



SFS-ISO 31000

Riskienhallinnan periaatteet – menestyksen avaimet

Lassi Väisänen
Suomen Riskienhallintayhdistys

Tervetuloa luentoaineiston käyttäjäksi

- Tämän luentoaineiston on laatinut Lassi Väisänen Suomen Riskienhallintayhdistyksestä. Aineisto on tuotettu SFS:n projektirahoituksella.
- Aineisto on suunnattu riskien hallinnan kanssa työskenteleville, siihen perehdyttäessä tai opetuskäyttöön ammattikorkeakouluissa ja yliopistoissa. Se esittelee riskienhallintastandardin SFS-ISO 31000 käyttötapoja ja yhteyksiä muihin alan keskeisiin julkaisuihin, sekä riskienhallinnan viitekehyksen, periaatteet ja prosessit.
- Tässä kalvosarjassa ei käsitellä standardia SFS-ISO 31000 yksityiskohtaisesti, vaan se on tarkoitettu johdannoksi riskienhallintaan.

Copyright

- **Tämän luentoaineiston tekijänoikeudet omistaa Suomen Standardisoimisliitto SFS ry.**
- **Esitystä saa vapaasti hyödyntää, myös opetuksessa, ja sitä saa tarvittaessa muokata. Aineistoa lainattaessa lähde tulee mainita.**
- **Aineiston käyttö kaupallisiin tarkoituksiin on kielletty.**
- **Tämä materiaali on päivitetty viimeksi 31.3.2018**

Riskien hallinnan periaatteet – menestyksen avaimet

Riskien, epävarmuuksien jne. arviointiin haetaan kaiken aikaa parhaita tapoja, joilla päästään nopeasti riskihavainnon teosta sitä koskeviin päätöksiin.



Mihin ISO 31000 kiinnittää huomiota?

Muut standardit ja mallit

ISO 31000

Riskien arviointi

Epävarmuuksien arviointi

Useat muut mallit ja menetelmät keskittyvät tunnistamaan ja arvioimaan riskejä

Epävarmuuden kautta arvioidaan tunnistamattomien riskien tai kehityssuuntien (epävarmuuksien) vaikutuksia toimintaympäristöön ja esim. organisaation tuloksen tekokykyyn, kykyyn täyttää vaatimukset jne.

Mennyt tarkastelujakso

Tulevat kvartaalit ja vuodet

Tarkastelu keskittyy kontrollien toimivuuteen. Kohteena aina yksittäinen tunnistettu riski – ei välttämättä suurempi asiakokonaisuus.

Riskienhallinta laajentaa tarkastelunäkökulmaa tulevaisuuteen erilaisten skenaario-, yms. menetelmien avulla. Yksittäisten riskien lisäksi suurempia kokonaisuuksia.

Ohjekeskeinen

Yhdistävä ja kokoava

Tarkastellaan yksittäistä riskiä asetettujen kontrollien näkökulmasta ja kuinka se on käyttäytynyt, eikä keskitytä siihen, miten se tulee käyttäytymään

Tavoitteena tehdä johtopäätöksiä eri havaintojen, analyysien jne. pohjalta. Johtopäätösten avulla voidaan tarjota johdolle parempaa tietoa organisaation riskeistä ja niiden vaikutuksista tulevaisuudessa.

Mihin käyttöön ISO 31000 standardi on hyvä?

