Tiedonhallintalautakunta
Informationshanteringsnämnden

Koulutus: Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)

17.8.2022

Saavutettava

Julkri-koulutuksen sisältö

- Taustaa
- Kriteeristön sisältö ja rakenne
- Luokittelu, riskilähtöisyys ja kriteerien soveltaminen
- Julkri-työkalun käyttö
- Käyttötapaukset
- Tukimateriaaleja

Taustaa

Taustaa Julkrille

- Oli selkeä tarve Katakria laajemmalle ja myös Pitukrin näkökulmia sisältävälle kriteeristölle.
- Keskeisin ero Katakriin ja Pitukriin verrattuna on laajuus
  - Julkri sisältää turvallisuusluokitellun tiedon turvaamisen kriteerien lisäksi sekä julkisen että salassa pidettävän tiedon sekä varautumisen ja jatkuvuuden hallinnan sekä tietosuojan kriteereitä.
- Kriteeristö on laadittu Tiedonhallintalautakunnan alaisessa tietoturvallisuusjaostossa yhteistyössä Tietosuojavaltuutetun toimiston kanssa.

Julkrin hyödyt

- Kriteeristö tukee organisaation riskilähtöistä turvallisuusjohtamista
- Julkria voi hyödyntää lainmukaisuuden arvioinnissa ja osana tietosuoja-asetuksen mukaista osoitusvelvollisuutta
- Tukee koko julkishallinnon tietoturvan kehittämisen ja arvioinnin tarpeita
- Käyttötapaukset helpottavat kriteeristön tilannekohtaista soveltamista
- Excel-työkalu helpottaa kriteeristön käyttöä

Julkrin käyttökohteet

- Organisaatio voi käyttää Julkria esimerkiksi:
  - organisaation tai sen osan tietoturvallisuuden arvioinnissa
  - palveluun tai sen toimittajaan kohdistettavien tietoturvavaatimusten tunnistamisessa
  - palvelun arvioinnissa suhteessa hankinnan ja palvelusopimuksen vaatimuksiin
  - tietosuojaa koskevien vaatimusten toteutumisen arvioinnissa
- **Huom!**
  - **Sovellettavat kriteerit tulee aina valita tapauskohtaisesti**
  - **Julkri ei sovellu vaatimusmäärittelyksi, mutta valittuja kriteereitä voi hyödyntää vaatimusmäärittelyn osana**

Julkrin taustalla oleva lainsäädäntö ja suositukset

- Laki julkisen hallinnon tiedonhallinnasta (TihL) (906/2019)
  - Valtioneuvoston asetus turvallisuusluokittelusta (1101/2019)
- Laki viranomaisen toiminnan julkisuudesta (621/1999)
- EU:n yleinen tietosuoja-asetus ((EU) 2016/679)
  - Tietosuojalaki (1050/2018)
- Ja lisäksi muita tiedonhallintalautakunnan suosituksia ja standardeja kuten ISO/IEC 27002, SFS-EN ISO/IEC 27001:2017, SFS-EN ISO/IEC 27005:2018 ja SFS ISO 31000:2018

Julkrissa on huomioitu tiedonhallintalaista tulevat tietoturvallisuuden velvoitteet

- Tiedonhallintalaissa on säädetty tietoturvallisuustoimenpiteisiin liittyviä vaatimuksia ja vastuita
  - Tietoturvallisuustoimenpiteiden vähimmäistaso
  - Velvollisuus seurata toimintaympäristön tilaa, velvollisuus varmistua tietoaineistojen ja tietojärjestelmien turvallisuudesta koko niiden elinkaaren ajan
  - On tunnistettava olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti
  - Hankittavaan tietojärjestelmään on toteutettava asianmukaiset tietoturvallisuustoimenpiteet

Niinpä…

- Julkri on suositus ja lainsäädännön vaatimukset voidaan täyttää myös muulla kuin kriteereissä kuvatulla tavalla, mutta
- kriteeristöä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä. Kuitenkin,
- jos organisaatio tarvitsee todistuksen Julkri-kriteeristöön perustuvasta vaatimuksenmukaisuudesta, niin kaikkien arviointiin sisältyvien kriteerien tulee toteutua arvioinnin kohteessa.
- Jos kriteerin toteuttaminen ei kuitenkaan ole mahdollista, on yksilöitävä ja perusteltava kompensoivat menettelyt, joilla varmistetaan, että riski on hyväksyttävällä tasolla kriteerin toteuttamatta jättämisestä huolimatta

Rajaukset

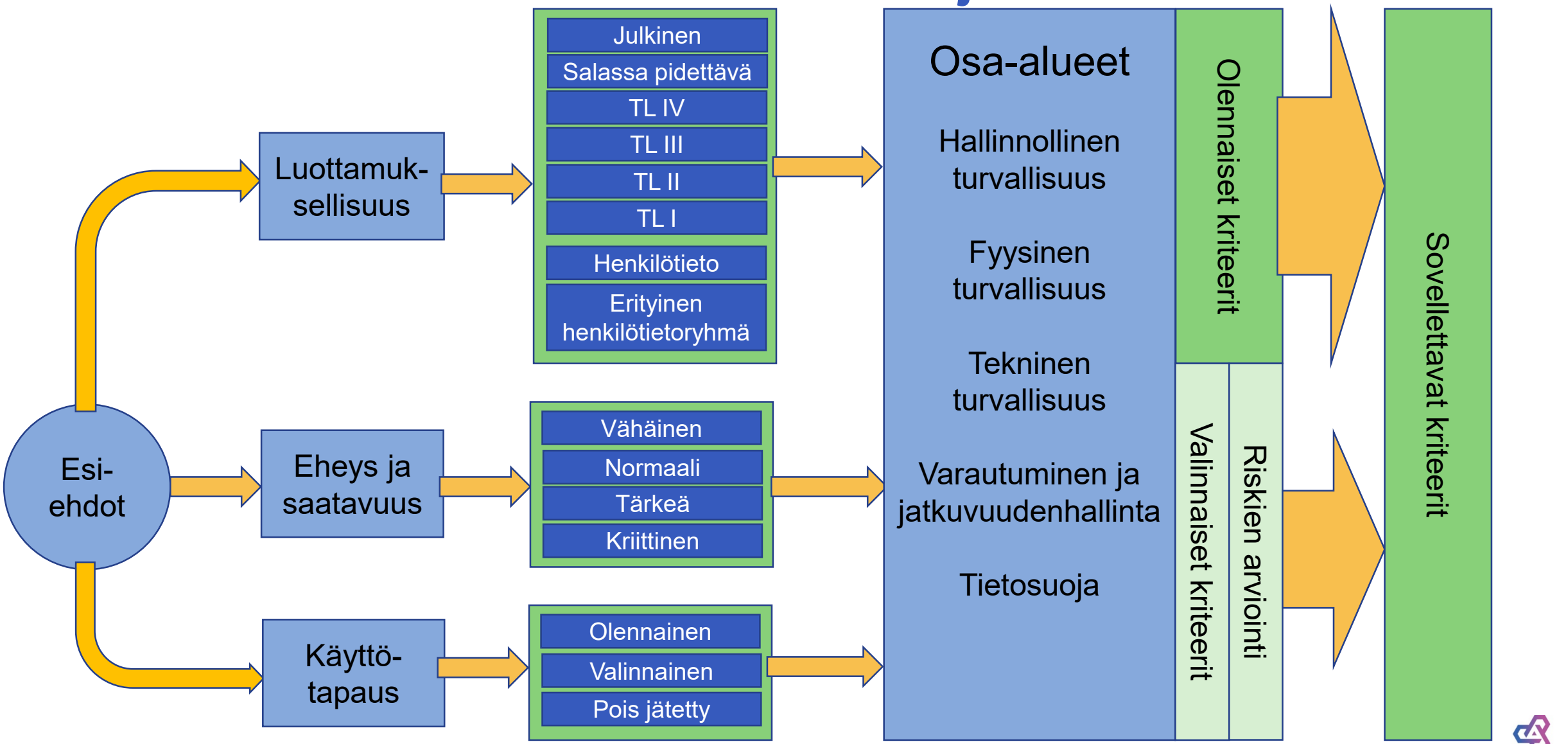
- Julkri ei sisällä
  - Toimialakohtaisen erityislainsäädäntöön perustuvia kriteerejä
  - Yksityiskohtaisia saavutettavuuden arviointia koskevia kriteereitä
  - Kansainvälisen turvallisuusluokitellun tiedon tietoturvallisuuden arviointiin liittyviä kriteerejä
  - Valmiuslain piiriin kuuluvia toiminnan jatkuvuutta poikkeusoloissa koskevia kriteerejä

Kriteeristön sisältö ja rakenne

Julkrin osa-alueet

- Hallinnollinen turvallisuus (HAL) kattaa yleisiä hallinnollisen turvallisuuden, henkilöstöturvallisuuden, tietojärjestelmien ja niiden hankinnan sekä käyttöturvallisuuden kriteereitä. (kriteereitä 36)
- Fyysisen turvallisuuden (FYY) osa-alue sisältää luvattoman tietoihin pääsyn estäviä ja rajoittavia kriteereitä, mitkä liittyvät toimitiloihin ja säilytysratkaisuihin. (kriteereitä 42)
- Tekninen turvallisuus (TEK) kattaa tietojärjestelmien ja tietoliikenneyhteyksien teknisiin ominaisuuksiin, turvalliseen käyttöön ja toimintamalleihin liittyvät kriteerit. (kriteereitä 97)
- Varautumisen ja jatkuvuudenhallinnan (VAR) osa-alue koostuu normaaliolojen varautumista ja jatkuvuudenhallintaa koskevia kriteereitä. (kriteereitä 12)
- Tietosuoja-osa-alueelle (TSU) on koottu yksinomaan henkilötietojen käsittelyä koskevia kriteereitä, joita ovat esimerkiksi käsittelyn lainmukaisuutta, tietosuojaperiaatteita sekä rekisteröidyn oikeuksia koskevat kriteerit. (kriteereitä 35)

