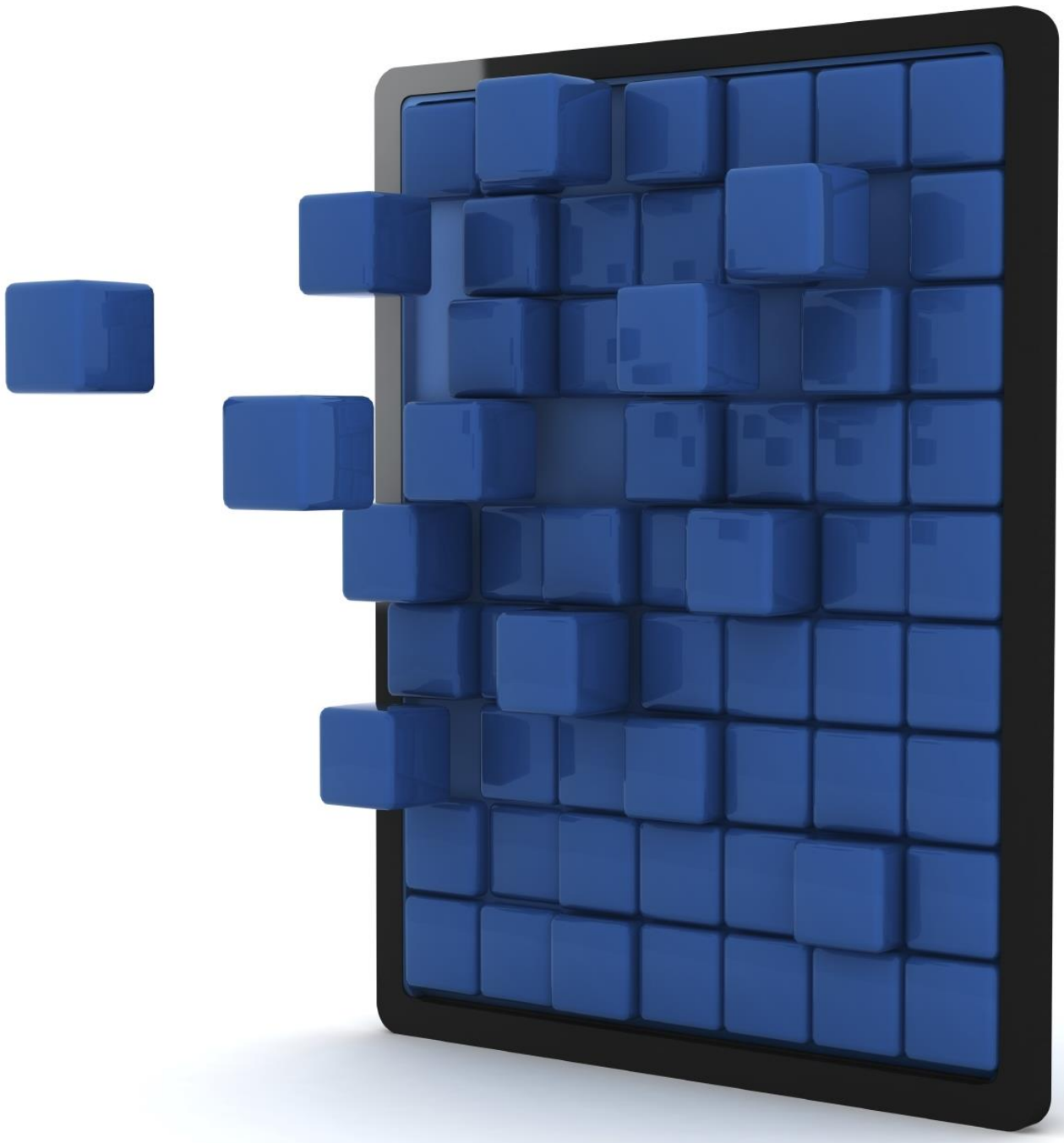
ITSEARVIOINNIN TARKASTUSLISTA



ITSEARVIOINNIN TARKASTUSLISTA

Tämä kysymyslista on tarkoitettu energiayritysten käyttöön niiden suunnitellessa kyberturvallisuuden itsearviointia.

Oletteko muodostaneet organisaatiossanne kyberturvallisuuden, tietoturvallisuuden, tai kokonaisturvallisuuden tiimin, jonka vastuulle kuuluu tietoturvan kehittäminen ja valvonta?

- Onko tiimillä organisaation johdon tuki? Miten tuki käytännössä ilmenee?
- Onko kehitystiimissä mukana henkilöitä kaikilta automaation kannalta kriittisiltä osa-alueilta, kuten esimerkiksi
  - tuotannon (automaation) kunnossapidosta ja kehittämisestä,
  - yritys-, laitos- ja sähköverkkojen ICT-järjestelmien ylläpidosta ja kehittämisestä,
  - automaation hankinnoista,
  - tuotannon järjestelmien pääkäyttäjistä,
  - kokonaisturvallisuudesta ja sen kehittämisestä, ja
  - henkilö- ja ympäristöturvallisuuden kehittämisestä?