Organisaation johto ISO 31000



ISO Guide
Terminology

ISO 19600

Rahavirrat



Emergency and
crisis
management

Tukitoiminnot



ISO 22301

Hankinta

Talous

Henkilöstö

Jne. toiminta

ISO 27001

ASIS

Päätöksen teossa käytettävä sisäisen ja ulkoisen tiedon määrä kasvaa

ISO 9001

ISO 45001

ISO 14001

ISO 14001

Materiaalivirrat

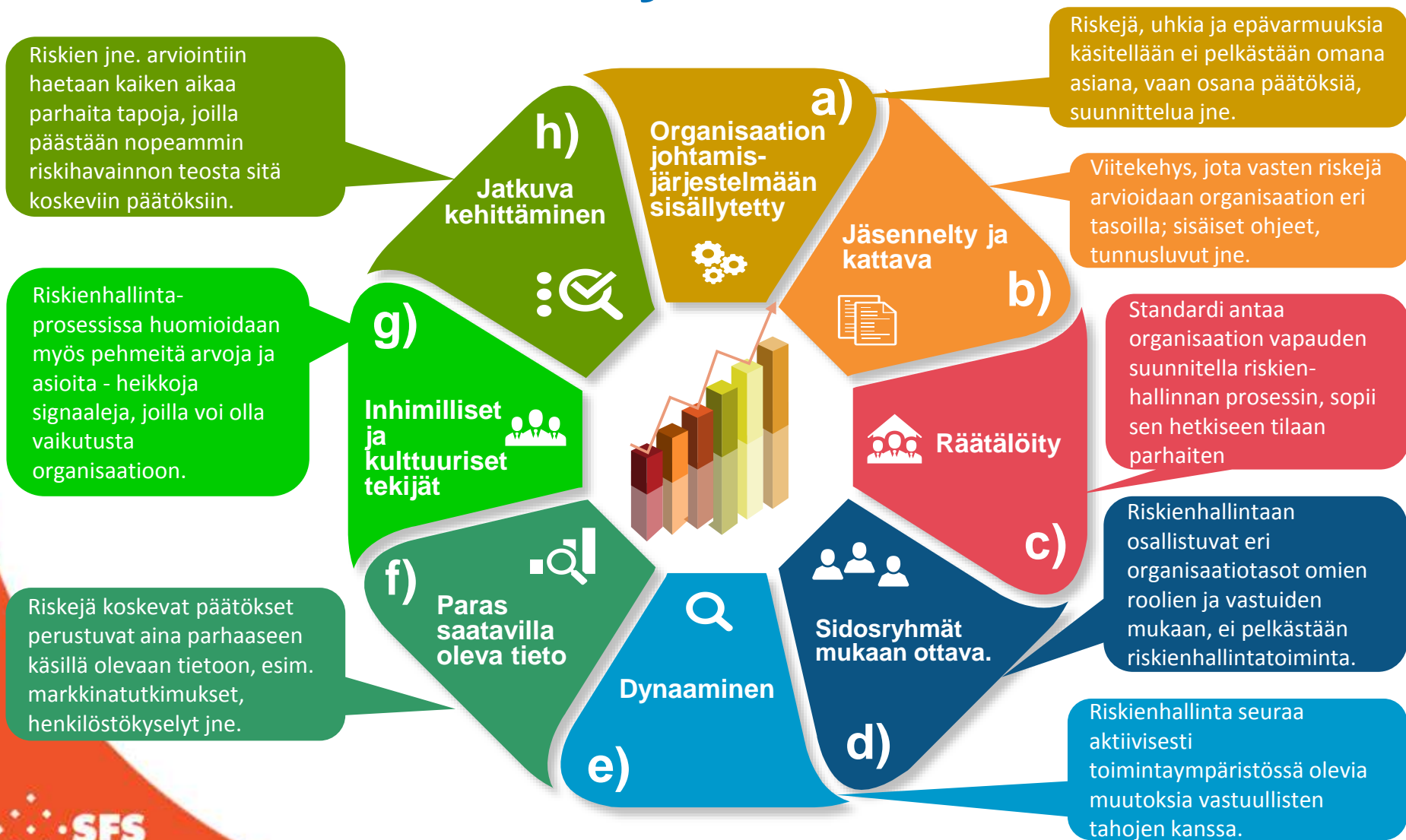


Tuotanto



Terminology

Organisaation arvon luominen ja säilyttäminen



Mitä riskejä missäkin arvioidaan

ISO Management System Standards

- Quality
- Safety and Security
- General management
- Health and Medical
- Environment and Energy
- Industry
- Services
- Information Technology

Riskitieto

- Liiketoiminta-alue
- Tavoitteet
- Tehtävät
- Liiketoiminnan seurantamittarit
- Jne.