Kokonaiskuva kriteeristön sisällöstä ja rakenteesta



Tiedonhallintalautakunta
Informationshanteringsnämnden

Kriteeristön ominaisuuksia

- Kriteerit koostuvat pääkriteereistä, sekä niitä täydentävistä alikriteereistä
- Kukin kriteeri on luokiteltu eri turvallisuuden näkökulmista sen mukaan, miltä tasolta alkaen sitä sovelletaan
  - Eri turvallisuustasojen vaatimukset on eri kriteereissä
- Kriteerit ovat mahdollisimman yksilöllisiä, eli samaan kriteeriin ei ole sisällytetty useita eri asioita
- Kriteerit on laadittu mahdollisimman toteutusneutraaleiksi

Yksittäisen kriteerin sisältö

Tunniste	**FYY-04, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä**
Nimi	Tiedon säilytys
Vaatimus	Tietoja on säilytettävä siten, että pääsy niihin suojataan sivullisilta.
Yleiskuvaus	Suojaaminen tarkoittaa käytännössä esimerkiksi tiedon tai tietoa sisältävän päätelaitteen riittävän turvallista säilyttämistä. Tietojen käsittelyssä on huomioitava lisäksi toiminta työskentelytaukojen aikana, jolloin asiakirjat ja päätelaitteet on turvallisuusluokan perusteella sijoitettava soveltuvalle turvallisuusalueelle ja/tai säilytysyksikköön tauon ajaksi. Tiedon säilytyksellä viitataan tilanteeseen, jossa tieto ei ole sen käsittelijän välittömässä valvonnassa.
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom; TLA 10 §
Viitteet	Julkri: HAL-19; Katakri: F-04
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 28–29

1. Kriteerin yksilöivä tunnus
2. Kriteerin luokittelut turvallisuuden eri näkökulmista
3. Kriteerin vaatimus
4. Kriteerin yleiskuvaus
5. Toteutusesimerkki
6. Lainsäädäntöviitteet
7. Viitteet muihin Julkri-kriteereihin ja Katakri-kriteereihin
8. Viitteet muihin lisätietoihin

Pääkriteerit: Hallinnollinen turvallisuus

- Periaatteet
- Tehtävät ja vastuut
- Resurssit
- Suojattavat kohteet
- Vaatimukset
- Riskienhallinta
- Seuranta ja valvonta
- Häiriöiden hallinta
- Dokumentointi
- Henkilöstön luotettavuuden arviointi
- Salassapito- ja vaitiolovelvollisuus
- Ohjeet
- Koulutukset
- Käyttö- ja käsittelyoikeudet
- Työskentelyn tietoturvallisuus koko palvelussuhteen ajan
- Hankintojen turvallisuus
- Tietojärjestelmien toiminnallinen käytettävyys ja vikasietoisuus
- Asiakirjajulkisuuden toteuttaminen
- Tietojen käsittely

Pääkriteerit: Fyysinen turvallisuus

- Fyysisen turvallisuuden riskien arviointi
- Fyysisten turvatoimien valinta (monitasoinen suojaus)
- Tiedon käsittely
- Tiedon säilytys
- Turvallisuusalue
- Hallinnollinen alue
- Turva-alue
- Tietojen kuljettaminen
- Tietojen kopioiminen
- Tietojen kirjaaminen
- Tietojen fyysinen tuhoaminen

Pääkriteerit: Tekninen turvallisuus

- Verkon rakenteellinen turvallisuus
- Tietoliikenneverkon vyöhykkeistäminen
- Suodatus- ja valvontajärjestelmien hallinnointi
- Hallintayhteydet
- Langaton tiedonsiirto
- Kasautumisvaikutus
- Pääsyoikeuksien hallinnointi
- Tietojenkäsittely-ympäristön toimijoiden tunnistaminen
- Tietojärjestelmien fyysinen turvallisuus
- Järjestelmäkovennus
- Haittaohjelmilta suojautuminen
- Turvallisuuteen liittyvien tapahtumien jäljitettävyys
- Poikkeamien havainnointikyky ja toipuminen
- Ohjelmistojen turvallisuuden varmistaminen
- Hajasäteily (TEMPEST) ja elektroninen tiedustelu
- Tiedon salaaminen
- Muutoshallintamenettelyt
- Etäkäyttö
- Ohjelmistohaavoittuvuuksien hallinta
- Varmuuskopiointi
- Sähköisessä muodossa olevien tietojen tuhoaminen
- Tietojärjestelmien saatavuus
- Tietojärjestelmien toiminnallinen käytettävyys

Pääkriteerit: Varautuminen ja jatkuvuudenhallinta

- Varautumista ohjaava lainsäädäntö
- Jatkuvuusvaatimusten määrittely
- Jatkuvuussuunnitelmat
- Resurssit ja osaaminen
- Henkilöstön saatavuus ja varajärjestelyt
- Tietoliikenteen varmistaminen
- Tietoteknisten ympäristöjen varmentaminen
- Vikasietoisuus
- Tietojärjestelmien toipumissuunnitelmat

Pääkriteerit: Tietosuoja

- Käsiteltävien henkilötietojen tunnistaminen
- Organisaation roolit
- Yhteisrekisterinpitäjät
- Henkilötietojen käsittelijä
- Tehtävät ja vastuut
- Henkilötietojen käsittelyn ohjeet
- Käsittelyn lainmukaisuus
- Tarpeellisuus ja oikeasuhtaisuus
- Käyttötarkoitussidonnaisuus
- Tietojen minimointi
- Säilytyksen rajoittaminen
- Täsmällisyys
- Käsittelyn turvallisuus
- Tietoturvaloukkaukset
- Osoitusvelvollisuus
- Tietosuojariskien hallinta
- Tietosuojan vaikutustenarviointi
- Henkilötietojen siirto ETA:n ulkopuolelle
- Rekisteröidyn oikeudet
- Automatisoidut yksittäispäätökset
- Seloste käsittelytoimista

Luokittelu, riskilähtöisyys ja kriteerien soveltaminen

Luokittelu – vaatimukset tiukentuvat

- Kriteerit on luokiteltu luottamuksellisuuden, eheyden ja saatavuuden näkökulmista eri tasoille.
- Lisäksi kriteerit on luokiteltu sen mukaan, sovelletaanko niitä henkilötietojen tai erityisiin henkilötietoryhmiin kuuluvien tietojen arvioinnissa.
- Pääkriteeri-alikriteeri rakennetta on hyödynnetty niin, että samaan aihealueeseen liittyvät vaatimukset tiukentuvat siirryttäessä korkeammille turvallisuuden tasoille.

Kriteerien luokittelut

- Kukin kriteeri on luokiteltu eheyden, saatavuuden ja luottamuksellisuuden näkökulmista
- Lisäksi kriteerit on luokiteltu henkilötietojen näkökulmista
- Luokittelu kuvaa, miltä ”tasolta” alkaen kriteeriä lähtökohtaisesti sovelletaan
  - Esim: ”Salassa pidettävä” kriteeriä, sovelletaan salassa pidettäville ja sitä luottamuksellisemmille tiedoille
- Kukin kriteeri on luokiteltu vähintään yhdestä näkökulmasta
- Kriteeriä ei ole luokiteltu, jos se ei ole relevantti jostain näkökulmasta

Eheys	Saatavuus	Luottamuksellisuus	Henkilötieto
Vähäinen	Vähäinen	Julkinen	Henkilötieto
Normaali	Normaali	Salassa pidettävä	Erityinen henkilö-tietoryhmä
Tärkeä	Tärkeä	Turvallisuusluokka IV	
Kriittinen	Kriittinen	Turvallisuusluokka III	
		Turvallisuusluokka II	
		Turvallisuusluokka I	

Luokittelu - eheys

Eheys on tiedon ominaisuus, joka tarkoittaa sitä, että tietoa ei ole muutettu luvatta tai että se ei ole muuttunut vahingossa ja että mahdolliset muutokset voidaan todentaa.

Taso	Kuvaus	Esimerkki
Vähäinen	Tiedon häviämisestä tai muuttumisesta ei aiheudu olennaista haittaa.	Toimisto-ohjelmistot, järjestelmien virhelokit.
Normaali	Tiedon häviäminen tai muuttuminen aiheuttaa kohtuullista haittaa, mutta se voidaan havaita ja siitä voidaan toipua.	Henkilöstöhallinnon järjestelmät.
Tärkeä	Tiedon häviäminen tai muuttuminen aiheuttaa merkittävää haittaa tai mainevahinkoa ja sen havaitseminen voi olla vaikeaa.	Laboratoriotuloksia välittävät integraatioalustat, joissa yksittäisten mittausten virheiden havainnointi voi olla vaikeaa. Henkilötietojen käsittelyyn liittyvät lokitiedot.
Kriittinen	Tiedon häviäminen tai muuttumista ei voida hyväksyä missään tilanteessa.	Yhteiskunnan toimivuuden kannalta keskeiset maksuliikennejärjestelmät tai raideliikenteen ohjausjärjestelmä

Luokittelu - saatavuus

Saatavuus tarkoittaa sitä, miten tieto, tietojärjestelmä tai palvelu on hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Taso	Kuvaus	Esimerkki
Vähäinen	Tiedon saatavuuden osalta pystytään hyväksymään useiden viikkojen mittaisia häiriöitä.	Henkilöstön pysäköintipaikkojen rekisteri, puiston penkkien vikarekisteri
Normaali	Tiedon saatavuuden osalta pystytään hyväksymään enintään päivien mittaisia häiriöitä.	Arkistojärjestelmä
Tärkeä	Tiedon saatavuuden osalta pystytään hyväksymään enintään tuntien mittaisia häiriöitä.	Potilastietojärjestelmä
Kriittinen	Tiedon saatavuuden osalta pystytään hyväksymään enintään minuuttien mittaisia häiriöitä.	Keskitetyt käyttäjän tunnistamispalvelut

