita. Tietojärjestelmän varasuunnitelman kehittäminen, ylläpito, testaus, koulutus ja harjoittelu ovat myös kuvattuina. Tekniset varautumissuunnitteluun liittyvät näkökohdat on käsitelty edellä lueteltuja kolmea järjestelmätyyppiä koskien. Se auttaa valmiussuunnittelijoita tunnistamaan, valitsemaan ja toteuttamaan asianmukaiset tekniset valmiudet. (Swanson ym., 2010, ES-1 - ES-2.)

NIST Special Publication 800-150 (Draft) (2016)
Guide to Cyber Threat Information Sharing

Kyberturvallisuuden ylläpitämisessä organisaatioiden välinen ja organisaation sisäinen uhkatiedon vaihto on eräs keskeisimmistä toimenpiteistä. Erityisesti yritysten keskinäinen yhteistyö esimerkiksi oman toimialansa sisällä on hyödyllinen toimintamalli kyberturvallisuuden kehittämiseksi jokaisessa toimintaan osallistuvassa yrityksessä ja koko toimialan sisällä. Yhteistyö mahdollistaa resurssien

jakamisen sekä alueen yleisen tietotason kehittymisen kokemusten ja erilaisten kyvykkyyksien hyödyntämisen kautta. Yrityksen proaktiivinen toimintakyky kehittyy yhteistoiminnan seurauksena. Lisäksi yhteistoimintamallit kyberturvallisuuden eri toimijoiden kanssa, kuten erityisesti kansallisen CERT-organisaation kanssa, tuovat merkittäviä etuja yrityksille turvallisuustilannetietoisuuden parantamiseksi ja toimintansa hallitsemiseksi toimintaympäristönsä kyberturvallisuusriskien osalta. Yleisesti ottaen yhteistyö auttaa kehittämään turvallista, vastuullista ja tehokasta tiedonvaihtoa siihen osallistuvien tahojen kesken. (Johnson, Badger, Waltermire, Snyder & Skorupka, 2016, 2 - 3.)

Kyseessä olevaa ohjeluonnosta voi pitää peruskonseptina ja sisältöluettelona kehitettäessä edellä mainittua yhteistoimintaa. Ohje pitää sisällään tietoa kyberuhkatyypeistä ja teknologioista huomioiden tiedon jakamisen hyödyt ja haasteet. Organisaatiot voivat hyödyntää ohjetta suunnitellessaan ja toteuttaessaan yhteistoimintaa eri tahojen kanssa. (Johnson ym., 2016, 2 - 3.)

Yhteistoiminnassa käsiteltäviksi aiheiksi ja tiedonvaihtoalueiksi ohje suosittelee uhkiin liittyvistä toimijoista saatavat indikaatiot, havaitut toimintataktiikat, käytetyt tekniikat ja proseduurit sekä CERT-organisaation turvallisuushälytystiedot. Indikaatiot voivat muodostua epäilyttävistä IP-osoitteista ja nimipalvelimista tai verkko-osoitteista, jotka viittaavat haitallisiin sisältöihin. Organisaatioiden yhteistoiminta voi olla erityisen hyödyllistä vaihdettaessa kokemustietoja erilaisten työkalujen ja mekanismien käytöstä, kun on jouduttu ratkomaan kohdalle sattuneita haastavia kyberturvallisuuden uhkatilanteita. (Johnson ym., 2016, 2 - 3.)

Ohje auttaa esimerkiksi asettamaan yhteistyölle tavoitteita, tavoitteiden priorisointia sekä kehittämään uhkatietolähteiden hyödyntämistä, tiedonjakokäytänteitä ja yhteistyöosaamista.

Ohjeesta löytyvät seuraavat neljä aihekokonaisuutta:

1. Yleiskuvaus organisaation kyberturvallisuutta uhkaavien haitallisten tapahtumien koordinoinnista ja niihin liittyvistä tiedonvaihtotarpeista sekä organisaation haasteista käynnistettäessä tiedonvaihtoon liittyviä prosesseja. Lisäksi osio pitää sisällään kuvaukset tiedonvaihdon ja haitallisten tapahtumien koordinoinnin peruskonsepteista, kuten kyberhyökkäyksen elinkaari, uhkatiedustelu, tiedon vaihdon rakenne sekä viralliset ja epäviralliset tiedonvaihdon yhteisöt.

