

SecMeter

TSAT - Katakri security assessment tool (Katakri 2020)

Käyttäjän ohje

Tämä ohje kertoo, miten täytät SecMeter TSAT -lomakkeen Katakri 2020 -itsearviointiversion (SecMeter_TSAT_Katakri2020.pdf) ja miten sen automaattinen pisteytys, yhteenveto ja johdon raportti toimivat. Lomake kattaa kaikki 61 Katakri 2020 -kriteeristön vaatimusta ja pohjautuu viralliseen Katakri 2020 -arviointityökaluun (v1.01).

Huomio

Tämä arviointiväline on tarkoitettu yrityksen sisäiseen Katakri-arviointiin, ei virallinen viranomaisen suorittama Katakri-arviointi tai -todistus.

Vaatimusten pitkät kuvaukset, lisätiedot ja lähdeviittaukset (906/2019, 1101/2019, EU 2013/488) on jätetty tästä työvälineestä pois.

1. Lomakkeen rakenne

Lomake on 26-sivuinen, ja jokaisen sivun yläreunassa on tummansininen navigointipalkki, jossa on kuusi osiota. Klikkaamalla osiota siirryt suoraan sen ensimmäiselle sivulle:

- Etusivu - perustiedot
- T Turvallisuus (5 sivua)
- F Fyysinen turvallisuus (9 sivua)
- I Tekninen turvallisuus (9 sivua)
- Yhteenveto - automaattisesti laskettu tilanne osa-alueittain
- Johdon raportti - automaattisesti kirjoitettu tekstiraportti

Aktiivinen osio näkyy palkissa valkoisena, muut osiot tummansinisenä. Otsikkotekstin alla T-, F- ja I-osioden arviointisivuilla on lisäksi "< Edellinen" ja "Seuraava >" -linkit, joilla voi selata koko 23 arviointisivun sarjaa (T-osio, sitten F-osio, sitten I-osio) järjestyksessä ilman navigointipalkkiin palaamista.

Sivu	Navigointipalkin nimi	Sisältö
1	Etusivu	Perustiedot ja tavoiteltava turvallisuusluokka (TL)
2-6	T Turvallisuus	Vaatimukset T-01 - T-13 (13 kpl, 5 sivua)
7-15	F Fyysinen turvallisuus	Vaatimukset F-01 - F-08.4 (27 kpl, 9 sivua)
16-24	I Tekninen turvallisuus	Vaatimukset I-01 - I-21 (21 kpl, 9 sivua)
25	Yhteenveto	Osa-aluekohtaiset tilastot, kokonaisarvio ja näytön valmius
26	Johdon raportti	Automaattisesti generoitu tekstiraportti

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. Kentän sisältö päivittyy vaatimusten arvioinnin perusteella.
Tummansininen palkki	Klikkaamalla yläpalkin osiota siirryt suoraan sen ensimmäiselle sivulle.

3. Etusivun täyttäminen

Täytä ensin lomakkeen perustiedot:

- Arvioitavan yrityksen nimi
- Järjestelmä / kohde - mitä järjestelmää tai kokonaisuutta arviointi koskee
- Arvioijan nimi / rooli
- Arviointipäivä (muoto pp.kk.vvvv)
- Tavoiteltava turvallisuusluokka (TL). Valitse TL IV, TL III tai TL II
- Arvioinnin laajuus / kuvaus. Vapaa kuvaus siitä, mitä arviointi kattaa

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

4. Vaatimusten arviointi (23 arviointisivua)

Lomakkeella arvioidaan kaikki 61 Katakri 2020 -vaatimusta, jaoteltuna kolmeen osa-alueeseen:

Turvallisuus (T, 13 vaatimusta),

Fyysinen turvallisuus (F, 27 vaatimusta)

Tekninen turvallisuus (I, 21 vaatimusta).

"Pyydettävä näyttö" -rivi, kertoo minkälaista dokumentaatiota tai todistetta arviointitulosta varten kannattaa pyytää.

Jokaiselle vaatimukselle täytetään kaksi pudotusvalikkoa oikeassa reunassa, päällekkäin:

1. Käy läpi tarkastuskysymykset ja tarkista pyydetty näyttö.
2. Valitse ylemmästä valikosta ("Arviointitulos") vaatimuksen arviointitulos.
3. Valitse alemmasta valikosta ("Näytön valmiusaste") kuinka valmiina näyttö on esitettäväksi auditoijalle.