Luokittelu - luottamuksellisuus

Taso	Kuvaus	Esimerkki
Julkinen	Viranomaisen asiakirjat ovat julkisia, jollei laissa erikseen toisin säädetä. (julkisuuslaki 1 §)	Kunnanvaltuuston pöytäkirjat julkisilta osiltaan, organisaation julkiset internet-sivut.
Salassa pidettävä	Viranomaisen asiakirja on pidettävä salassa, jos se laissa on säädetty salassa pidettäväksi tai jos viranomainen lain nojalla on määrännyt sen salassa pidettäväksi taikka jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus. (julkisuuslaki 22 §)	Potilasasiakirjat, tiedot sosiaalihuollon asiakkaasta, psykologiset testit ja soveltuvuuskokeet.
Turvallisuusluokka IV (TL IV)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **lievää vahinkoa** tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle.	Tiedonhallintalain 18 §:ssä mainittujen suojattavien etujen kannalta olennaisen tietojärjestelmän turvajärjestelyiden dokumentaatio, jonka paljastuminen ei keskeytä toimintaa, mutta saattaa edellyttää muutoksia paljastuneissa suunnitelmissa.
Turvallisuusluokka III (TL III)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **vahinkoa** tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle;	Tiedonhallintalain 18 §:ssä mainittujen suojattavien etujen kannalta elintärkeiden toimintojen turvajärjestelyiden dokumentaatio, jonka paljastumisen vuoksi toiminta joudutaan keskeyttämään.
Turvallisuusluokka II (TL II)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **merkittävää vahinkoa** tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle;.	Tiedonhallintalain 18 §:ssä mainittujen suojattavien etujen kannalta elintärkeiden toimintojen turvajärjestelyiden dokumentaatio, jonka paljastumisen vuoksi laajan ihmisjoukon turvallisuutta ei voida taata ja jonka seurauksena toiminta joudutaan keskeyttämään pitkähköksi ajaksi.
Turvallisuusluokka I (TL I)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **erityisen suurta vahinkoa** tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle.	Tiedonhallintalain 18 §:ssä mainittujen suojattavien etujen kannalta yhteiskunnan toimintakyvyn kannalta keskeisiin toimintoihin, kuten kriittiseen infrastruktuurin tai elintärkeän toiminnan turvajärjestelyjä koskevan tiedon paljastuminen, jonka seurauksena viranomaisen tai muun kriittisen infrastruktuurin toimijan toiminta todennäköisesti estyy ja vahinko on laajamittaista.

Luottamuksellisuus - turvallisuusluokittelu (TL IV – TL I)

- **Turvallisuusluokkaa koskeva merkintä on tehtävä, jos…(TihL 18 § 1 mom)**
- **Julkisuuslaki 24 § 1 mom kohdat 2, 5 ja 7-11**:
  2) …Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön…
  5) poliisin, Rajavartiolaitoksen, Tullin, vankeinhoitoviranomaisen ja Maahanmuuttoviraston taktisia ja teknisiä menetelmiä ja suunnitelmia…
  7) …turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat…
  8) …onnettomuuksiin tai poikkeusoloihin varautumista, väestönsuojelua…
  9) …asiakirjat, jotka koskevat valtion turvallisuuden ylläpitämistä…
  10) …sotilastiedustelua, puolustusvoimien varustamista, kokoonpanoa, sijoitusta tai käyttöä…
  11) …tietoja raha- ja valuuttapoliittisista päätöksistä tai toimenpiteistä taikka niiden valmistelusta…
- **TihL 18 § 1 mom:** ”… **ja** asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.”

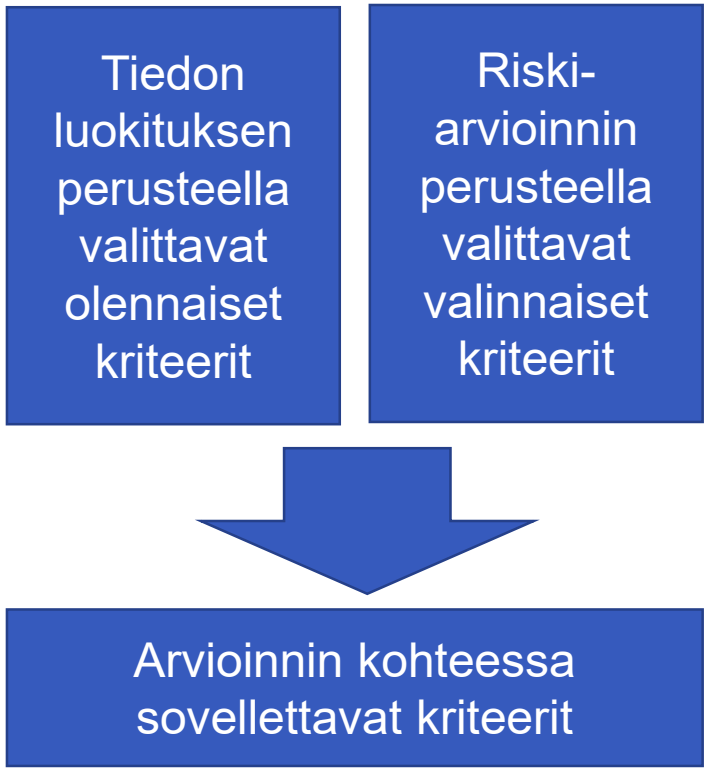
Julkri suositus korostaa riskiarviointia

- Luokittelu kuvaa missä tilanteissa kriteeriä on lähtökohtaisesti sovellettava.
  - Esimerkiksi jos kriteeri on luokiteltu tasolle ”Salassa pidettävä”, tulee sitä lähtökohtaisesti soveltaa kaikille salassa pidettäville ja sitä korkeammille tasoille luokitelluille tiedoille
  - Tällaiset kriteerit työkalu määrittelee esiehtojen perusteella ”Olennaisiksi”

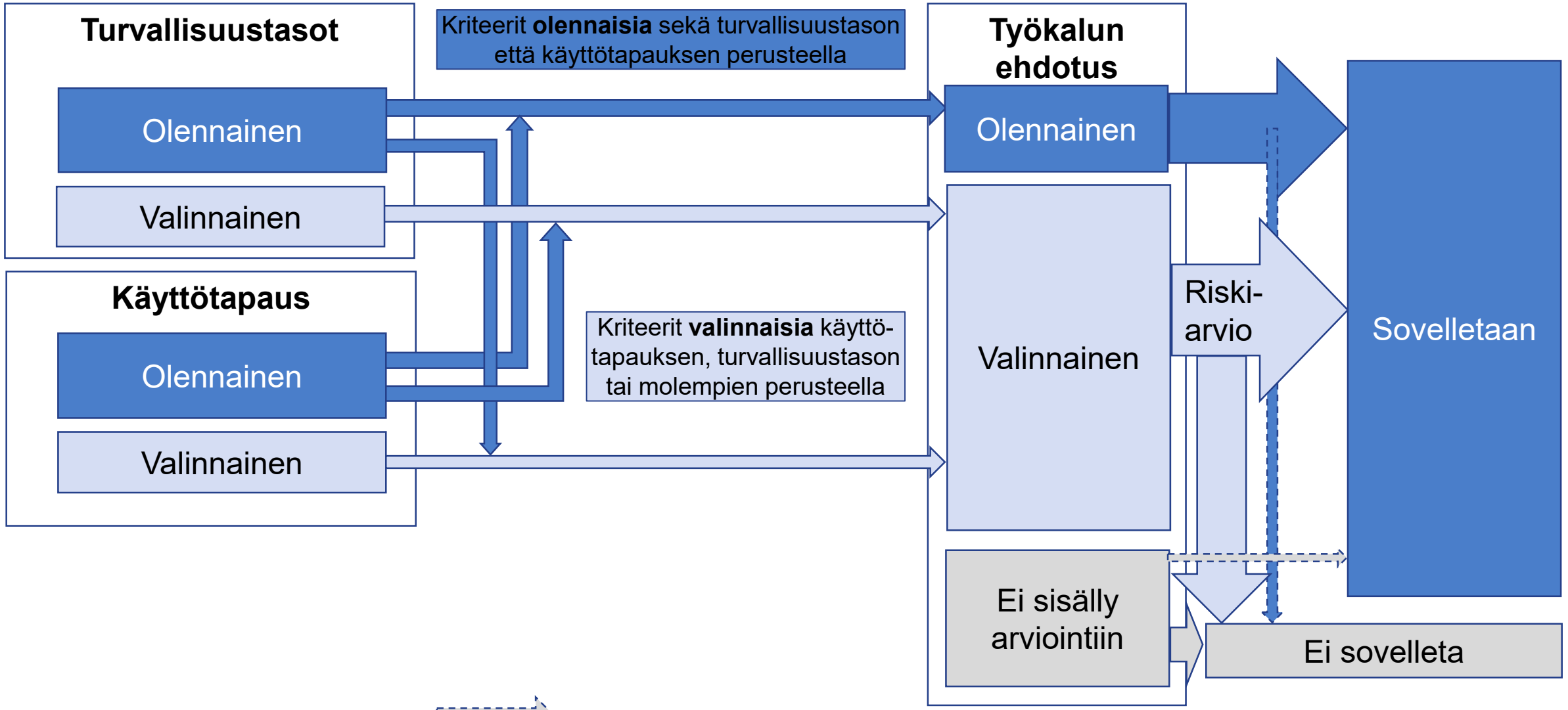
- Seuraavaksi korkeamman tason kriteereitä sovelletaan riskilähtöisesti
  - Esimerkiksi jos kriteeri on luokiteltu luottamuksellisuuden näkökulmasta tasolle ”TL IV” – kriteeri on valinnainen ”Salassa pidettäville” tiedoille
  - Tällaiset kriteerit työkalu määrittelee esiehtojen perusteella ”Valinnaisiksi”
  - Valinnaisten kriteerien soveltamisesta organisaatio päättää riskiarvion perusteella

Riskilähtöisyyden huomiointi kriteeristössä

- Julkrin tavoitteena on ohjata käyttäjiä toteuttamaan olennaiset kriteerit ja täydentämään niitä riskilähtöisesti valituilla valinnaisilla kriteereillä
- Riskilähtöisyydellä haetaan oikeaa tasapainoa riskien suuruuden ja niiden pienentämisen kustannusten välillä
- Kokonaisriskin arvioinnissa voidaan ottaa huomioon kompensoivat kontrollit



Kriteerien olennaisuus, valinnaisuus ja soveltaminen



Huom! Tapauskohtaisen harkinnan ja riskiarvion perusteella voidaan soveltamispäätöksissä poiketa työkalun ehdotuksista.