2. Välittömien kyberturvallisuuskykyjen tarpeellisuuden tunnistaminen. Kyvykäs organisaatio kykenee tehokkaasti osallistumaan yhteistyöhön muiden organisaatioiden kanssa haitallisten tapahtumien selvittämisessä tarvittavaan koordinaatioon ja uhkatiedon jakamiseen. Lisäksi yksittäisen organisaation tulee voida toteuttaa toimintansa itsearviointia, havaitsemaan puutteita toiminnassaan ja kehittämään kyberturvallisuuttaan toiminnan jatkuvan parantamisen keinoja hyväksi käyttäen.

3. Avainkykyjen tunnistaminen toteutettaessa haitallisten tapahtumien koordinointi- ja tiedonjakokykyjä. Toimenpiteet voidaan ryhmitellä seuraavasti: tiedonvaihdon suhteiden luonti, toimintaan osallistuminen ja toiminnan ylläpitäminen. Lisäksi aihekokonaisuus pitää sisällään ohjeistuksen siitä, miten varmistetaan tiedonjakoprosessin jatkuvuus ja elinkaari.

4. Viimeinen asiakokonaisuus pitää sisällään yleiset suositukset toiminnan toteutuksesta.

Ohjeen liitteessä A on kuvattu useita tyypillisiä skenaarioita, joilla voidaan parantaa organisaation kyberturvallisuutta uhkaavien haitallisten tapahtumien käsittelyä hyödyntäen erilaisia tiedonvaihtomekanismeja. Näitä skenaarioita ovat: kansallinen tiedonvaihto haittaohjelmahyökkäyksistä tiettyyn teollisuussektoriin, kampanja-analyysit, palvelunestohyökkäykset tiettyyn teollisuussektoriin, sähköpostikalastelun torjunta yhteistyöllä, palvelinongelmien ratkaisu liikekumppanien yhteistyöllä, CERT-yhteistyö ja luottokorttivarkaudet. (Johnson ym., 2016, 27 - 29.)

NIST Special Publication 800-160 (Second Public Draft) (2016)
Systems Security Engineering

Tietoteknisten järjestelmien kyberturvallisuuden luominen lähtee järjestelmäsuunnittelusta, jonka jälkeen turvallisuuteen tähtääviä toimenpiteitä tulee toteuttaa koko järjestelmän elinkaaren ajan. (Ross, McEvilley & Oren, 2016, 1 - 2.)

Tämä järjestelmäsuunnittelun turvallisuutta käsittelevä ohje on tarkoitettu käytettäväksi yhdessä kansainvälisen ohjelmistosuunnittelua koskevan ISO/IEC/IEEE 15288 standardin kanssa. Ohjetta suositellaan käytettäväksi sellaisenaan tai sovellettuna kyberturvallisuuden suunnitteluprosessiin niin, että sen suosittelemat toimenpiteet ulottuvat kaikilta osiltaan järjestelmän koko elinkaaren kattavaan suunnitteluun. (Ross ym., 2016, 5 - 6.)

Ohje antaa järjestelmäsuunnittelun perustiedot tavoiteltaessa mahdollisimman korkeaa toiminnan luotettavuutta tämän päivän kybertoimintaympäristössä. Luotettavuuden varmistaminen tässä yhteydessä tarkoittaa kaikkia niitä toimenpiteitä, jotka täyttävät kattavat kriittiset vaatimukset järjestelmän sisältämille komponenteille, alijärjestelmille, pääjärjestelmille, tiedonsiirtoverkoille, ohjelmistosovelluksille ja koko käyttöorganisaatiolle. Vaatimukset voivat pitää sisällään esimerkiksi turvallisuus- ja luotettavuusvaatimuksia, riippuvuussuhteita, toimintaan liittyviä vaatimuksia sekä sietokyky- ja selviytymiskykyvaatimuksia laajassa mitassa potentiaalisia häiriöitä ja uhkia vastaan. Luotettavuuden varmistukseen liittyvät tehokkaat toimenpiteet edellyttävät vaatimusten riittävää täyttämistä ja hyvin suunniteltuja toimenpiteitä. Järjestelmän kyberturvallisuuden suunnittelussa on tällöin kyse seuraavien toimenpiteiden yhdistelmästä: hyvä perussuunnittelu, siihen liitetyt turvallisuusperiaatteet, konseptit ja tekniikat järjestelmän elinkaaren jokaisessa vaiheessa konseptisuunnittelusta aina käytöstä poistoon asti. (Ross ym., 2016, 5 - 7.)