Arviointiasteikko on sama kaikilla vaatimuksilla ja vastaa virallisen Katakri 2020 -työkalun asteikkoa:

Arviointitulos	Tarkoittaa
1 - Puutteellinen	Turvallisuustoimenpiteitä ei ole määritelty tai ne eivät täytä vähimmäisvaatimuksia
2 - Osittainen	Toimenpiteitä on suunnitteilla tai toteutettu osittain, mutta ne eivät ole vielä riittäviä tai dokumentoituja
3 - Perustaso (Lakisääteinen)	Turvallisuusvaatimukset täyttyvät ja perustoimenpiteet ovat dokumentoituja ja käytössä. Tämä on minimitaso hyväksynnälle
4 - Hallittu ja valvottu	Turvallisuuskäytännöt ovat vakiintuneita, valvottuja ja osoitettavissa
5 - Optimoitu	Toimintaa kehitetään jatkuvasti ja turvallisuus on integroitunut syvälle yrityksen prosesseihin
Ei sovellu	Vaatus ei koske arvioitavaa kohdetta - jätetään pois keskiarvolaskennasta

Vaatumuksen voi jättää myös tyhjäksi ("-"), jos sitä ei ole vielä arvioitu. Yhteenveto ja raportti laskevat silloin tilanteen vain täytettyjen vaatimusten perusteella ja kertovat, montako vaatimusta on vielä arvioimatta.

Näytön valmiusaste on erillinen kolmiportainen asteikko, jolla seurataan, onko vaatimuksen täyttymisestä olemassa esitettävää todistetta, riippumatta siitä, mikä arviointitulos on.

Vaatus voi olla esimerkiksi käytännössä hyvin toteutettu (taso 4-5), mutta silti "Ei näyttöä", jos kirjallista todistetta ei ole vielä koottu:

Näytön valmiusaste	Tarkoittaa
Aukoton näyttö (Valmis)	Todiste on olemassa, ajan tasalla ja näytettävissä auditoijalle heti (esim. allekirjoitettu dokumentti, voimassa oleva loki, valokuva lukituksesta).
Osittainen näyttö (Päivitettävä)	Prosessi tai suojaus on käytössä, mutta kirjallinen todiste puuttuu, on vanhentunut (esim. luonnosvaiheessa) tai sitä ei ole testattu.
Ei näyttöä (Puuttuu)	Vaatumuksen täyttymisestä ei ole mitään dokumentoitua tai todennettavaa näyttöä.

5. Yhteenveto-sivu

Yhteenveto-sivu päivittyy automaattisesti antamiesi arviointien mukaan, eikä sitä täytetä käsin. Sivun näyttää osa-aluekohtaisen roll-upin:

- Jokaiselle kolmelle osa-alueelle (T, F, I): vaatimusten kokonaismäärä, montako on arvioitu numeerisesti, ja osa-alueen keskiarvo 1-5-asteikolla (vaaleanpunaiset, lukitut kentät). "Ei sovellu" -vaatimukset jätetään pois keskiarvolaskennasta.
- Kokonaistilanne-kenttä näyttää, montako 61 vaatimuksesta on arvioitu ja koko lomakkeen keskiarvon.
- Kokonaisarvio-kenttä näyttää sanallisen kypsyystason keskiarvon perusteella:

Keskiarvo (1-5)	Kypsyystaso
4,5 - 5,0	5 - Optimoitu
3,5 - 4,49	4 - Hallittu ja valvottu
2,5 - 3,49	3 - Perustaso (Lakisääteinen)
1,5 - 2,49	2 - Osittainen
alle 1,5	1 - Puutteellinen

- Näytön valmius -kenttä näyttää, montako vaatimusta on arvioitu näytön osalta, ja kuinka moni niistä on kussakin kolmesta valmiusluokasta (Aukoton / Osittainen / Ei näyttöä).

6. Johdon raportti -sivu

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

- Yrityksen nimen, arviointipäivän ja tavoitellun turvallisuusluokan
- Kuinka moni 61 vaatimuksesta on arvioitu ja kokonaiskeskiarvon sekä sitä vastaavan kypsyystason
- Osa-aluekohtaiset keskiarvot yhdellä rivillä (T, F, I), sekä heikoimman ja vahvimman osa-alueen
- Listan vaatimuksista, jotka alittavat tason 3 (Perustaso / Lakisääteinen, minimitaso hyväksynnälle)
- Näytön valmiusasteen kokonaismäärät (Aukoton / Osittainen / Ei näyttöä)
- Erillisen listan vaatimuksista, joilta puuttuu näyttö kokonaan ("Ei näyttöä") - nämä kannattaa priorisoida ennen auditointia riippumatta arviointitulos-pistemäärästä
- Huomion siitä, jos kaikkia 61 vaatimusta ei ole vielä arvioitu
- Suosituksen jatkotoimista kokonaiskeskiarvon perusteella

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