Kriteerien soveltaminen on tasapainottelua

Työkalun antamat ehdotukset ovat vain suosituksia!

Organisaation tulee aina perustaa lopulliset päätökset kriteerien soveltamisesta tapauskohtaiseen riskiarvioon!

Julkri-työkalun käyttö

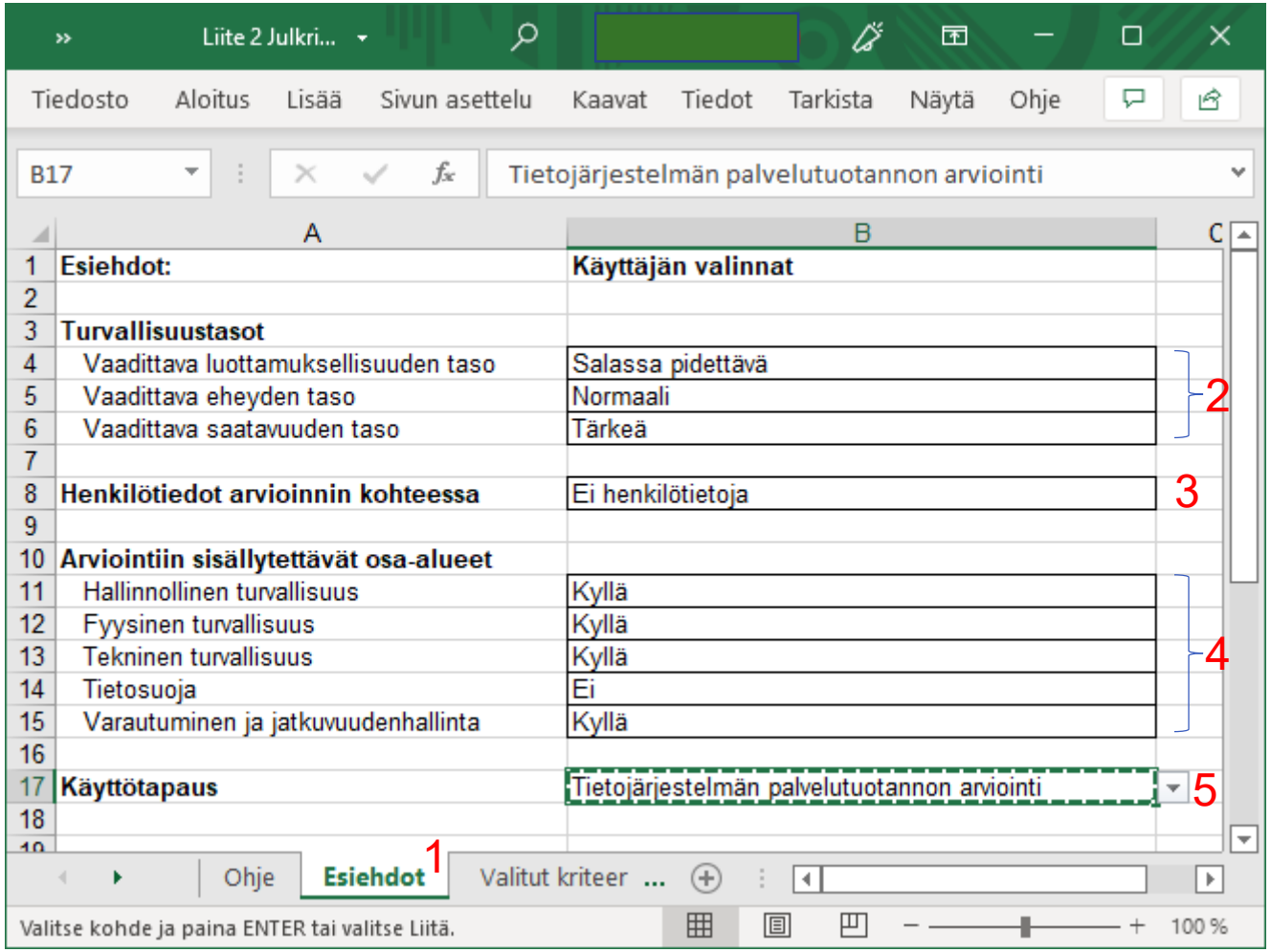
Työkalun käytön vaiheet

1. Käyttäjä selvittää kohteen lähtötiedot, jotka tarvitaan esiehtojen antamisessa
2. Käyttäjä antaa esiehdot, jonka perusteella työkalu ehdottaa ”olennaiset” ja ”valinnaiset” kriteerit
3. Käyttäjä valitsee riskiarvion perusteella sovellettavat kriteerit
    a) Kriteerien tietojen katsominen
4. Kohteen arviointi toteutetaan sovellettavien kriteerien perusteella

1 Lähtötietojen selvitys

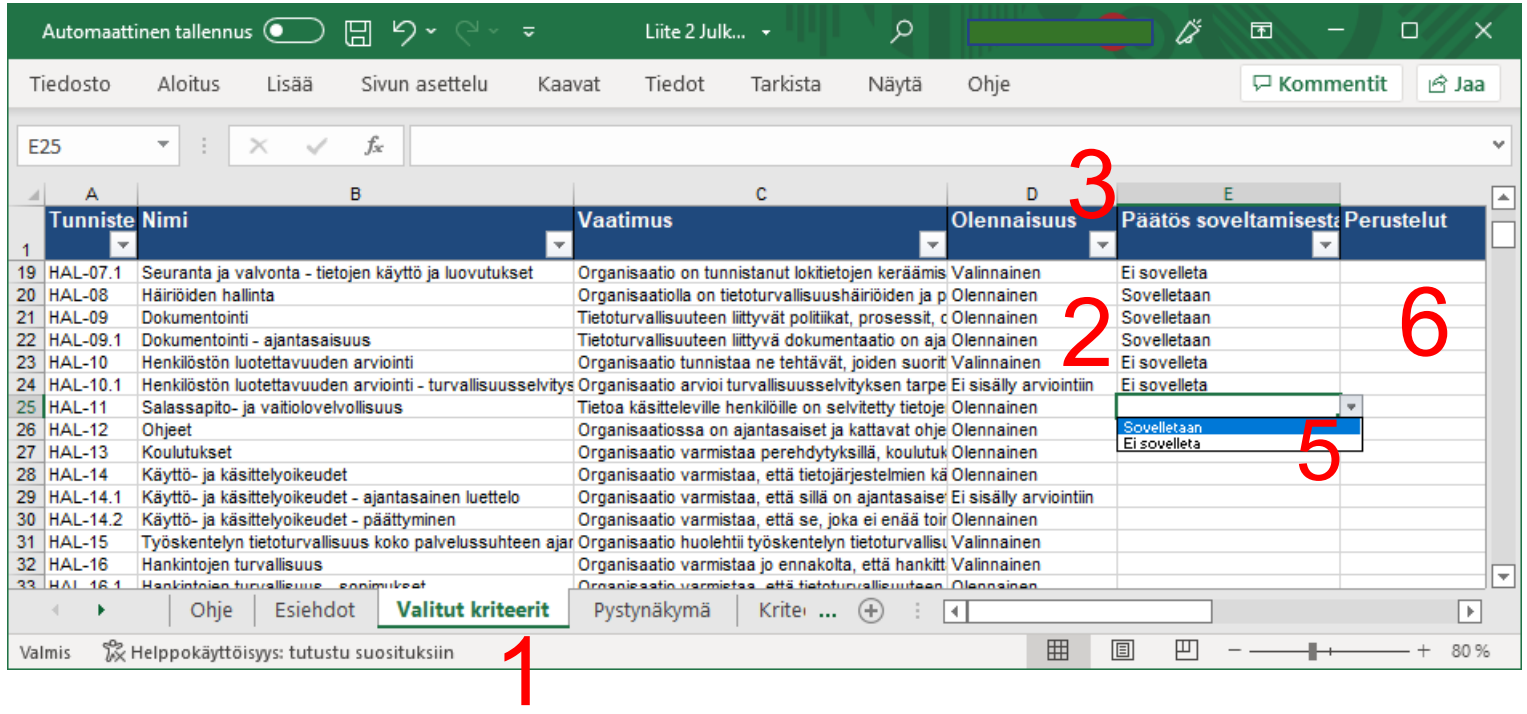
- Jo ennen kriteeristön käyttöä tulee selvittää minkälaisesta arviointikohteesta on kyse.
  - Minkä tasoisia vaatimuksia kohteelle asetetaan luottamuksellisuuden, eheyden ja saatavuuden suhteen?
  - Käsitelläänkö henkilötietoja sekä kuuluvatko ne erityisiin henkilötietoryhmiin? (eli käsitelläänkö ns. arkaluonteisia henkilötietoja)
  - Voidaanko jotain osa-alueita rajata arvioinnin ulkopuolelle?
  - Soveltuuko arviointiin joku aiemmin määritelty käyttötapaus?
- Tiedonhallintamalli, kohteiden luokittelut sekä selkeät ohjeet kohteiden luokittelusta helpottavat lähtötietojen selvittämistä!