Mikään suunnitteluprosessi ei mahdollista järjestelmän ehdottoman turvallisuuden saavuttamista, vaan epävarmuutta joudutaan jokaisessa suunnittelukohteessa olevassa järjestelmässä sietämään. Järjestelmähankinnan yhteydessä onkin huomioitava epävarmuus, joka välttämättä jää tavoitteiden ja toteutuksen väliseksi ristiriidaksi. Turvallisuussuunnittelun tavoite tuleekin määritellä siten, että erilaiset rajoitteet ja välttämättömät suunnitteluperusteet ohjaavat turvallisuuden näkökulmasta tarkasteltuna tarkoituksen mukaisen järjestelmäkokonaisuuden aikaansaamiseen. Tällöin se on optimissaan sekä aktiivisen että passiivisen suojautumisen muodostama yhdistelmä, joka pitää sisällään järjestelmän elinkaaren kaikki vaiheet ja kaikki kyberturvallisuuden asteet (normaalitilanne, epävarmuus, vajaatoiminta ja palautuminen). Tarkoituksenmukaisuus voidaan määritellä kompromissiksi seuraavien ominaisuuksien välillä: suunniteltavan järjestelmän turvallisuuden varmistaminen, sen suorituskykyisyys ja sen tehokkuus estävät suunnittelemattomien toimintojen ja toimintarajoitteiden esiintyminen järjestelmässä. Tarkoituksenmukaisuutta ohjaa lopulta

hankintaspesifikaatio, jonka kohteista ja niiden priorisoinnista vastaavat hankevastuussa olevat sidosryhmät turvallisuuteen liittyvien tavoitteiden ja vaatimusten kautta. (Ross ym., 2016, 8 - 9.)

Aktiivinen suojautuminen pitää sisällään systeemiominaisuuden/toiminnallisuuden ja suorituskyvyn määrittelyt. Tällöin korostuvat ehdottomat vaatimukset järjestelmän käytölle, hyödyntämiselle ja vuorovaikutukselle teknologioiden/laitteiden, toimintaympäristön, ihmisten ja fyysisten systeemielementtien muodostamassa kokonaisuudessa. (Ross ym., 2016, 14.)

Passiivinen suojautuminen puolestaan mahdollistaa sekä aktiivisen suojauksen että järjestelmän yleisen toiminnallisuuden niin toteutukseltaan kuin rakenteeltaankin. Se pitää sisällään järjestelmäarkkitehtuurin ja -suunnittelun sekä säännöt jotka ohjaavat järjestelmän käyttöä, vuorovaikutussuhteita ja toiminnallista hyödyntämistä. (Ross ym., 2016, 14.)

Ohjeen tarkoitus on

- luoda pohja IT-järjestelmän käyttöönotolle sisältäen periaatteet, käsitteet ja toiminnot,
- edistää yhteistä ajattelutapaa järjestelmän turvallisuuden takaamiseksi riippumatta sen laajuudesta, koosta, monimutkaisuudesta tai järjestelmän elinkaaren vaiheesta,
- tarjota näkökulmia ja osoittaa, miten järjestelmätekniikan turvallisuusperiaatteita, konsepteja ja toimintoja voidaan tehokkaasti soveltaa järjestelmien suunnitteluprosesseihin,
- edistää järjestelmien turvallisuustekniikkaa julkaisemalla sen soveltamiseksi toimenpiteitä, tutkimustietoa ja
- antaa perusteita henkilöstön koulutukseen ja koulutusohjelmien kehittämiseen, mukaan lukien yksittäisten sertifikaattien ja muiden ammatillisten arviointiperusteiden kehittäminen.

