

RISKIEN KARTOITTAMINEN JA ARVIOINTI

Hallintokunta/tytäryhteisö:

Kartoituksen ajankohta:

Osallistujat:

Vastuuhenkilö:

Riski	Riski-luokka	Riskin tarkennus	Nykyiset hallintakeinot	T	V	T×V	Toimenpiteet	Vastuuhenkilö ja aikataulu

Ohje:

TARKOITUS JA PERIAATTEET

Riskikartoituksen tarkoitus on tunnistaa ja arvioida keskeiset riskit, jotka voivat estää tavoitteiden saavuttamista, heikentää palvelujen laatua tai aiheuttaa taloudellisia, oikeudellisia tai mainehaittoja.

1) Tunnista riski

Kirjaa riski selkeästi. Kirjaa riski aina mahdollisimman konkreettisesti: mitä voisi tapahtua (esim. "järjestelmäkatko estää asiainninn"), miksi se voisi tapahtua (esim. "varmistuksia ei testata") ja mitä siitä aiheutuu (esim. "palvelu keskeytyy, mainehaitta, lisäkustannuksia").

2) Luokittele

Valitse 1 pääluokka:

STR = strateginen riski (tavoitteet, elinvoima, palveluverkko, isot linjaukset),

OPS = operatiivinen/toiminnallinen (palvelutuotanto, prosessit, kumppanit, jatkuvuus),

FIN = talous- ja rahoitusriski (budjetti, kustannukset, rahoitus, korko, saatavat) ja

COM = vaatimusten mukaisuus- ja maineriski (lait, päätöksenteko, hankinnat, eettisyys, luottamus).

Jos riski liittyy ensisijaisesti tavoitteisiin → STR

Jos riski liittyy arjen toimintaan/palveluun → OPS

Jos riski liittyy määrärahoihin/rahoitukseen → FIN

Jos riski liittyy lakiin/velvoitteisiin/maineeseen → COM.

Lisäksi voit käyttää tarvittaessa riskitarkenteita: H=henkilöstö, O=omaisuus, T=toimittaja Y=ympäristö, H=hankinta, TU=turvallisuus, TT=tietosuoja, J=tieto-, kyber- ja tietojärjestelmä, S=sopimukset, V=viestintä, M=maine.

Riskien luokittelun viitekehyksenä käytetään kansainvälistä COSO-viitekehystä. COSO on kansainvälinen sisäisen valvonnan ja riskienhallinnan viitekehys (Committee of Sponsoring Organizations of the Treadway Commission), jota käytetään organisaation riskien tunnistamiseen, arviointiin ja hallintaan sekä valvonnan toimivuuden jäsentämiseen.

3) Kuvaa nykyiset hallintakeinot

Mitä jo tehdään riskin ehkäisemiseksi tai vaikutusten rajaamiseksi (ohjeet, prosessit, valvonta, tekniset suojaukset, seuranta).

4) Arvioi riski (nykytilassa)

Anna arviot: Todennäköisyys (T) 1–5 ja Vaikutus (V) 1–5 → riskitaso = $T \times V$.

Tulkinta: 1–6 matala, 8–12 keskitaso, 15–25 korkea.

5) Määritä toimenpiteet

Kirjaa tarvittavat toimenpiteet.

6) Määritä vastuuhenkilö ja aikataulu

Kirjaa vastuuhenkilö(t) ja aikataulu