2 Esiehtojen antaminen



1. Välilehti ”Esiehdot”
2. Valitse turvallisuustasot (luottamuksellisuus, eheys ja saatavuus)
3. Valitse henkilötietojen käsittelyn taso
4. Valitse arviointiin sisällytettävät osa-alueet (oletusarvoisesti kaikki)
5. Valitse tarvittaessa käyttötapaus

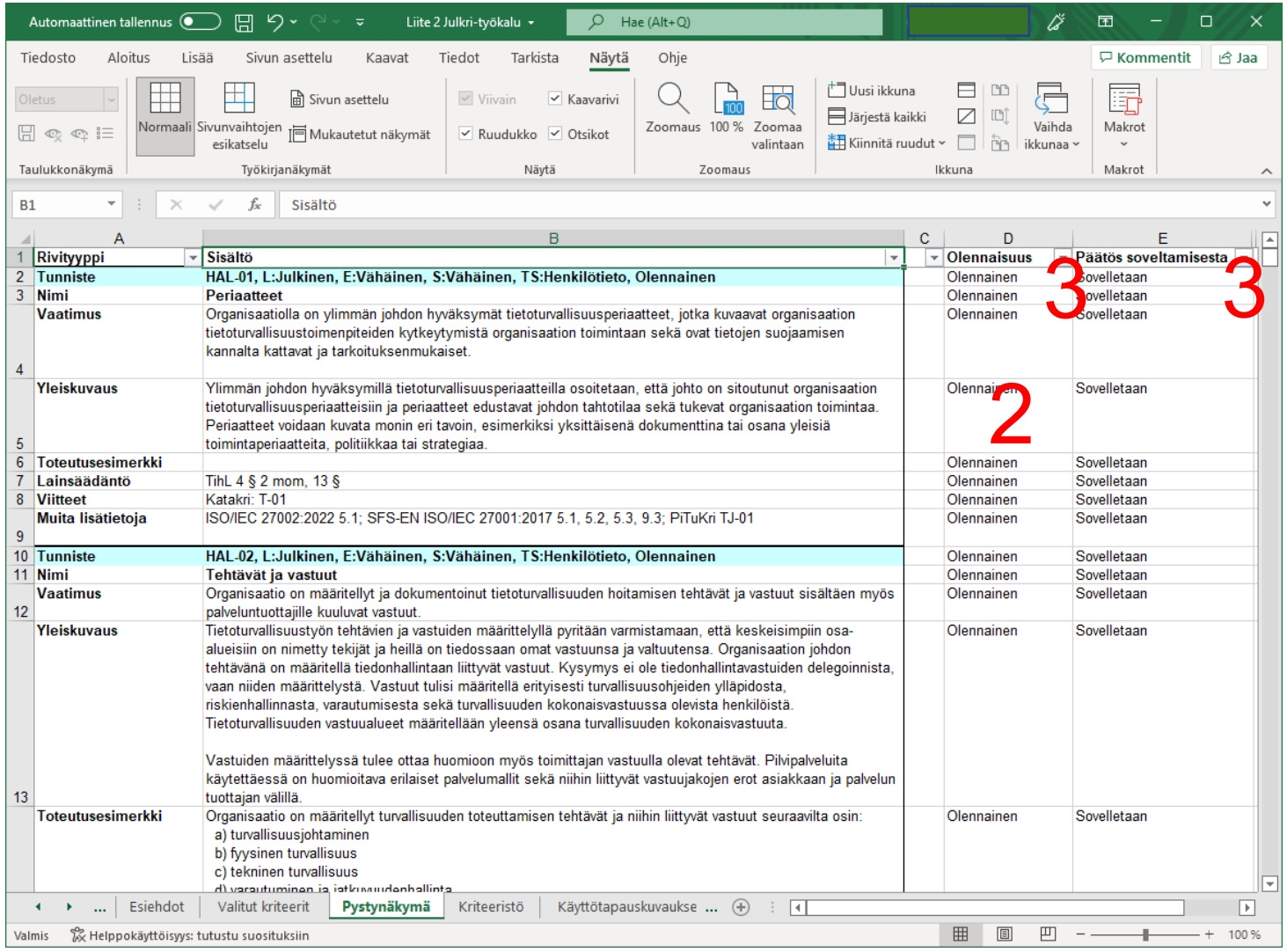
3 Sovellettavien kriteerien valinta



Huom! Organisaatio voi harkinnan ja riskiarvion perusteella poiketa soveltamisen lähtökohdista perustelluista syistä!

1. Välilehti ”Valitut kriteerit”
2. Työkalu määrittelee olennaisuuden esiehtojen perusteella
3. Voit suodattaa näkyviin vain valinnaiset kriteerit
4. Soveltamisen lähtökohdat kriteerin olennaisuuden perusteella
   a) Olennainen -> Sovelletaan
   b) Valinnainen -> Riskiarvion perusteella
   c) Ei sisälly arviointiin -> Ei sovelleta
5. Merkitse päätös soveltamisesta kullekin kriteerille alasvetovalikon avulla
6. Kirjaa perustelut

3 a Kriteerien tietojen katsominen



	A	B	C	D	E
1	**Rivityyppi**	**Sisältö**		**Olennaisuus**	**Päätös soveltamisesta**
2	**Tunniste**	**HAL-01, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto, Olennainen**		Olennainen	Sovelletaan
3	**Nimi**	**Periaatteet**		Olennainen	Sovelletaan
4	**Vaatimus**	Organisaatiolla on ylimmän johdon hyväksymät tietoturvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan sekä ovat tietojen suojaamisen kannalta kattavat ja tarkoituksenmukaiset.		Olennainen	Sovelletaan
5	**Yleiskuvaus**	Ylimmän johdon hyväksymillä tietoturvallisuusperiaatteilla osoitetaan, että johto on sitoutunut organisaation tietoturvallisuusperiaatteisiin ja periaatteet edustavat johdon tahtotilaa sekä tukevat organisaation toimintaa. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi yksittäisenä dokumenttina tai osana yleisiä toimintaperiaatteita, politiikkaa tai strategiaa.		Olennainen	Sovelletaan
6	**Toteutusesimerkki**			Olennainen	Sovelletaan
7	**Lainsäädäntö**	TihL 4 § 2 mom, 13 §		Olennainen	Sovelletaan
8	**Viitteet**	Katakri: T-01		Olennainen	Sovelletaan
9	**Muita lisätietoja**	ISO/IEC 27002:2022 5.1; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3, 9.3; PiTuKri TJ-01		Olennainen	Sovelletaan
10	**Tunniste**	**HAL-02, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto, Olennainen**		Olennainen	Sovelletaan
11	**Nimi**	**Tehtävät ja vastuut**		Olennainen	Sovelletaan
12	**Vaatimus**	Organisaatio on määritellyt ja dokumentoinut tietoturvallisuuden hoitamisen tehtävät ja vastuut sisältäen myös palveluntuottajille kuuluvat vastuut.		Olennainen	Sovelletaan
13	**Yleiskuvaus**	Tietoturvallisuustyön tehtävien ja vastuiden määrittelyllä pyritään varmistamaan, että keskeisimpiin osa-alueisiin on nimetty tekijät ja heillä on tiedossaan omat vastuunsa ja valtuutensa. Organisaation johdon tehtävänä on määritellä tiedonhallintaan liittyvät vastuut. Kysymys ei ole tiedonhallintavastuiden delegoinnista, vaan niiden määrittelystä. Vastuut tulisi määritellä erityisesti turvallisuusohjeiden ylläpidosta, riskienhallinnasta, varautumisesta sekä turvallisuuden kokonaisvastuussa olevista henkilöistä. Tietoturvallisuuden vastuualueet määritellään yleensä osana turvallisuuden kokonaisvastuuta. Vastuiden määrittelyssä tulee ottaa huomioon myös toimittajan vastuulla olevat tehtävät. Pilvipalveluita käytettäessä on huomioitava erilaiset palvelumallit sekä niihin liittyvät vastuujakojen erot asiakkaan ja palvelun tuottajan välillä.		Olennainen	Sovelletaan
	Toteutusesimerkki	Organisaatio on määritellyt turvallisuuden toteuttamisen tehtävät ja niihin liittyvät vastuut seuraavilta osin: a) turvallisuusjohtaminen b) fyysinen turvallisuus c) tekninen turvallisuus d) varautuminen ja jatkuvuudenhallinta		Olennainen	Sovelletaan

1

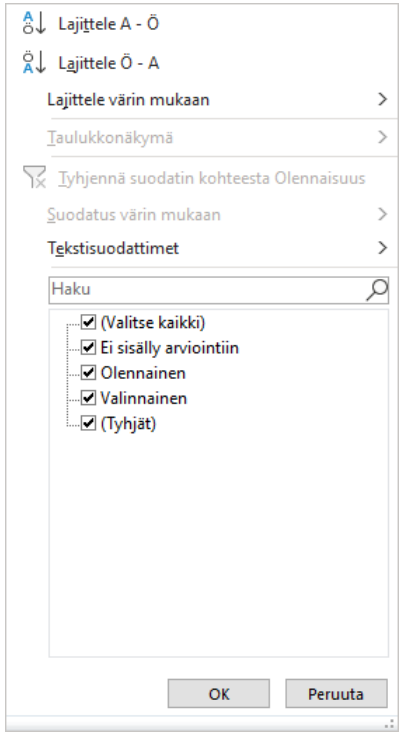
2

3

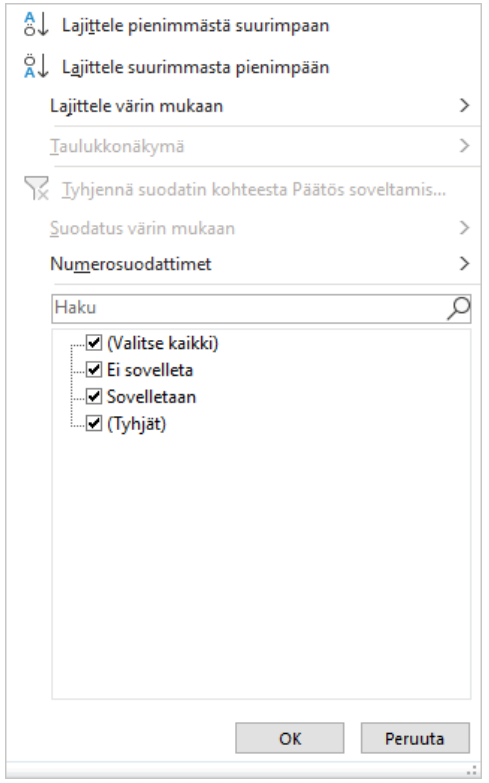
3

1. Kriteerien yksityiskohtaisia tietoja voi katsoa joko liitteistä 1A ja 1B tai välilehdellä ”Pystynäkymä”
2. Välilehdellä näkyvät myös kriteerien olennaisuustiedot annettujen esiehtojen perusteella
3. Kriteerejä voi suodattaa olennaisuuden ja soveltamispäätöksen perusteella