Riskien liittäminen organisaation

- Tavoitteisiin
- Arvoihin
- Jne. asioihin

Riskien liittäminen organisaation

- Tavoitteisiin
- Arvoihin
- Jne. asioihin

01 Osa johdon raportointia
Riskitieto osana johdon raportointia, tarkasteltuna avaintunnuslukujen kautta

02 Toiminnan katselmointi
Toiminnan seurantamittarit: mitä ja miten johto haluaa seurata.

03 ISO 31000
Riskitieto liittyen toiminnan

- Tavoitteisiin
- Tehtäviin

04 Muut ISO-standardit
Riskit liittyen aihe-aluekohtaisiin standardeihin



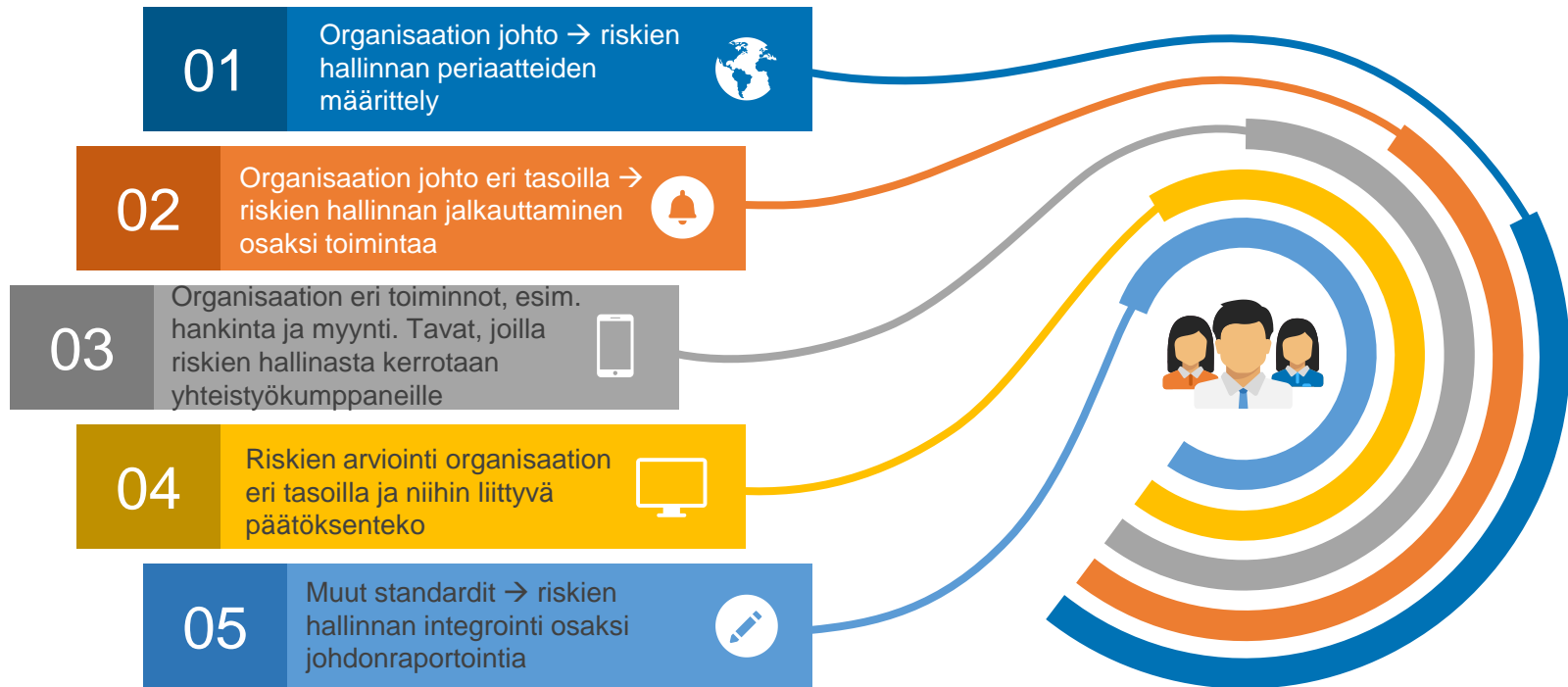
04

03

02

01

Kenelle ISO 31000 on tarkoitettu?



Riskienhallintaprosessin vaiheet

Mikä tekee jostakin asiasta riskin, uhan tai epävarmuuden. Mitä tavoitetta, arvoa tms. ilmiö tai tapahtuma vaarantaa jne.

Mitä ja mille osapuolille kerrotaan riski- ja epävarmuushavainnoista ja niitä koskevista toimenpiteistä

Millä tavoin riskienkäsittely on osa organisaation johtamis- ja päätöksenteko-järjestelmää

Miten riskejä koskeva lähde-tieto, analyysit, päätökset jne. tallennetaan ja jaetaan osana päätöksentekodokumentaatiota jne.

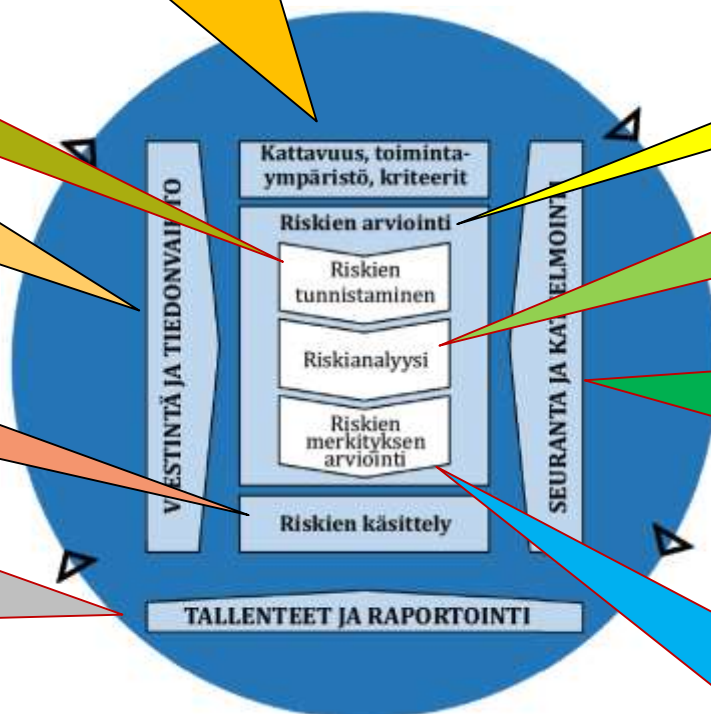
Mitä, miten ja keiden toimesta arvioidaan toimintaympäristöä?

Viitekehys, mitä vasten riskejä arvioidaan organisaation eri tasoilla; sisäiset ohjeet, tunnusluvut jne

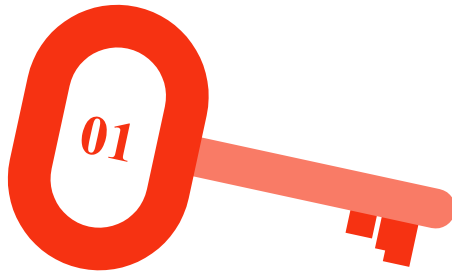
Mallit ja menetelmät miten ko. organisaatiotasolla ja osa-alueella analysoidaan riskejä

Kenen toimesta, riskejä seurataan ja katselmoidaan, missäkin yhteyksissä johtoryhmät, jne.

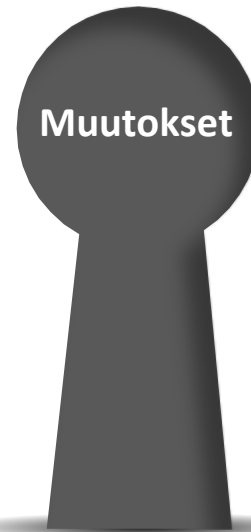
Millä tavoin ja mitä viitekehystä vasten arvioidaan riskin vaikuttavuutta – tulos ja tase, jokin standardi, asiakkaan vaatimus jne.



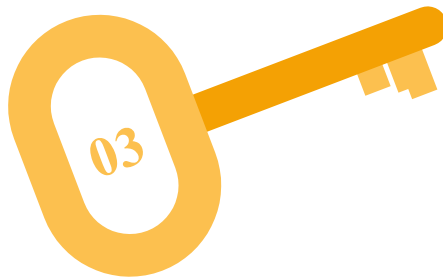
Mitä on muuttunut sitten vuoden 2010 version?



Riskien hallinnan periaatteiden arviointi ja katselmointi, joiden avulla riskien hallinta onnistuu



Korostetaan johdon roolia riskien hallinnan yhdistämisessä organisaation johtamiseen, ohjeistuksiin ja toimintatapaan



Korostetaan riskien hallinnan luonnetta asioiden säännöllistä uudelleen tarkastelua sekä huomioiden uudet kokemukset, osaamisen.
Tehtyjen analyysien pohjalta voidaan uudistaa prosessia, tai sen osia ja kontrolleja prosessin jokaisella tasolla



Sisällön virtaviivaistamisen tarkoituksena on avata mallia vastaamaan toiminnan moninaisiin tarpeisiin ja sisältöihin

Mitä hyötyä standardista on?

- **Standardissa esitetään riskienhallinnan periaatteet ja yleiset ohjeet**
- **Standardi**
 - Soveltuu kaiken tyyppisille organisaatioille
 - On toimiala- ja sektoririippumaton
- **Standardia voidaan soveltaa**
 - Organisaation elinkaaren kaikissa vaiheissa monilla eri osa-alueilla
 - Kaikentyyppisiin riskeihin riippumatta siitä, onko niillä myönteisiä vai haitallisia seurauksia.
- **Tavoitteena on**
 - Tämänhetkisten ja tulevien standardien esittämien riskienhallintaprosessien yhdenmukaistaminen
 - Tarjota yleinen toimintamalli, joka täydentää muita standardeja näiltä osin, eikä sitä ole tarkoitettu korvaamaan kyseisiä standardeja
- **Tätä kansainvälistä standardia ei ole tarkoitettu käytettäväksi sertifiointin perustana eikä riskianalyysien tekemiseen, vaan periaatteiden ja prosessin toteuttamiseen**

Tarjoaa laajan viitekehyksen



- Riskienhallintaprosessin kehittäminen perustuu ISO 31000 viitekehykseen pitäen sisällään riskien johtamiseen, raportointiin liittyvät toimet.
- Tarjoaa yleisen toimintamallin, joka tukee erityisriskejä tai -sektoreita käsitteleviä standardeja, eikä sitä ole tarkoitettu korvaamaan kyseisiä standardeja
- ISO 31000 on vapaaehtoinen ohjeisto riskienhallinnalle – ei sertifioitava tuote
- Erityisosa-alueilla käytetään tarvittavia menetelmiä riskianalyysien tekoon

Tarjoaa yhteiset termit

- **Määrittelee 29 erilaista termiä, joita käytetään riskienhallinnan yhteydessä**
- **Esimerkkejä termeistä:**
 - Riski - epävarmuuden vaikutus tavoitteisiin
 - Riskienhallinta - koordinoitu toiminta, jolla organisaatiota johdetaan ja ohjataan riskien
 - Riskiin suhtautuminen - organisaation lähestymistapa riskin arvioimiseen ja sen tavoittelemiseen, säilyttämiseen, ottamiseen tai välttämiseen
- **Yhteinen kieli lisää yhteistä ymmärtämistä ja ennen kaikkea auttaa organisaatiota viestimään riskienhallintaan liittyvistä asioista muille osapuolille**