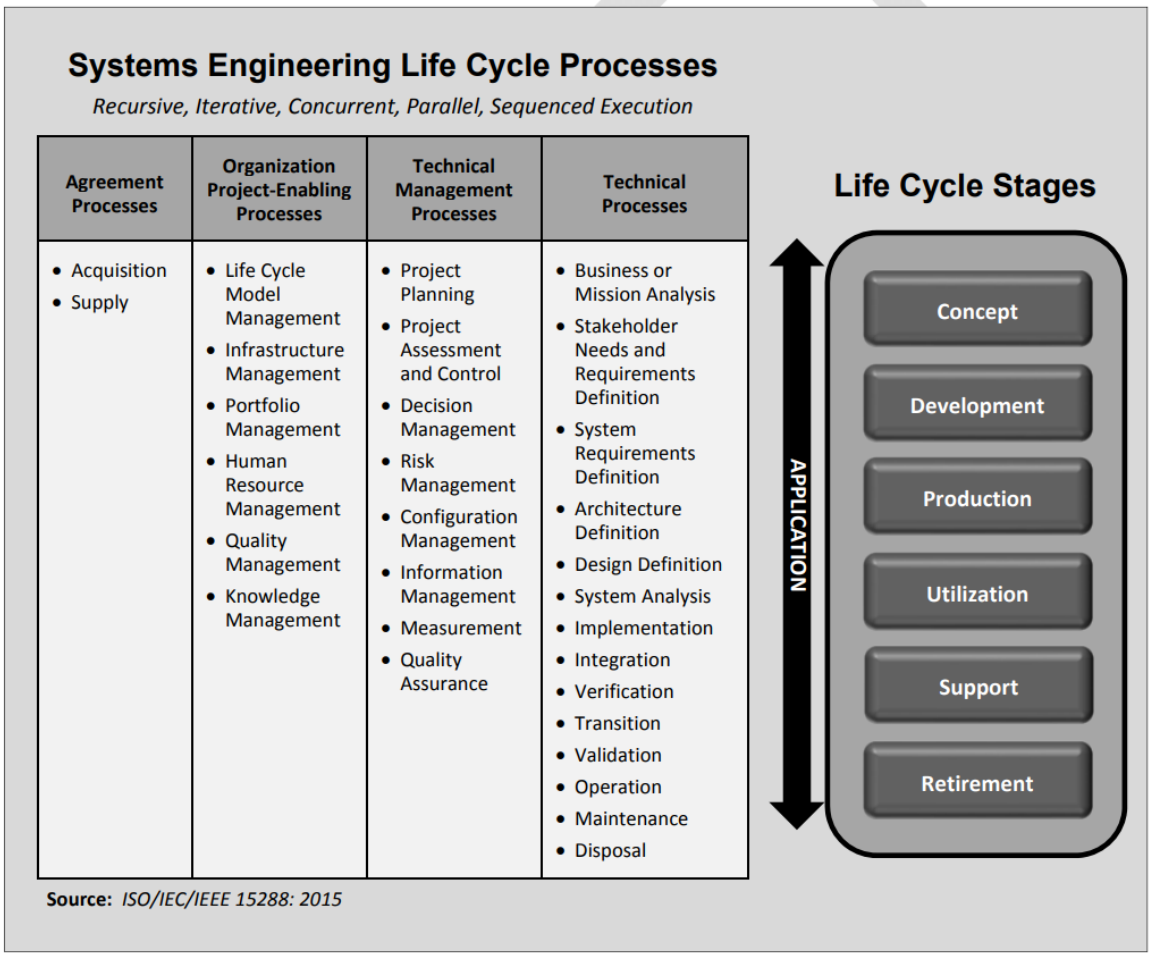
Järjestelmien turvallisuustekniikan voidaan soveltaa jokaisen järjestelmän elinkaaren eri vaiheessa. Turvallisuussuunnittelussa järjestelmätyypit tai elinkaarivaiheet voivat olla seuraavat (Ross ym., 2016, 1 - 2.):

- uudet järjestelmät
- toiminnalliset muutokset järjestelmiin
- suunnitellut päivitykset toimiville järjestelmille samalla kun ylläpidetään päivittäisiä toimintoja
- suunnitellut päivitykset järjestelmiin, jotka johtavat uusiin järjestelmiin
- ketterät järjestelmät
- System-of-Systems (SOS)
- käytöstä poistuvat järjestelmät

Järjestelmäsuunnitteluprosessit puolestaan voivat olla seuraavat:

- sopimuksellinen prosessi
- organisaationallinen projektin mahdollistava prosessi
- teknillinen hallintaprosessi
- teknillinen prosessi

Kuviossa 14 edellä mainitut prosessit on avattu yleisellä tasolla ja sidottu järjestelmien elinkaarivaiheisiin. (Ross ym., 2016, 23.)



