Käyttäjän ohje

Tämä ohje kertoo, miten täytät SecMeter TSAT -lomakkeen (SecMeter TSAT.pdf) ja miten sen automaattinen pisteytys, yhteenveto ja johdon raportti toimivat.

Tämä on yrityksen sisäiseen käyttöön tarkoitettu kevennetty kartoitus, ei sertifioitu tai virallinen ISO 27001 -auditointityökalu eikä korvaa ISO 27001 -sertifiointiauditointia tai akkreditoidun auditoijan arviota.

1. Lomakkeen rakenne

Lomake on viisisivuinen, ja jokaisen sivun yläreunassa on tummansininen navigointipalkki, josta pääset suoraan mille tahansa sivulle klikkaamalla:

- Etusivu - perustiedot
- Arviointi 1/2 ja Arviointi 2/2 - kymmenen osa-alueen pisteytys
- Yhteenveto - automaattisesti laskettu kokonaistulos
- Johdon raportti - automaattisesti kirjoitettu tekstiraportti

Aktiivinen sivu näkyy palkissa valkoisena, muut sivut tummansinisenä.

2. Värikoodit

Väri / kenttä	Selitys
Valkoinen kenttä	Täytettävä kenttä. Voit kirjoittaa tekstiä, ja pitkä teksti rivittyy automaattisesti kentän sisällä.
Vaaleanpunainen kenttä	Automaattisesti laskettu ja lukittu kenttä. Et voi kirjoittaa siihen itse - sen sisältö päivittyy Arviointi-sivujen pisteytyksen perusteella.
Tummansininen palkki	Navigointi (ylä) ja sivutieto (ala). Klikkaamalla ylä-palkin osiota siirryt suoraan kyseiselle sivulle.

3. Etusivun täyttäminen

Täytä ensin lomakkeen perustiedot:

- Arvioitavan yrityksen nimi
- Arvioijan nimi / rooli
- Arviointipäivä (muoto pp.kk.vvvv)
- Toimittajan yhteyshenkilö
- Arvioinnin laajuus / kuvaus - vapaa kuvaus siitä, mitä arviointi kattaa

Yrityksen nimi ja arviointipäivä näkyvät myöhemmin myös automaattisesti generoidussa johdon raportissa, joten kannattaa täyttää ne ensin.

4. Osa-alueiden pisteytys (Arviointi 1/2 ja 2/2)

Lomakkeella arvioidaan kymmenen tietoturvan osa-aluetta, jotka pohjautuvat ISO/IEC 27001:2022 -standardin Annex A -kontrolliteemoihin (ks. luku 8 alla):

- tietoturvapolitiikka ja hallinto, riskienhallinta,
- pääsynhallinta,
- salaus ja tietosuoja,
- verkon ja infrastruktuurin turvallisuus,
- haavoittuvuuksien hallinta, poikkeamienhallinta,
- jatkuvuuden- ja toipumisenhallinta,
- alihankkijoiden ja toimitusketjun hallinta sekä henkilöstön tietoturvatietoisuus.

Jokaisen osa-alueen alla lomakkeessa näkyy harmaalla myös vastaava ISO 27001 -viite.

Jokaiselle osa-alueelle:

1. Valitse pudotusvalikosta pistemäärä 1-5.
2. Kirjoita tarvittaessa lyhyt huomio tai peruste vieressä olevaan tekstikenttään (vapaaehtoinen).

Pisteytysasteikko on sama kaikilla osa-alueilla:

Piste	Tarkoittaa
1	Puutteellinen
2	Heikko
3	Tyydyttävä
4	Hyvä
5	Erinomainen

Osa-alueen voi jättää myös tyhjäksi ("-"), jos sitä ei ole vielä arvioitu - yhteenveto ja raportti laskevat silloin keskiarvon vain täytettyjen osa-alueiden perusteella ja kertovat, montako osa-aluetta on vielä arvioimatta.

5. Yhteenveto-sivu

Yhteenveto-sivu päivittyy automaattisesti antamiesi pisteiden mukaan, eikä sitä täytetä käsin:

- Jokaisen osa-alueen pisteet näkyvät vaaleanpunaisissa, lukituissa kentissä.
- Kokonaispistemäärä-kenttä näyttää keskiarvon, arvioitujen osa-alueiden määrän (esim. 8/10) ja yhteispisteet.

Riskiluokitus-kenttä näyttää sanallisen riskitason keskiarvon perusteella:

Keskiarvo	Riskiluokitus
4,0 - 5,0	Matala riski
3,0 - 3,99	Kohtalainen riski
2,0 - 2,99	Korkea riski
alle 2,0	Kriittinen riski

6. Johdon raportti -sivu

Viimeinen sivu kirjoittaa automaattisesti valmiin, luettavan tekstiraportin, joka sisältää:

- Yrityksen nimen ja arviointipäivän
- Kokonaiskeskiarvon ja riskiluokituksen sanallisesti
- Vahvuudet - osa-alueet, jotka saivat 4 tai 5 pistettä
- Kehityskohteet - osa-alueet, jotka saivat 1 tai 2 pistettä
- Huomion siitä, jos kaikkia osa-alueita ei ole vielä arvioitu
- Suosituksen jatkotoimista riskitason perusteella

Raportti on tarkoitettu sellaisenaan johdolle esitettäväksi tai kopioitavaksi esimerkiksi sähköpostiin tai esitykseen.

7. Vinkki

- Voit lähettää sen sellaisenaan eteenpäin. Vastaanottaja näkee sekä pisteytyksen että valmiin raportin. Vaaleanpunaisia kenttiä ei voi eikä tarvitse muokata käsin, ne ovat aina pisteytyksen peilikuva.

8. ISO/IEC 27001:2022 -perusta

Lomakkeen kymmenen osa-aluetta on koottu ISO/IEC 27001:2022 -standardin Annex A -kontrolliteemoista sekä standardin päävaatimuksista (kohdat 6.1 ja 9.1) kevennetyksi, käytännönläheiseksi kolmannen osapuolen arviointirungoksi. Alla oleva taulukko näyttää, mihin ISO 27001 -kohtiin kukin osa-alue pääasiassa perustuu.

Lomakkeen osa-alue	ISO/IEC 27001:2022 -viite
1. Tietoturvapolitiikka ja hallinto	Annex A 5.1, 5.2, 5.4
2. Riskienhallinta	Kohdat 6.1 ja 9.1 (pääkohdat, ei Annex A)
3. Pääsynhallinta	Annex A 5.15-5.18, 8.2, 8.5
4. Salaus ja tietosuoja	Annex A 5.12, 5.34, 8.24
5. Verkon ja infrastruktuurin turvallisuus	Annex A 8.20-8.23
6. Haavoittuvuuksien hallinta	Annex A 8.8, 8.9, 8.32
7. Poikkeamienhallinta	Annex A 5.24-5.28
8. Jatkuvuuden- ja toipumisenhallinta	Annex A 5.29, 5.30, 8.13, 8.14
9. Alihankkijoiden ja toimitusketjun hallinta	Annex A 5.19-5.23
10. Henkilöstö ja tietoturvatietoisuus	Annex A 6.1-6.8