3

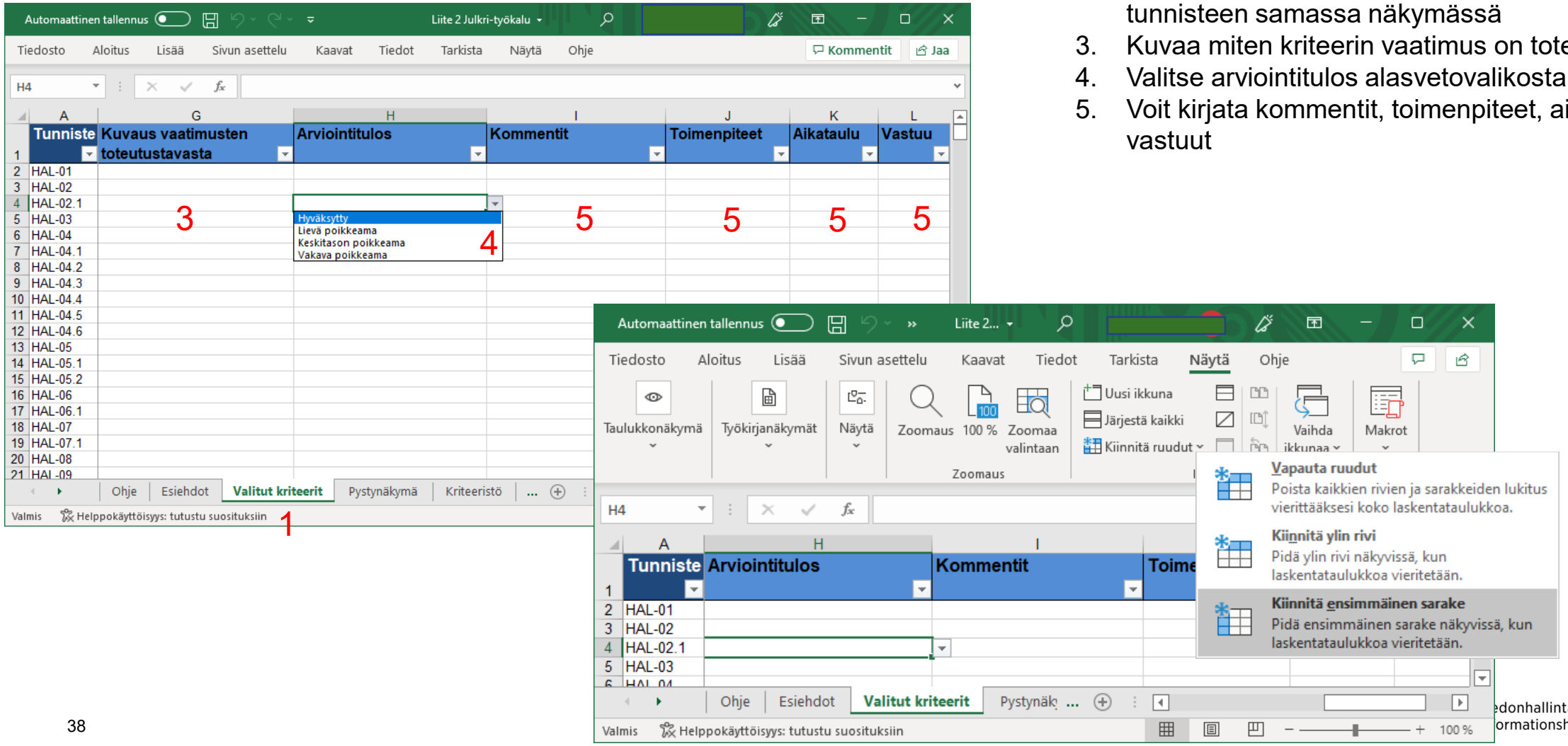


3



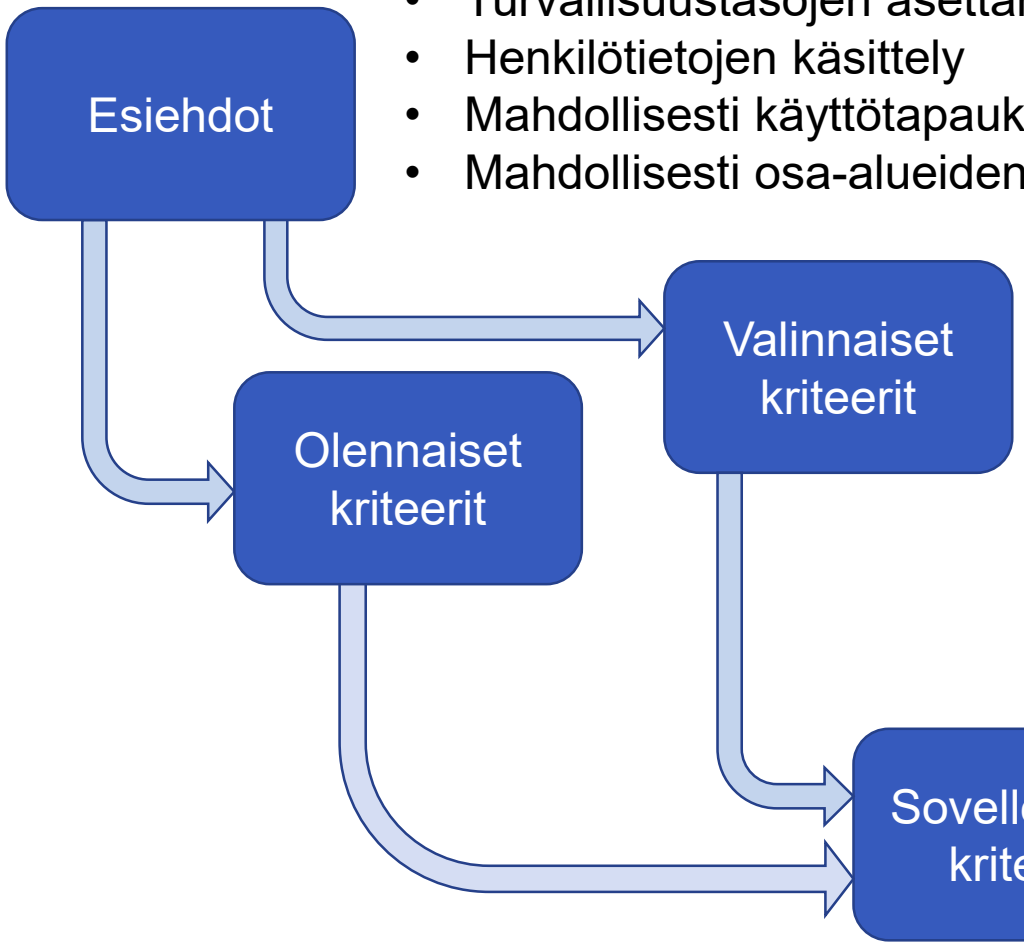
4 Arvioinnin tuloksen kirjaaminen

1. Välilehti ”Valitut kriteerit”
2. Voit kiinnittää A-sarakkeen, jotta näet kriteerin tunnisteen samassa näkymässä
3. Kuvaa miten kriteerin vaatimus on toteutettu
4. Valitse arviointitulos alasvetovalikosta
5. Voit kirjata kommentit, toimenpiteet, aikataulut ja vastuut



Yhteenveto kriteeristön soveltamisesta

1 ja 2



- Turvallisuustasojen asettaminen
- Henkilötietojen käsittely
- Mahdollisesti käyttötapauksen valinta
- Mahdollisesti osa-alueiden rajaukset

3 ja 3a

- Riskilähtöinen täydentäminen

4

- Kehittäminen
- Arvioinnit

Käyttötapaukset

Käyttötapausten tausta ja tavoitteet

- Käyttötapaukset ovat tiettyyn tarkoitukseen etukäteen määriteltyjä kriteerijoukkoja
- Käyttötapausten avulla voi tehostaa kriteeristön käyttöä samantyyppisissä arviointitilanteissa
- Julkrissa on sekä ennalta määriteltyjä käyttötapauksia että mahdollisuus määritellä organisaatiokohtaisia käyttötapauksia
- Käyttötapauksissa määritellään kriteerikohtaisesti
  - Käyttötapaukseen sisältyvät kriteerit
  - Valinnaiset kriteerit
  - Arvioinnista pois jätettävät kriteerit
- Käyttötapausten määrittelyt vaikuttavat kriteerien määräytymiseen olennaisiksi, valinnaisiksi tai pois-jätettäviksi esiehtojen perusteella

Ennalta määritellyt käyttötapaukset

- Julkri sisältää valmiita ennalta määriteltyjä käyttötapauksia. Niihin on poimittu kyseiseen tilanteeseen soveltuvat kriteerit
  1. Tiedonhallintayksikön hallinnollinen turvallisuusarviointi
  2. SaaS-pilvipalvelun arviointi
  3. Asiantuntijatyön hankinta
  4. Tietojärjestelmän palvelutuotannon arviointi

- Organisaatiot voivat myös itse määritellä käyttötapauksia usein toistuviin arviointitilanteisiin. **Vaatii huolellisuutta.**

1. Tiedonhallintayksikön hallinnollinen turvallisuusarviointi

- Käyttötapaus on tarkoitettu tiedonhallintayksikön tiedonhallintalain mukaisen tietoturvallisuuden vähimmäistason ja tietosuojan arviointiin.

- Se sisältää arvioinnin hallinnollisen turvallisuuden, tietosuojan sekä varautumisen ja jatkuvuuden hallinnan näkökulmista. Käyttötapausta voi täydentää fyysisen turvallisuuden ja tietojärjestelmäarvioinneilla.

