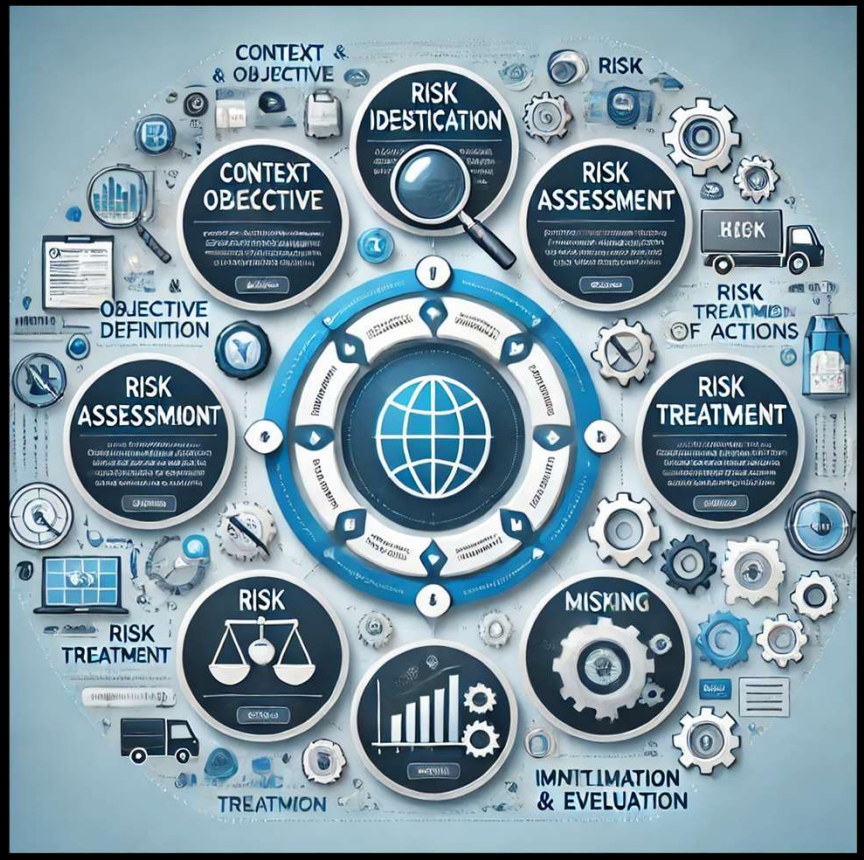

Tunne huominen.
XAMK
Kaakkois-Suomen
ammattikorkeakoulu

Riskienhallinta IT-ympäristössä



Kaakkois-Suomen ammattikorkeakoulu
South-Eastern Finland University of Applied Sciences

www.xamk.fi

Kaakkois-Suomen
ammattikorkeakoulu

Riskienhallinta IT-ympäristöissä

Riskienhallinta IT-ympäristössä on järjestelmällinen prosessi, jonka tavoitteena on tunnistaa, arvioida ja hallita tietotekniseen ympäristöön kohdistuvia riskejä. Riskienhallinta keskittyy erityisesti tietojen luottamuksellisuuden, eheyden ja saatavuuden varmistamiseen.

Riskienhallinnan prosessi IT-ympäristössä

Riskienhallinnan kokonaisuuden vastuu kuuluu organisaation ylimmälle johdolle. Käytännössä tämä tarkoittaa vastuuta riskienhallinnan strategian määrittämisestä, riskinsietokyvyn määrittämistä ja jäännösriskien hyväksymistä. Lisäksi organisaation johdon kuuluu osallistua riskienhallintaan strategisella tasolla.

Riskienhallinnan prosessi voidaan jakaa seuraaviin osa-alueisiin:

1. Tavoitteiden ja kontekstin määrittäminen
2. Riskien tunnistaminen
3. Riskiarviointi
4. Riskienkäsittely
5. Toimenpiteiden toteutus
6. Seuranta ja arviointi

Tavoitteiden ja kontekstin määrittäminen

- Ensimmäisessä vaiheessa määritellään organisaation tavoitteet ja IT-ympäristöön liittyvä toimintaympäristö.

- Tämä sisältää:
  - ✓ IT-omaisuuden kartoituksen (esim. palvelimet, työasemat, tietokannat, verkot, sovellukset).
  - ✓ Organisaation arvokkaiden tietojen ja prosessien tunnistamisen.
  - ✓ Lainsäädännön ja standardien, kuten GDPR:n tai ISO 27001:n, vaatimusten huomioimisen.