KUVIO 14. Järjestelmäsuunnittelun prosessit ja järjestelmien elinkaaret (Ross ym., 2016, 23)

Ohjeessa on omana lukunaan kuvattu turvallisuustekniikan ja suojaustarpeiden näkökulmista katsottuna järjestelmien perusrakenteet, järjestelmäelementit niiden toimintaympäristössä huomioiden turvallisuuden merkitys, turvallisuusarkkitehtuuri, luotettavuus ja varmuus. Ohjeessa kuvataan myös laajasti järjestelmien turvallisuustekniset näkökohdat yleisesti määriteltyihin järjestelmien suunnitteluprosesseihin ja standardeihin sidottuina. Ohjeistuksessa on esitetty tietoturvaparannuksia, jotka lisäävät tai laajentavat tarkasteluprosessin tuloksia, toimintoja ja tehtäviä. Parannetut suunnitteluprosessit koskevat toimenpiteitä koko järjestelmän elinkaaren ajan. (Ross ym., 2016, 23 - 151.)

Ohje sisältää laajan liitekokonaisuuden muun sisällön käytännön soveltamisen tueksi.

NIST Special Publication 800-115 (2008)
Technical Guide to Information Security Testing and Assessment

Organisaation oman informaatioturvallisuuden tilannekuvan muodostamisen yksi ulottuvuus on käyttöön soveltuvien testaus ja arviointimenetelmien hyödyntäminen. Se on useiden eri prosessien kokonaisuus, joiden avulla pyritään määrittämään organisaation resurssien (järjestelmät, verkot, toimintaproseduurit, henkilöstö) kyky täyttää niille asetetut turvallisuustavoitteet. Prosessit koostuvat tyypillisesti kolmesta eri menetelmästä, jotka ovat testaaminen, tutkiminen ja haastattelu. Testaaminen on kohteiden toiminnan spesifikaatioiden täyttymisen todentamista. Tutkiminen koostuu kohteen havainnoinnista, tarkastuksista, katselmoinneista tai analysoinneista. Toimenpiteillä pyritään ymmärtämään tai selkeyttämään kohteen toimintaa tai saaman todisteita jostakin sen toiminnasta. Haastattelu voi kohdistua yksittäisiin henkilöihin tai toiminallisiin ryhmiin. Haastatteluihin liittyvien keskustelujen avulla pyritään muodostamaan käsitys turvallisuustilanteesta, selkeyttämään sitä ja paikallistamaan kehitystarpeita. Jokainen prosessikokonaisuus palvelee organisaation mahdollisuuksia toteuttaa tehokasta ja tarkoituksenmukaista turvallisuusvarmistusta. (Scarfone, Souppaya, Cody & Orebaugh, 2008, ES-1 - ES-2.)

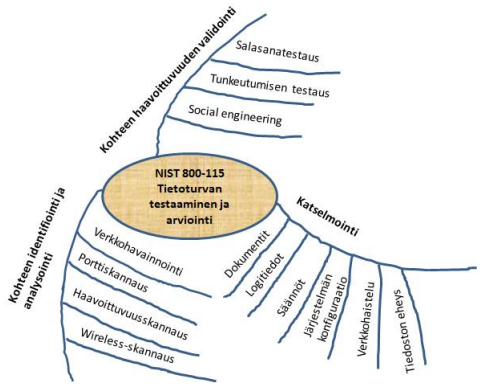
Informaatioturvallisuuden arvioinnin perusteena olevien testaus- ja tutkimusmenetelmien onnistumiseksi ohje suosittelee organisaatiolle seuraavia toimenpiteitä:

- informaatioturvallisuuden arviointipolitiikan luominen
- toistettavan ja dokumentoitavan arviointimenetelmän käyttöönotto
- arviointitapahtuman kohteiden määrittäminen
- tulosten analysointi, heikkouksien osoittamien ja riskien pienentäminen

Ohje pitää sisällään seuraavat kolme arvioinnin pääperiaatetta ja niihin liittyviä testaus- ja tarkastustekniikoita:

- katselmointi ja siihen liittyvät tekniikat
  - järjestelmien, sovellusten, verkkojen, toimintapolitiikkojen ja –menetelmien arviointi
- kohteen identifiointi ja analysointi ja niihin liittyvät tekniikat
  - järjestelmien, porttien ja palvelujen haavoittuvuuksien testaaminen
- kohteen haavoittuvuuden validointi ja siihen liittyvät tekniikat
  - haavoittuvuuksien paikallistaminen

Kuviossa 15 on esitetty informaatioturvallisuuden arvioinnin kolme pääperiaatetta ja niihin liittyvät tekniikat. (Scarfone ym., 2008, 1-1 - 1-2.)