2. SaaS-pilvipalvelun arviointi

- Käyttötapaus on tarkoitettu SaaS-palveluina tuotettujen pilvipalveluiden turvallisuuden arviointiin
- Käyttötapaus rajoittuu luottamuksellisuuden osalta enintään salassa pidettävän tiedon käsittelyyn pilvipalveluissa
- Käyttötapauksella voidaan arvioida, täyttääkö arvioitava palvelu tiedonhallintalain mukaiset vaatimukset tietoturvallisuuden varmistamiseksi. Arvioinnissa voidaan käyttää hyväksi pilvipalveluiden tuottajan sertifikaatteja, dokumentaatiota ja muita mahdollisia todisteita turvallisuusvaatimusten toteutumisesta
- Jos käytettävässä palvelussa on tarkoitus käsitellä henkilötietoja, tulee arvioinnissa huomioida myös tietosuojaa koskevat kriteerit.

3. Asiantuntijatyön hankinta

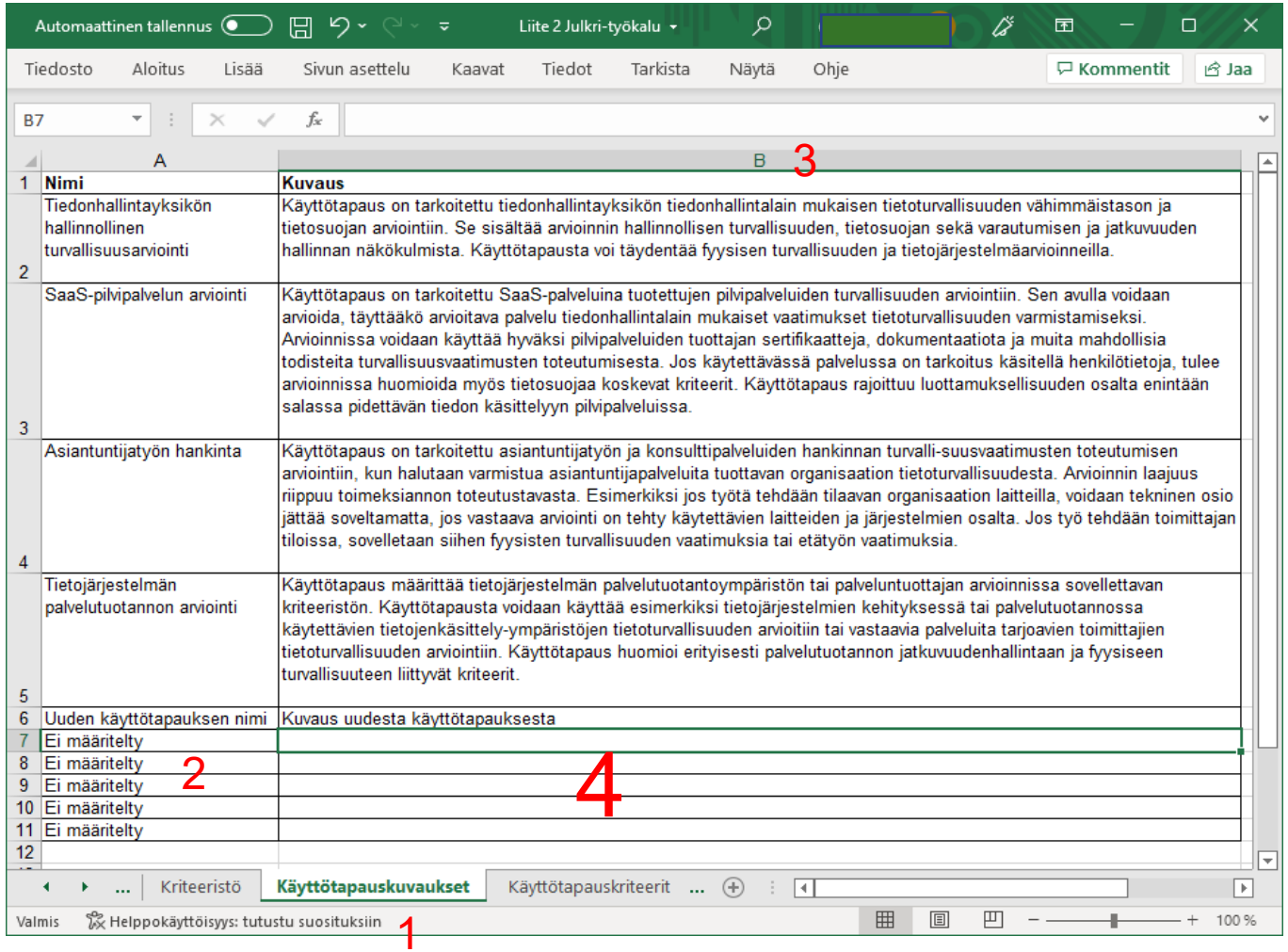
- Käyttötapaus on tarkoitettu asiantuntijatyön ja konsulttipalveluiden hankinnan turvallisuusvaatimusten toteutumisen arviointiin, kun halutaan varmistua asiantuntijapalveluita tuottavan organisaation tietoturvallisuudesta.
- Arvioinnin laajuus riippuu toimeksiannon toteutustavasta.
  - Esimerkiksi jos työtä tehdään tilaavan organisaation laitteilla, voidaan tekninen osio jättää soveltamatta, jos vastaava arviointi on tehty käytettävien laitteiden ja järjestelmien osalta. Jos työ tehdään toimittajan tiloissa, sovelletaan siihen fyysisten turvallisuuden vaatimuksia tai etätyön vaatimuksia.

4. Tietojärjestelmän palvelutuotannon arviointi

- Käyttötapaus määrittää tietojärjestelmän palvelutuotantoympäristön tai palveluntuottajan arvioinnissa sovellettavan kriteeristön
- Käyttötapausta voidaan käyttää, esimerkiksi tietojärjestelmien kehityksessä tai palvelutuotannossa käytettävien tietojenkäsittely-ympäristöjen tietoturvallisuuden arvioitiin tai vastaavia palveluita tarjoavien toimittajien tietoturvallisuuden arviointiin.

- Käyttötapaus huomioi erityisesti palvelutuotannon jatkuvuudenhallintaan ja fyysiseen turvallisuuteen liittyvät kriteerit

Organisaation omien käyttötapausten kuvaaminen



	A	B
1	**Nimi**	**Kuvaus**
2	Tiedonhallintayksikön hallinnollinen turvallisuusarviointi	Käyttötapaus on tarkoitettu tiedonhallintayksikön tiedonhallintalain mukaisen tietoturvallisuuden vähimmäistason ja tietosuojan arviointiin. Se sisältää arvioinnin hallinnollisen turvallisuuden, tietosuojan sekä varautumisen ja jatkuvuuden hallinnan näkökulmista. Käyttötapausta voi täydentää fyysisen turvallisuuden ja tietojärjestelmäarvioinneilla.
3	SaaS-pilvipalvelun arviointi	Käyttötapaus on tarkoitettu SaaS-palveluina tuotettujen pilvipalveluiden turvallisuuden arviointiin. Sen avulla voidaan arvioida, täyttääkö arvioitava palvelu tiedonhallintalain mukaiset vaatimukset tietoturvallisuuden varmistamiseksi. Arvioinnissa voidaan käyttää hyväksi pilvipalveluiden tuottajan sertifikaatteja, dokumentaatiota ja muita mahdollisia todisteita turvallisuusvaatimusten toteutumisesta. Jos käytettävässä palvelussa on tarkoitus käsitellä henkilötietoja, tulee arvioinnissa huomioida myös tietosuojaa koskevat kriteerit. Käyttötapaus rajoittuu luottamuksellisuuden osalta enintään salassa pidettävän tiedon käsittelyyn pilvipalveluissa.
4	Asiantuntijatyön hankinta	Käyttötapaus on tarkoitettu asiantuntijatyön ja konsulttipalveluiden hankinnan turvalli-suusvaatimusten toteutumisen arviointiin, kun halutaan varmistua asiantuntijapalveluita tuottavan organisaation tietoturvallisuudesta. Arvioinnin laajuus riippuu toimeksiannon toteutustavasta. Esimerkiksi jos työtä tehdään tilaavan organisaation laitteilla, voidaan tekninen osio jättää soveltamatta, jos vastaava arviointi on tehty käytettävien laitteiden ja järjestelmien osalta. Jos työ tehdään toimittajan tiloissa, sovelletaan siihen fyysisten turvallisuuden vaatimuksia tai etätyön vaatimuksia.
5	Tietojärjestelmän palvelutuotannon arviointi	Käyttötapaus määrittää tietojärjestelmän palvelutuotantoympäristön tai palveluntuottajan arvioinnissa sovellettavan kriteeristön. Käyttötapausta voidaan käyttää esimerkiksi tietojärjestelmien kehityksessä tai palvelutuotannossa käytettävien tietojenkäsittely-ympäristöjen tietoturvallisuuden arvioitiin tai vastaavia palveluita tarjoavien toimittajien tietoturvallisuuden arviointiin. Käyttötapaus huomioi erityisesti palvelutuotannon jatkuvuudenhallintaan ja fyysiseen turvallisuuteen liittyvät kriteerit.
6	Uuden käyttötapauksen nimi	Kuvaus uudesta käyttötapauksesta
7	Ei määritelty	
8	Ei määritelty	
9	Ei määritelty	
10	Ei määritelty	
11	Ei määritelty	
12		

Ensin määritellään käyttötapauksen nimi ja laaditaan yleiskuvaus käyttötapauksen käyttötarkoituksesta

