SecMeter - TSAT Third-party security assessment tool

Kolmannen osapuolen tietoturva-arviointi (Third-Party Security Assessment Tool)

Tämä lomake ohjaa kolmannen osapuolen / toimittajan tietoturvan arvioinnin läpi. Osa-alueet pohjautuvat ISO/IEC 27001:2022 -standardin Annex A -kontrolliteemoihin. Täytä ensin perustiedot alla, siirry sitten Arviointi-sivuille pisteyttämään kymmenen osa-aluetta (1-5), ja Yhteenveto- sekä Johdon raportti -sivut päivittyvät automaattisesti antamiesi pisteiden perusteella. Vaaleanpunaiset kentät ovat lukittuja ja lasketaan automaattisesti.

Arvioitavan yrityksen nimi

Arvioijan nimi / rooli

Arviointipäivä (pp.kk.vvvv)

Toimittajan yhteyshenkilö

Arvioinnin laajuus / kuvaus

Asteikko kaikilla osa-alueilla: 1 = puutteellinen, 2 = heikko, 3 = tyydyttävä, 4 = hyvä, 5 = erinomainen.

Huomio: osa-alueet on koottu ISO/IEC 27001:2022 Annex A -kontrolliteemoista kevennetyksi arviointirungoksi. Kyseessä ei ole sertifioitu tai virallinen ISO 27001 -auditointityökalu.

SecMeter - TSAT Third-party security assessment tool

Osa-alueiden pisteytys (valitse pistemäärä 1-5 ja lisää tarvittaessa huomio)

Osa-alue	Pisteet	Huomio / peruste (vapaaehtoinen)
1. Tietoturvapolitiikka ja hallinto (ISO/IEC 27001:2022, Annex A 5.1, 5.2, 5.4) Onko yrityksellä dokumentoitu, johdon hyväksymä tietoturvapolitiikka ja nimetyt vastuut?	-	
2. Riskienhallinta (ISO/IEC 27001:2022, kohdat 6.1 ja 9.1) Tehdäänkö säännöllisiä riskiarviointeja ja seurantaa osana johtamisjärjestelmää?	-	
3. Pääsynhallinta (ISO/IEC 27001:2022, Annex A 5.15-5.18, 8.2, 8.5) Käytetäänkö vähimpien oikeuksien periaatetta, roolipohjaisia käyttöoikeuksia ja monivaiheista tunnistautumista?	-	
4. Salaus ja tietosuoja (ISO/IEC 27001:2022, Annex A 5.12, 5.34, 8.24) Onko data luokiteltu ja salattu levossa ja siirron aikana, ja täyttääkö toiminta tietosuojavaatimukset?	-	
5. Verkon ja infrastruktuurin turvallisuus (ISO/IEC 27001:2022, Annex A 8.20-8.23) Onko verkko segmentoitu ja ulkoiset rajapinnat suojattu, suodatettu ja valvottu?	-	

SecMeter - TSAT Third-party security assessment tool

Osa-alueiden pisteytys (valitse pistemäärä 1-5 ja lisää tarvittaessa huomio)

Osa-alue	Pisteet	Huomio / peruste (vapaaehtoinen)
6. Haavoittuvuuksien hallinta (ISO/IEC 27001:2022, Annex A 8.8, 8.9, 8.32) Tehdäänkö säännöllisiä haavoittuvuusskannauksia, ja hallitaanko muutokset ja korjaukset hallitusti?	-	
7. Poikkeamienhallinta (ISO/IEC 27001:2022, Annex A 5.24-5.28) Onko yrityksellä testattu tietoturvapoikkeamien havainnointi- ja käsittelysuunnitelma?	-	
8. Jatkuvuuden- ja toipumisenhallinta (ISO/IEC 27001:2022, Annex A 5.29, 5.30, 8.13, 8.14) Onko liiketoiminnan jatkuvuus-, varmuuskopiointi- ja palautumissuunnitelmat testattu säännöllisesti?	-	
9. Alihankkijoiden ja toimitusketjun hallinta (ISO/IEC 27001:2022, Annex A 5.19-5.23) Arvioidaanko myös yrityksen omat alihankkijat ja pilvipalveluntarjoajat (neljännen osapuolen riski)?	-	
10. Henkilöstö ja tietoturvatietoisuus (ISO/IEC 27001:2022, Annex A 6.1-6.8) Saako henkilöstö taustatarkastukset, säännöllistä tietoturvakoulutusta ja tietojenkalastelusimulaatioita?	-	

SecMeter - TSAT Third-party security assessment tool

Automaattinen yhteenveto (päivittyy Arviointi-sivujen pisteytyksen mukaan)

Osa-alue	Pisteet
1. Tietoturvapolitiikka ja hallinto	
2. Riskienhallinta	
3. Pääsynhallinta	
4. Salaus ja tietosuoja	
5. Verkon ja infrastruktuurin turvallisuus	
6. Haavoittuvuuksien hallinta	
7. Poikkeamienhallinta	
8. Jatkuvuuden- ja toipumisenhallinta	
9. Alihankkijoiden ja toimitusketjun hallinta	
10. Henkilöstö ja tietoturvatietoisuus	

Kokonaispistemäärä:

Riskiluokitus:

SecMeter - TSAT Third-party security assessment tool

Johdon raportti (automaattisesti generoitu yhteenveto arvioinnin tuloksista)