Tunteeko auditointitiiminne kyberturvallisuuden merkityksen toimialanne kokonaisturvallisuudelle ja tuotannon luotettavuudelle?

Turvalliseen toimintaan kuuluvat esimerkiksi

- koko henkilöstön kyberturvallisuustietoisuuden kehittäminen,
- jatkuvuutta ja turvallisuutta tukevien toimintaohjeiden ja lupamenettelyjen käyttöönottaminen,
- tuotannon suojauskonseptien jatkuva kehittäminen ja käyttäminen,
- kyky tunnistaa teihin kohdistuvaa vakoilua ja tietomurtoja,
- jatkuva toteutuneiden häiriöiden, tehtyjen virheiden ja epäiltyjen hyökkäysten raportointi ja seuranta,
- häiriöistä palautumisen suunnittelu ja toistuva harjoitteleminen, sekä
- uusien varautumistapojen etsiminen ja käyttöönottaminen kyberuhkien muuttuessa yhä vaikeammin havaittaviksi.

Tunteeko organisaationne auditointitiimi teidän toimialanne kyberuhat?

- Oletteko arvioineet liiketoiminnan riskit ja uhat?
- Tiedättekö millaisia uhkia ja tietoturvaloukkauksia on esiintynyt teidän toimialallanne ja käyttämänne kaltaisissa järjestelmissä?

ITSERVIOINTI

Tarkastuslista

Tunnetteko kaikkien automaatiojärjestelmiinne kuuluvien ohjausten ja laitteiden sijainnit sekä niiden ominaisuudet?

- Miten tiedot on dokumentoitu ja miten ne pidetään ajan tasalla?
  - Miten tietoja päivitetään? Mitä työkaluja käytetään?
  - Ovatko tiedot käytettävissä tietoteknisen tai tietoliikennehäiriön sattuessa?
- Mitkä laitteet käyttävät analogia- ja mitkä digitaalitekniikkaa?
- Mitkä laitteet ovat kytkettävissä tai kytketty IP (*Internet Protocol*) -verkkoon?
  - Mitkä laitteet ovat saavutettavissa IP-yhdyskäytävien kautta?
- Miten ja mitä verkkoja käyttäen laitteet on kytketty toisiinsa?
  - Onko järjestelmästä piirretty ajantasainen verkkokaavio?
    - Miten verkkokaaviota pidetään yllä ja kenen vastuulla ylläpito on?
- Mitkä laitteista sijaitsevat suojatuissa ja/tai valvotuissa tiloissa? Ja mitkä eivät?
- Mitkä ohjauslaitteet ovat viranomaismääräysten alaisia?

Mitkä ovat toimintanne tärkeimmät ja kriittisimmät osat?

- Onko automaatiojärjestelmällenne tehty kyberturvallisuusnäkökulman sisältävä riskiarviointi?
- Minkä järjestelmän osien tai laitteiden häiriö tai menettäminen voi aiheuttaa merkittäviä vaaroja ihmisille, ympäristölle tai organisaation taloudelliselle jatkuvuudelle?

Oletteko määritelleet yhdessä omistajien kanssa auditointien tavoitteet ja rajaukset?

- Mitkä järjestelmät auditoidaan ja milloin?
- Miten ja mihin tavoitteet ja rajaukset ovat dokumentoituna?
- Mitä kriteerejä kohteiden valinnassa käytetään?

Oletteko arvioineet käyttämänne tietoturvapolitiikat, toimintaohjeet sekä tehtävien jaon?

- Onko edellä mainituissa puutteita?
  - Miten puutteet on dokumentoitu ja onko korjaavat toimenpiteet resursoitu?
  - Miten kehittämistä seurataan?

Oletteko arvioineet organisaation nykyiset riskit, uhat ja haavoittuvuudet?

- Milloin kyberuhat sisältävä riskiarvio on päivitetty?
- Miten arvioitte omaan organisaatioonne kohdistuvat tietoturvauhat?
- Etsittekö tietoturvahaavoittuvuuksia omista järjestelmistänne?
  - Mitä menetelmiä käytätte tietoturvahaavoittuvuuksien etsimiseen?

Oletteko dokumentoineet auditointien tulokset?

- Miten seuraatte auditoinneissa havaittujen puutteiden korjaamista?

Kenelle jaatte tietoa auditoinnin tuloksista?

- Onko teillä prosessi, miten organisaationne toimintaa kehitetään auditoinnin tulosten pohjalta?
- Onko teillä prosessi, miten auditointia kehitetään saatujen kokemisten perusteella?

Auditoinnin tulokset ovat luottamuksellisia.
Yksityiskohtaiset tiedot paljastaisivat miten juuri teitä vastaan hyökättäisiin tehokkaasti