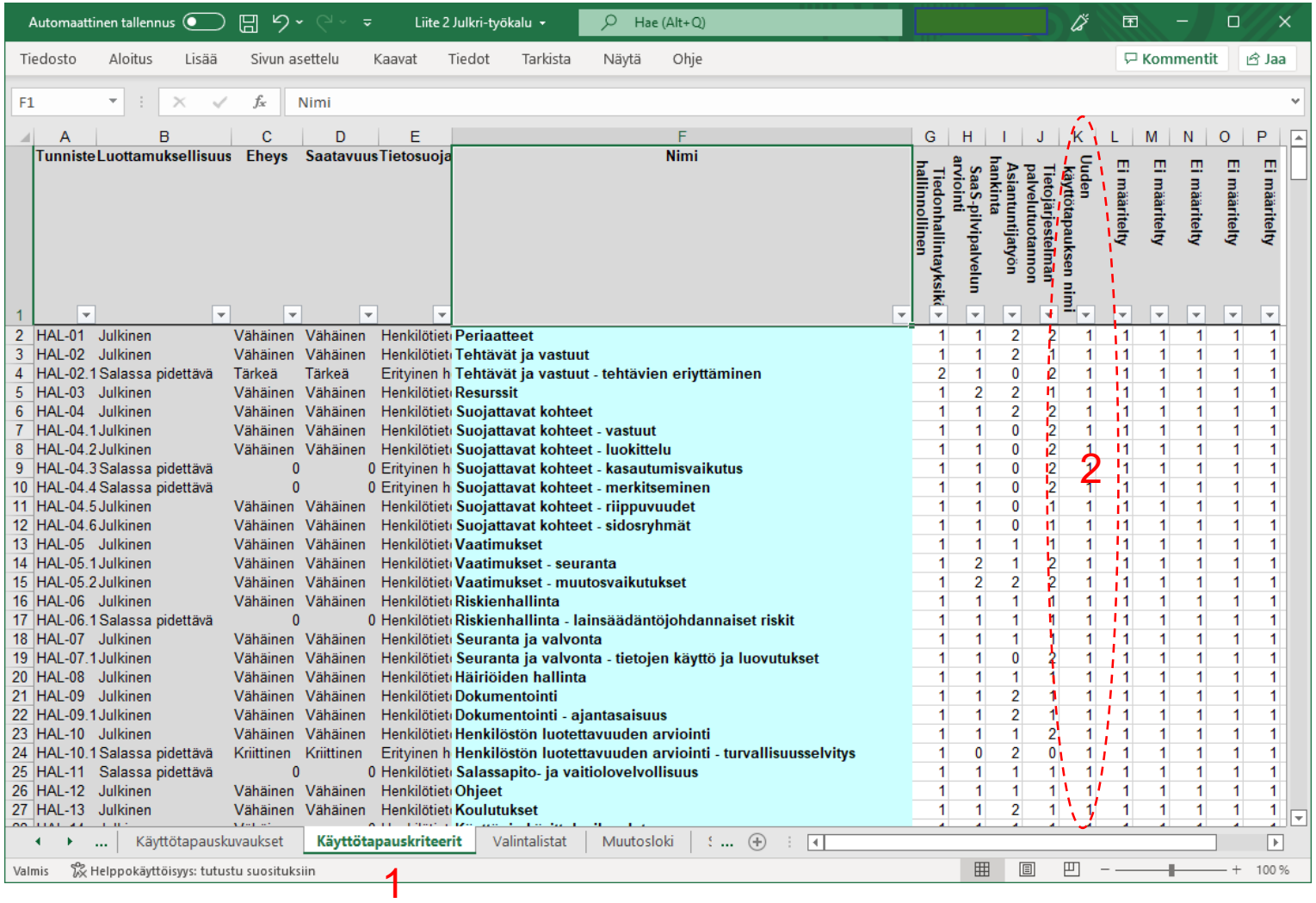
1. Välilehti ”Käyttötapauskuvaukset”
2. Lisää käyttötapauksen nimi sarakkeeseen A
   a) Nimi välittyy automaattisesti muille näytöille
3. Kuvaa käyttötapaus sarakkeeseen B
4. Organisaatioiden käytettävissä ovat rivit 6-11, etukäteen määritellyt käyttötapaukset ovat riveillä 2-5

Vinkkejä:

A. Käyttötapaus kannattaa kuvata riittävän tarkasti, jotta käyttäjä voi päätellä sen soveltuvuuden arviointitilanteeseen

B. Tarvittaessa käyttötapauksesta voi laatia erillisen kuvauksen, jossa täsmennetään millä perusteilla käyttötapauksen kriteerit on valittu

Käyttötapauksen kriteerien määrittely



	Tunniste	Luottamuksellisuus	Eheys	Saatavuus	Tietosuoja	Nimi	Tiedonhallintayksikkö hallinnollinen	Tiedonhallintayksikkö arviointi	SaaS-pilvipalvelun hankinta	Asiantuntijatyön palvelutuotannon	Tietojärjestelmän	Uuden käyttötapauksen nimi	Ei määritelty	Ei määritelty	Ei määritelty	Ei määritelty	Ei määritelty
2	HAL-01	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Periaatteet	1	1	2	2	1	1	1	1	1	1	1
3	HAL-02	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Tehtävät ja vastuut	1	1	2	1	1	1	1	1	1	1	1
4	HAL-02.1	Salassa pidettävä	Tärkeä	Tärkeä	Erityinen h	Tehtävät ja vastuut - tehtävien eriyttäminen	2	1	0	2	1	1	1	1	1	1	1
5	HAL-03	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Resurssit	1	2	2	1	1	1	1	1	1	1	1
6	HAL-04	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Suojattavat kohteet	1	1	2	2	1	1	1	1	1	1	1
7	HAL-04.1	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Suojattavat kohteet - vastuut	1	1	0	2	1	1	1	1	1	1	1
8	HAL-04.2	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Suojattavat kohteet - luokittelu	1	1	0	2	1	1	1	1	1	1	1
9	HAL-04.3	Salassa pidettävä	0	0	Erityinen h	Suojattavat kohteet - kasautumisvaikutus	1	1	0	2	1	1	1	1	1	1	1
10	HAL-04.4	Salassa pidettävä	0	0	Erityinen h	Suojattavat kohteet - merkitseminen	1	1	0	2	1	1	1	1	1	1	1
11	HAL-04.5	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Suojattavat kohteet - riippuvuudet	1	1	0	1	1	1	1	1	1	1	1
12	HAL-04.6	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Suojattavat kohteet - sidosryhmät	1	1	0	1	1	1	1	1	1	1	1
13	HAL-05	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Vaatimukset	1	1	1	1	1	1	1	1	1	1	1
14	HAL-05.1	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Vaatimukset - seuranta	1	2	1	2	1	1	1	1	1	1	1
15	HAL-05.2	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Vaatimukset - muutosvaikutukset	1	2	2	2	1	1	1	1	1	1	1
16	HAL-06	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Riskienhallinta	1	1	1	1	1	1	1	1	1	1	1
17	HAL-06.1	Salassa pidettävä	0	0	Henkilötiet	Riskienhallinta - lainsäädäntöjohdannaiset riskit	1	1	1	1	1	1	1	1	1	1	1
18	HAL-07	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Seuranta ja valvonta	1	1	1	1	1	1	1	1	1	1	1
19	HAL-07.1	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Seuranta ja valvonta - tietojen käyttö ja luovutukset	1	1	0	2	1	1	1	1	1	1	1
20	HAL-08	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Häiriöiden hallinta	1	1	1	1	1	1	1	1	1	1	1
21	HAL-09	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Dokumentointi	1	1	2	1	1	1	1	1	1	1	1
22	HAL-09.1	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Dokumentointi - ajantasaisuus	1	1	2	1	1	1	1	1	1	1	1
23	HAL-10	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Henkilöstön luotettavuuden arviointi	1	1	1	2	1	1	1	1	1	1	1
24	HAL-10.1	Salassa pidettävä	Kriittinen	Kriittinen	Erityinen h	Henkilöstön luotettavuuden arviointi - turvallisuusselvitys	1	0	2	0	1	1	1	1	1	1	1
25	HAL-11	Salassa pidettävä	0	0	Henkilötiet	Salassapito- ja vaitiolovelvollisuus	1	1	1	1	1	1	1	1	1	1	1
26	HAL-12	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Ohjeet	1	1	1	1	1	1	1	1	1	1	1
27	HAL-13	Julkinen	Vähäinen	Vähäinen	Henkilötiet	Koulutukset	1	1	2	1	1	1	1	1	1	1	1

Jokaiselle kriteerille määritellään sisältyykö se käyttötapaukseen ja onko se valinnainen

1. Välilehti ”Käyttötapauskriteerit”
2. Määrittele jokaisen kriteerin osalta
   a) Kriteeri ei sisälly käyttötapaukseen = 0
   b) Kriteeri sisältyy käyttötapaukseen = 1 tai,
   c) Kriteeri on valinnainen = 2
3. Määrittelyt tehdään kyseisen käyttötapauksen sarakkeeseen jokaiselle kriteerille erikseen

Käyttötapausten vaikutus kriteerien valintaan

- Ei sisälly käyttötapaukseen (0)
  - Kriteeri ”**Ei sisälly arviointiin**” riippumatta siitä, miten muut esiehdot on asetettu
- Olennainen (1)
  - Kriteerin sisältyminen arviointiin määräytyy turvallisuus-tasojen sekä mahdollisesti muiden esiehtojen perusteella
- Valinnainen (2)
  - Kriteeri on ”**Valinnainen**” paitsi, jos se ei sisälly arviointiin muiden esiehtojen perusteella

➢ Työkalu määrittelee siis kriteerien olennaisuuden, valinnaisuuden tai jättämisen arvioinnin ulkopuolelle käyttötapausten, turvallisuustasojen sekä osa-alueiden valinnan yhteisvaikutuksen perusteella.

Tukimateriaaleja

Kriteeristön käyttöä tukevia materiaaleja

- Tiedonhallintalautakunnan suositukset (vm.fi/tiedonhallintalautakunta)
  - Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta
  - Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä
  - Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa
- Tietoturvallisuuden auditointityökalu viranomaisille (Katakri 2020)
- Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)
- Traficomin Kyberturvallisuuskeskus (kyberturvallisuuskeskus.fi)
- Tietosuojavaltuutetun toimiston sivusto (tietosuoja.fi)
- ISO/IEC 27001 ja 27002 –standardit

Tiedonhallintalautakunta
Informationshanteringsnämnden

Lisätietoja

mika.kuronen@gov.fi
tuula.seppo@dvv.fi
hanna.heikkinen@dvv.fi