KUVIO 15. Informaatioturvallisuuden arvioinnin kolme pääperiaatetta (Scarfone ym., 2008, 1-1 - 1-2)

Kuviossa 15 on informaatioturvallisuuden arvioinnin kolme pääperiaatetta ja niihin liittyvät tekniikat. Ohje pitää sisällään myös seuraavat käytännön ohjeet onnistuneen informaatioturvallisuuden arvioinnin suorittamiseksi:

- Toteutuksen suunnittelun osa-alueet, kuten arviointipolitiikka, toimenpiteiden priorisointi, aikataulutus, valinta ja looginen käsittely. Lisäksi se pitää sisällään hahmotelman arviointiin liittyvistä oikeudellista näkökohdista, jotka organisaation tulee tarvittaessa huomioida.
- Toteutukseen liittyvät seikat, kuten toimenpiteiden koordinointi, itse toimenpiteiden suorittaminen organisaatioympäristössä, tulosten analysointi ja erilaiset datan käsittelyyn liittyvät huomiot.
- Toteutuksen jälkeiset toimenpiteet, kuten havaittuja ongelmia lieventävät suositukset ja tulosten raportointi.

Liitteissä ovat esimerkit testaus- ja tutkimusmenetelmistä. Ne auttavat organisaatioita sovellusohjelmistojen ja etäkäyttöjen haavoittuvuuksien selvittämisessä. (Scarfone ym., 2008, A-1 - G-3.)

Sovellusohjelmistojen testaustoimenpiteet ovat tehokkainta suorittaa heti tuotteen ohjelmiston kehitysvaiheessa. Niihin kohdistuvista hyökkäysvektoreista ovat esimerkkeinä muun muassa eri muotoiset tietovarkaudet, luvattomat hallintamenettelyt ja palvelunestohyökkäykset. Sovellusohjelmistojen turvatestaamiseen voidaan käyttää useita menetelmiä, joista esimerkkeinä ohjeessa ovat white- ja black box-testit, niiden yhdistelmä gray box-testi ja testeihin liittyvät yleiset ominaisuudet. (Scarfone ym., 2008, C-1.)

Etäkäytön toimivuuden testimetodit liittyvät haavoittuvuuksiin, jotka esiintyvät päätepalvelimissa, VPN-tekniikassa, SSH-tunneloinnissa, erillistietokoneissa ja modeemeissa. Etäkäytön testaaminen voidaan suoritta osana tunkeutumisen eston testausta, mutta erikseen toteutettuna testi voidaan keskittää osatestausta paremmin etäkäyttötoteutuksiin. Yleisesti käytetyt testaustekniikat ovat: luvattomien etäpalvelujen tunnistaminen porttiskannauksella, sääntöjen katselmointi luvattomien etäyhteyksien estämiseksi (konfiguraation katselmointi), etäyhteyksien pääsyoikeuksien testaaminen salasanatestauksella ja etäyhteyksien kommunikoinnin monitorointi verkkonuuskinnalla. (Scarfone ym., 2008, D-1.)

Lisäksi liitteenä on työkalusuosituksia katselmointiin, kohteen identifiointiin ja analysointiin sekä kohteen haavoittuvuuden validointiin. (Scarfone ym., 2008, A-1 - G-3.)

Lähteet

Chandramouli, R., Garfinkel, S., Nightingale, S. & Rose, S. (2016). Trustworthy Email. NIST Special Publication 800-177. Saatavilla: 23.7.2017
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-177.pdf

Chandramouli, R. (2016). Secure Virtual Network Configuration for Virtual Machine (VM) Protection. NIST Special Publication 800-125B. Saatavilla: 23.7.2017
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-125b.pdf

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. (2006). Minimum Security Requirements for Federal Information and Information Systems and Information Systems. Saatavilla: 18.7.2017
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. (2004). Standards for Security Categorization of Federal Information and Information Systems. Saatavilla: 18.7.2017 https://citadel-information.com/wp-content/uploads/2012/08/FIPS-PUB-199-final.pdf

Cooper, D., Polk, W., Regenscheid, A. & Souppaya, M. (2011). BIOS Protection Guidelines. Special Publication 800-147. Saatavilla: 18.7.2017
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf

Department of Defense. (2017). Department of Defense Instruction. DoDI 8510.01. Saatavilla: 18.7.2017
http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf?ver=2017-07-28-134447-703

Gilsinn, J. (2008). Establishing an Industrial Automation and Control Systems Security Program – An Overview of ISA-99.02.01 ISA EXPO 2008. Saatavilla: 18.7.2017
http://www.controlglobal.com/assets/Media/0811/Gilsinn_ISA-99.02.01.pdf

Huoltovarmuuskeskus. (2015). Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen vuonna 2014. KYBER-TEO 2014 -hankkeen tuloksia. Saatavilla: 18.7.2017
https://www.vtt.fi/inf/pdf/technology/2017/T298.pdf

International Organization for Standardization. International Organization for Standardization - When the world agrees.
Saatavilla: 18.7.2017 https://www.iso.org/home.html

Johnson, C., Badger, L., Waltermire, D., Snyder, J. & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150. Saatavilla: 23.7.2017 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf

Knowles, W., Prince, D., Hutchison, D., Ferdinand, J., Disso, J.F.P. & Jones, K. (2015). A, survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection 9*.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/201. Saatavilla: 18.7.2017 https://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0

National Institute of Standards and Technology. (2010). Guide for Applying the Risk Management Framework to Federal Information Systems - A Security Life Cycle Approach. Saatavilla: 23.7.2017 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf

National Institute of Standards and Technology. (2011). Information security. Guide for Conducting Risk Assessments. Saatavilla: 23.7.2017 https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=908030

National Institute of Standards and Technology. (2012). Information security. Guide for Conducting Risk Assessments. Saatavilla: 23.7.2017 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

Puolustusministeriö. (2015). KATAKRI – Kansallinen turvallisuusauditointikriteeristö. PowerPoint-esitys. Saatavilla: 18.7.2017 http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Regenscheid, A. (2014). BIOS Protection Guidelines for Servers. NIST Special Publication 800-147B. Saatavilla: 23.7.2017 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-147b.pdf

Ross, R., McEvilley, M. & Oren, J.C. (2016). Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. NIST Special Publication (SP) 800-160. Saatavilla: 23.7.2017 https://csrc.nist.gov/csrc/media/publications/sp/800-160/archive/2016-05-04/documents/sp800_160_second-draft.pdf

Scarfone, K., Dicoi, D., Sexton, M. & Tibbs, C. (2008). Guide to Securing Legacy IEEE 802.11 Wireless Networks. Special Publication 800-48 Revision 1. Saatavilla: 23.7.2017 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-48r1.pdf

Scarfone, K. & Hoffman, P. (2009). Guidelines on Firewalls and Firewall Policy. Special Publication 800-41 Revision 1. Saatavilla: 23.7.2017
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

Scarfone, K., Souppaya, M., Cody. A. & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment. Special Publication 800-115. Saatavilla: 23.7.2017
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. & Hahn, A. (2015). Guide to industrial control systems (ICS) security. NIST Special Publication 800-82 Revision 2. Saatavilla: 18.7.2017
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

Suomen Standardisoimisliitto SFS ry. (2013). SFS Käsikirja 631-3: Automaatio. Osa 3: Tietoturvallisuus. SFS ry, Helsinki.

Suomen Standardisoimisliitto ry. (2012). SFS-käsikirja ISO27001. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. SFS ry, Helsinki.

Suomen Standardisoimisliitto SFS ry. Standardi tutuksi. Saatavilla: 18.7.2017
http://www.sfs.fi/julkaisut_ja_palvelut/standardi_tutuksi

Suomen Standardisoimisliitto SFS ry. (2015). Tietoturvallisuuden hallintajärjestelmät. ISO/IEC 27000 -standardiperhe- diasarja oppilaitoksille. Saatavilla: 18.7.2017
https://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_iec_27000_tietoturvallisuuden_hallinta

Swanson, M., Bowen, P., Wohl, A., Gallup, D. & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems. NIST Special Publication 800-34 Rev. 1. Saatavilla: 23.7.2017
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf

Valtionvarainministeriö. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivusto. Valtionvarainministeriön internetsivusto. Saatavilla: 18.7.2017
https://www.vahtiohje.fi/web/guest/home

Informaatioteknologian tiedekunnan julkaisuja
No. 55/2018

ISBN 978-951-39-7541-8 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO