

FRAKTAL

Tietoturvan vuosikello

FRAKTALIN NÄKÖKULMIA / KESÄKUU 2025



Tietoturvan vuosikello

Sisällys

Johdanto

Tietoturvan vuosikello

Tietoturvan vuosikellon rakentamisen vaiheet

1. Tunnista toistuvat tehtävät
2. Aikatauluta tehtävät
3. Määritä vastuut
4. Valitse esitystapa

Seurannan varmistaminen

Esimerkkejä tietoturvan vuosikelloista



Johdanto

Tietoturvasta puhutaan usein vasta silloin, kun jokin menee pahasti pieleen – otsikot kertovat tietomurroista ja niiden vakavista seurauksista. Yrityksen kannalta tietoturvan laiminlyönti voi kuitenkin aiheuttaa liiketoiminnalle merkittäviä riskejä myös ilman suurta julkisuutta.

Tietoturvan vuosikello on työkalu, joka kokoaa tärkeimmät tietoturvatehtävät aikataulutettuun muotoon vuoden ajalle. Se auttaa varmistamaan, että keskeiset toimenpiteet eivät unohdu arjen kiireessä.

Tässä ohjeessa keskitymme siihen, miten yrityksessä voidaan käytännössä varmistaa, että tietoturvaa johdetaan suunnitelmallisesti ja että keskeiset toimenpiteet tulevat tehtyä ajallaan.

Tietoturvan hallinta helpottuu merkittävästi, kun:

1. tietoturvaan liittyvät keskeiset tehtäväkokonaisuudet on tunnistettu,
2. niiden asianmukaisesta toteutuksesta huolehditaan, ja
3. tehtävien toteutumista seurataan säännöllisesti.

Tietoturvan vuosikello toimii erinomaisena työkaluna näiden asioiden organisointiin ja seurantaan.



Tietoturvan vuosikello

TOISTUVAT TEHTÄVÄT HALLINTAAN

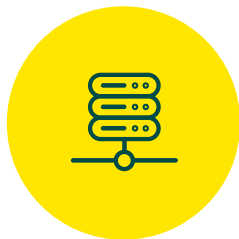
Tietoturvan vuosikello on käytännönläheinen työkalu, jonka avulla tietoturvatehtävät voidaan ryhmitellä ja aikatauluttaa selkeästi. Se perustuu ajatukseen, että tietyt tietoturvatoimet toistuvat säännöllisesti – esimerkiksi puolivuositain tai vuosittain. Kun nämä toimet sijoitetaan suunnitellusti kalenterivuoden varrelle, tietoturvan hallinta muuttuu systemaattiseksi ja rutiininomaiseksi osaksi arkea.

Yritys voi samalla huomioida oman toimintansa rytmin – esimerkiksi ruuhkahuiput ja lomakaudet – ja sijoittaa tietoturvatehtävät ajankohtiin, jolloin niihin ehditään keskittyä. Esimerkiksi henkilöstön koulutuksia ei kannata ajoittaa vuoden kiireisimmille viikoille.

TAVOITE

Tietoturvan vuosikellon tavoitteena on varmistaa, että tietoturvatehtävät tunnistetaan, dokumentoidaan, toteutetaan ajallaan – ja että niiden etenemistä seurataan johdonmukaisesti.

Tietoturvan vuosikellon rakentamisen vaiheet



1. Tunnista toistuvat tehtävät

Listaa vuosittain, puolivuositain tai neljännesvuositain toistuvat tietoturvatehtävät, kuten riskienarvioinnit, koulutukset, tarkastukset ja sopimuspäivitykset.



2. Aikatauluta tehtävät

Sijoita tehtävät kalenterivuodelle ottaen huomioon yrityksen ruuhkahuiput ja lomajaksot – näin varmistetaan, että tehtäville on aikaa ja resursseja.



3. Määritä vastuut

Nimeä jokaiselle tehtävälle vastuutaho (esim. rooli, tiimi tai henkilö), joka huolehtii sen toteutuksesta ja raportoinnista.



4. Valitse esitystapa

Toteuta vuosikello formaattiin, jota on helppo päivittää ja seurata – taulukko, tehtävälista tai visuaalinen kalenterikuvaus.

Kun vuosikello on valmis, varmista, että tehtävien toteuttamiselle on riittävä seuranta.



1. Tunnista toistuvat tehtävät

Tietoturvan vuosikellossa esiintyy tyypillisesti sellaisia tehtäviä, joita esimerkiksi tietoturvastandardit tai tietoturvan hyvät käytännöt edellyttävät. Näitä ovat esimerkiksi riskienhallintaan liittyvät tehtävät, ohjeiden säännöllinen katselmointi ja tietoturvakoulutukset. Kun rakennat omaa vuosikelloa yritykselle, voit miettiä, onko teillä (tai olisiko teillä syytä olla!) vuosikellossa toimia seuraavilta osa-alueilta.

Tietoturvan hallinta ja johtaminen

- Kokoukset ja tiedonjako: säännölliset kokoukset, raportit, ohjeiden katselmointi ja päivittäminen
- Vuosisuunnittelu: budjetointi, tavoitteiden ja mittareiden asettaminen, auditointi- ja testisuunnitelmien laatiminen

Riskienhallinta

- Esimerkiksi riskien tunnistamistyöpajat, riskien arviointi, riskien raportointi organisaation sisällä

Koulutukset ja tietoturvatietoisuus

- Esimerkiksi vuosittaiset koulutukset, kertauskoulutukset, perehdytykset, tietoiskut, tietoturvapäivät, koulutukset tietyille kohderyhmille (esim. johdolle)

Tekniset tietoturvan hallintakeinot

- Esimerkiksi käyttöoikeuksien tarkistaminen, varmuuskopioiden testaus
- Tietoturvan testaus (järjestelmät, konfiguraatiot jne)

Poikkeamanhallinta

- Esimerkiksi poikkeamanhallintaprosessin harjoittelu, yhteystietolistojen ajantasaisuuden varmistaminen

Vaatimuksenmukaisuus

- Esimerkiksi ulkoisiin tai sisäisiin vaatimuksiin perustuvat säännöllisesti suoritettavat auditoinnit (ISO 27001), kypsyystasomittaukset tai tietoturvatestaukset
- Yrityksen tekemät toimittajien auditoinnit



2. Aikatauluta tehtävät

Tietoturvatehtävien sijoittaminen kalenterivuodelle kannattaa tehdä liiketoiminnan rytmin mukaan. Ota huomioon esimerkiksi tilikauden vaihteet, lomajaksot ja kiireiset sesongit – tärkeintä on, että tehtäville jää riittävästi aikaa ja että ne saadaan toteutettua kunnolla.

Hyvä aikataulutus tuo:

- ennakoitavuutta, jolloin tehtäviin voidaan valmistautua,
- tasaisuutta, jolloin työkuorma ei kasaudu yhteen ajankohtaan, ja
- sitoutumista, kun tehtävät suunnitellaan järkevään ajankohtaan jo etukäteen.

Esimerkki: Henkilöstön tietoturvakoulutus ajoitetaan syksylle, lomakauden jälkeen – ei kiireiselle, lomaa edeltävälle ajalle.



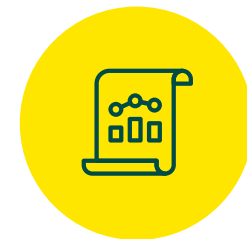
3. Määritä vastuut

Jotta tietoturvatehtävät tulevat varmasti tehdyiksi, jokaiselle tehtävälle on oltava nimetty vastuuhenkilö tai -rooli. Ilman selkeää omistajuutta asiat jäävät helposti tekemättä tai epäselväksi, kuka niistä huolehtii.

Vastuun määrittelyssä on hyvä huomioida:

- tehtävän sisältö – onko tehtävän tekemiseen riittävästi osaamista yrityksessä, vai tarvitaanko sen toteuttamiseen ulkoinen kumppani (esimerkiksi yrityksen IT-kumppani)
- roolit ja resurssit – onko tehtävälle olemassa luonnollinen omistaja?
- tarve dokumentoida vastuu – vuosikelloon kannattaa kirjata vastuurooli näkyviin.

Vinkki: Jos vastuuhenkilö vaihtuu, vuosikello toimii hyvänä työvälineenä vastuiden siirtämiseen uudelle henkilölle.



4. Valitse esitystapa

Tietoturvan vuosikello kannattaa toteuttaa muodossa, joka tekee sen seuraamisesta mahdollisimman helppoa. Jos yrityksessä on jo käytössä muu vuosikello, tietoturvatehtävät kannattaa yhdistää siihen – näin kaikki toimet löytyvät samasta paikasta, ja seuranta yksinkertaistuu.

Jos vuosikelloa ei vielä ole, kannattaa hyödyntää jotakin jo käytössä olevaa välinettä. Tietoturvan vuosikello voidaan toteuttaa esimerkiksi:

- taulukkomuotoisena (esim. Excel, Google Sheets)
- tehtäväluettelona (esim. Planner)
- visuaalisena esityksenä (esim. PowerPoint, Google Slides)

Myös erityisiä vuosikellosovelluksia on saatavilla.

Tärkeintä on valita formaatti, jota on helppo päivittää ja seurata käytännössä.

Seurannan varmistaminen

Pelkkä tietoturvan vuosikellon olemassaolo ei vielä takaa, että tehtävät tulevat hoidetuksi. Jotta vuosikello ohjaisi käytännön toimintaa, jokaiselle tehtävälle tulee määritellä selkeä vastuutaho – esimerkiksi rooli tai tiimi – joka huolehtii sen toteuttamisesta. Tehtävien suorittamisen tueksi tarvitaan riittävät ohjeet, jotta ne voidaan tehdä sovitulla tavalla riippumatta siitä, kuka tehtävän toteuttaa. Lisäksi seuranta helpottaa, että tehtävien suorittamisesta jää jokin dokumentoitu jälki. Tämä voi olla esimerkiksi:

- merkintä tiketointijärjestelmässä,
- kuittaus tehtävälistalla tai
- tieto henkilöstökoulutuksen suorittamisesta.

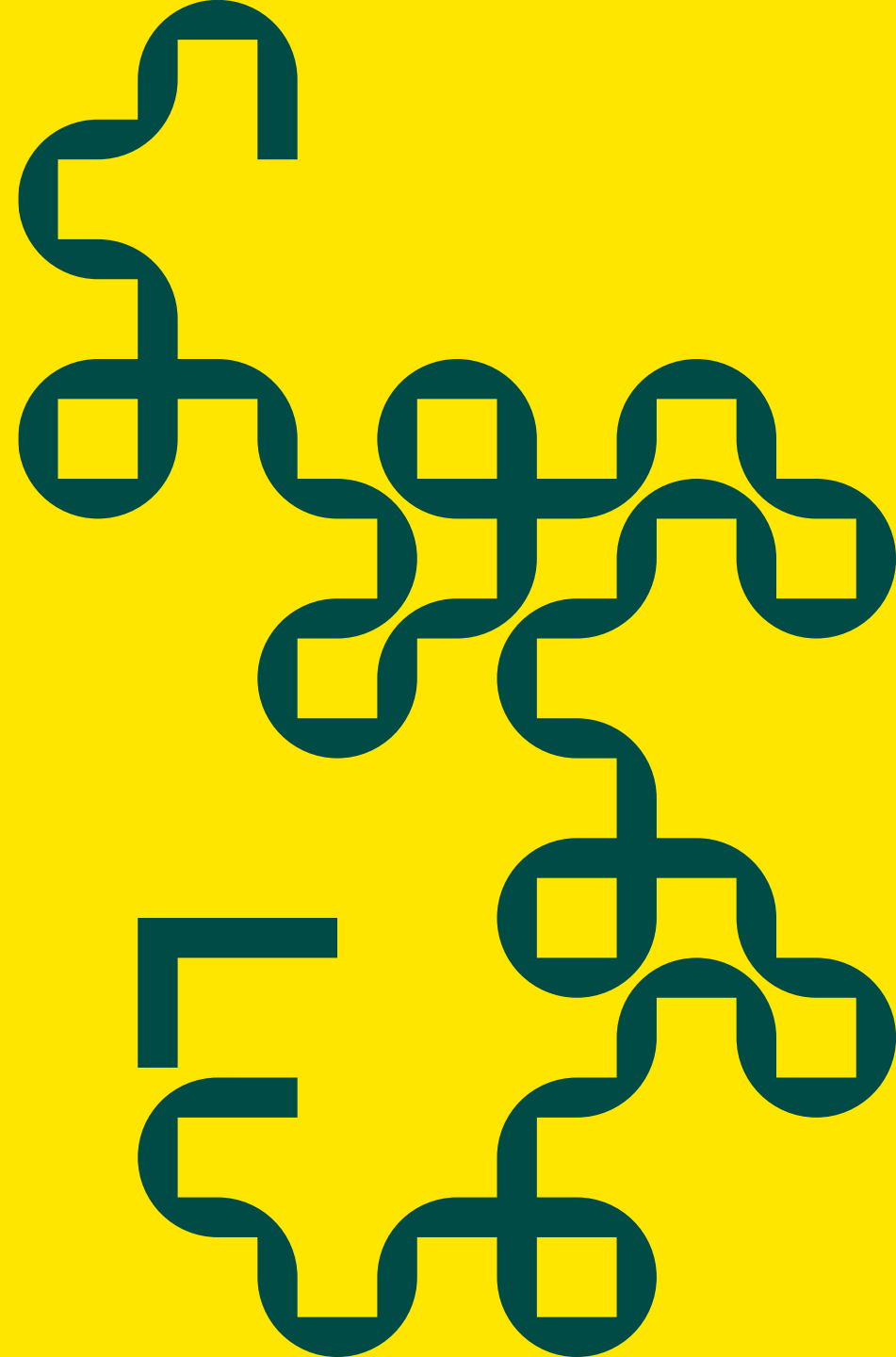
Myös seurannan vastuista tulee sopia. Tehtävien toteutumista voidaan seurata joko tehtäväkohtaisesti nimetyn vastuutahon avulla tai pienemmissä organisaatioissa esimerkiksi säännöllisissä kokouksissa.

Toteutusesimerkki, pieni yritys: Yrityksessä on joka toinen kuukausi toistuva kokous, jonka agendalle lisätään "Tietoturvan seuranta". Kokouksessa:

- käydään läpi tietoturvan ajankohtainen tilanne,
- tarkastellaan mahdollisia havaintoja, riskejä ja uutisia, sekä
- katsotaan, mitä tehtäviä tietoturvan vuosikellon mukaan olisi pitänyt tehdä ja mitä on seuraavaksi tulossa.

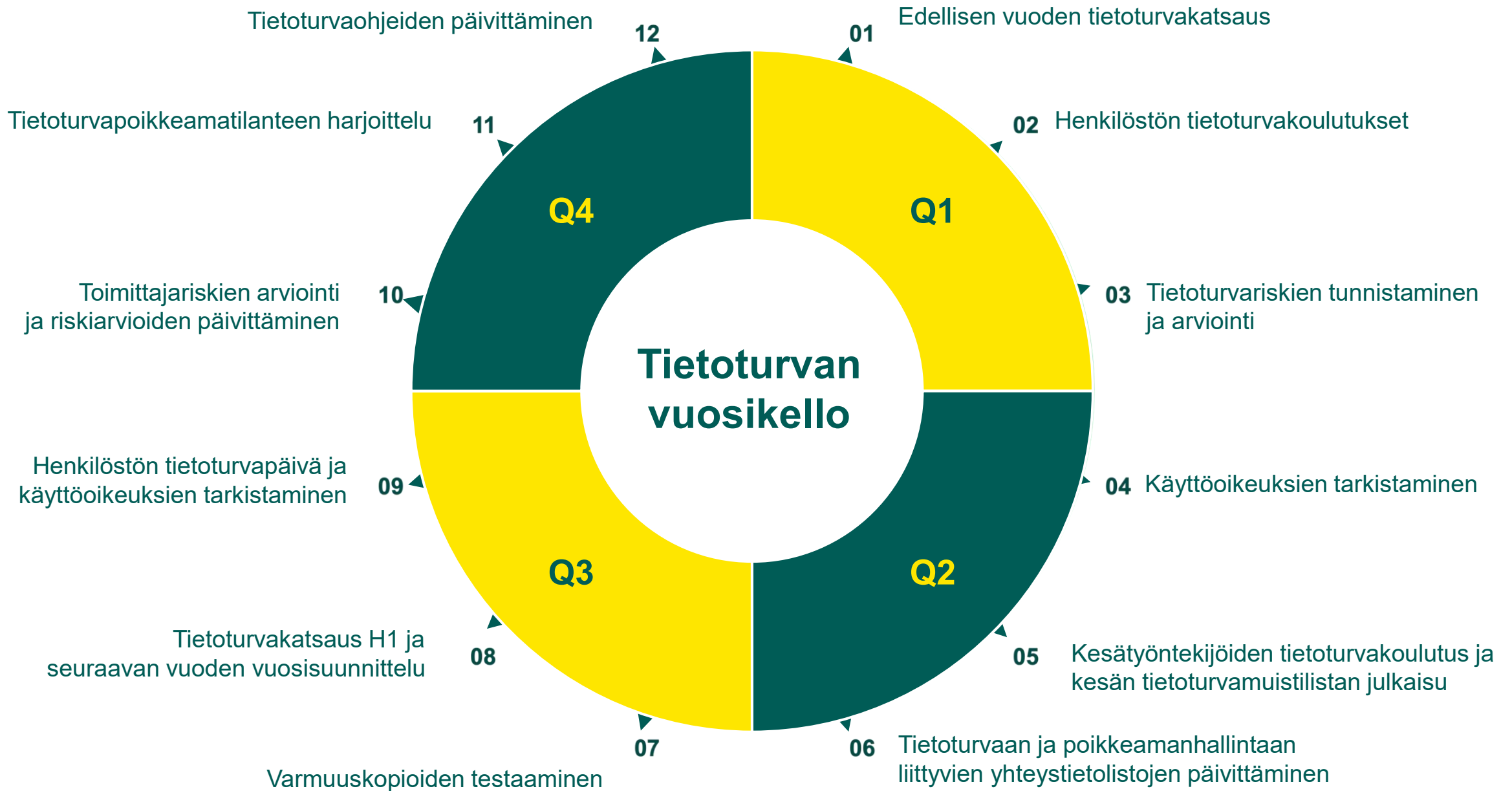
Samalla varmistetaan, että tehtävät on toteutettu sovitusti ja että tulevien tehtävien vastuuhenkilöt ovat tietoisia roolistaan.

Esimerkkejä tietoturvan vuosikelloista



Tietoturvan vuosikello, esimerkki

Kuukausi	Aktiviteetti	Aihepiiri
Tammikuu	Edellisen vuoden tietoturvakatsaus (mittarit, raportit)	Johtaminen
Helmikuu	Henkilöstön tietoturvakoulutukset	Koulutus ja tietoisuus
Maaliskuu	Tietoturvariskien tunnistaminen ja hallinta	Riskienhallinta
Huhtikuu	Käyttöoikeuksien tarkistaminen	Tekniset hallintakeinot
Toukokuu	- Kesän tietoturvamuiistilistan julkaisu - Kesätyöntekijöiden tietoturvakoulutus	- Koulutus ja tietoisuus - Koulutus ja tietoisuus
Kesäkuu	Tietoturvaan ja poikkeamanhallintaan liittyvien yhteystietolistojen päivittäminen	Poikkeamanhallinta
Heinäkuu	Varmuuskopioiden testaus	Tekniset hallintakeinot
Elokuu	- Tietoturvakatsaus H1 - Seuraavan vuoden vuosisuunnittelu	- Johtaminen - Johtaminen
Syyskuu	- Tietoturvapäivä - Käyttöoikeuksien tarkistaminen	- Koulutus ja tietoisuus - Tekniset hallintakeinot
Lokakuu	Toimittajariskien arviointi ja arvioiden päivittäminen	Riskienhallinta
Marraskuu	Tietoturvapoikkeamatilanteen harjoittelu	Poikkeamanhallinta
Joulukuu	Tietoturvaohjeiden päivittäminen	Johtaminen





Fraktal – tietoturva seuraavalle tasolle

www.fraktal.fi