Riskien tunnistaminen

- Riskit tunnistetaan analysoimalla:
  - ✓ Haavoittuvuudet: Esimerkiksi vanhentuneet ohjelmistot, heikot salasanat, puutteellinen pääsynhallinta.
  - ✓ Uhat: Haittaohjelmat, palvelunestohyökkäykset, tietojen kalastelu, sisäiset uhkatekijät.
  - ✓ Altistukset: Tiedot, jotka voivat joutua vaaralle alttiiksi uhkien hyödyntäessä haavoittuvuuksia.

- Käytetään työkaluja, kuten uhkamalleja, penetraatiotestauksia ja lokianalytiikkaa.

Riskiarviointi

- Riskit arvioidaan niiden **todennäköisyyden** ja **vaikutusten** perusteella. Käytetään esimerkiksi riskimatriisia, jossa riskeille annetaan:
  - ✓ Todennäköisyysasteikko (esim. pieni, keskisuuri, suuri).
  - ✓ Vaikutusasteikko (esim. vähäinen, kohtalainen, kriittinen).

- Tämän avulla riskit luokitellaan esimerkiksi:
  - ✓ Korkean prioriteetin riskeihin, jotka vaativat välitöntä käsittelyä.
  - ✓ Matalan prioriteetin riskeihin, jotka voivat odottaa.

Riskien käsittely

- Kun riskit on arvioitu, niihin sovelletaan sopivaa käsittelystrategiaa:

1) **Välttäminen:** Riskin aiheuttavan toiminnon tai prosessin välttäminen, esim. luopumalla vaarallisesta teknologiasta.
2) **Vähentäminen:** Toimenpiteet riskin todennäköisyyden tai vaikutusten pienentämiseksi, esim. tietoturvapäivitykset, monivaiheinen tunnistautuminen.
3) **Siirtäminen:** Riskin siirtäminen kolmannelle osapuolelle, kuten vakuutusyhtiölle tai palveluntarjoajalle.
4) **Hyväksyminen:** Jos riskin käsittely ei ole kustannustehokasta tai se on vähäinen, organisaatio voi hyväksyä riskin.

Toimenpiteiden toteutus

- Riskien käsittelyn vaatimat toimenpiteet implementoidaan. Tämä voi sisältää:
  - ✓ Teknisiä toimenpiteitä (esim. palomuurit, tietoturvaohjelmistot, varmuuskopiointi).
  - ✓ Hallinnollisia toimenpiteitä (esim. turvallisuuspolitiikat, koulutusohjelmat, käyttöoikeuksien hallinta).
  - ✓ Operatiivisia toimenpiteitä (esim. lokien tarkistus, häiriötilanteiden harjoitukset).

Seuranta ja arviointi

- Riskienhallintaa on seurattava jatkuvasti, koska uhkat, haavoittuvuudet ja liiketoimintaympäristö muuttuvat.
- Seuranta sisältää:
  - ✓ Säännölliset auditoinnit ja riskien uudelleenarvioinnit.
  - ✓ Incident response -prosessien arvioinnin.
  - ✓ Raportoinnin organisaation johdolle ja sidosryhmille.

Riskiarviointiin perustuva riskienkäsittely

Riskiarviointi luo perustan riskien käsittelystrategioille.

1) **Korkean riskin käsittely:**
   - **Esimerkki:** Käyttäjätilien epäilyttävät sisäänkirjautumisyritykset havaitaan usein.
   - **Toimenpide:** Ota käyttöön monivaiheinen tunnistautuminen ja epäonnistuneiden kirjautumisten estomekanismit.

2) **Keskisuuren riskin käsittely:**
   - **Esimerkki:** Järjestelmässä on vanhentunut ohjelmisto, mutta se ei ole suoraan alttiina internetille.
   - **Toimenpide:** Aikatauluta ohjelmiston päivitys ja segmentoi verkko, jotta uhkat eivät leviä.

3) **Matala riskin hyväksyminen:**
   - **Esimerkki:** Palvelimen fyysinen sijainti voi altistua pienelle vesivahingolle.
   - **Toimenpide:** Hyväksy riski, mutta seuraa tilannetta ja varmista, että varmuuskopiot ovat kunnossa.

Tunne huominen.