HENKILÖSTÖTURVALLISUUS

Auditoinnin tavoite

Selvittää, hallitaanko henkilöstöön liittyvät turvallisuusriskit koko työsuhteen elinkaaren ajan rekrytoinnista työsuhteen päättymiseen.

1. Onko yrityksellä hyväksytty ja ajantasainen henkilöstöturvallisuuden toimintamalli?

Hyväksymiskriteeri: Toimintamalli on kirjallinen, johdon hyväksymä, yrityksen toimintaan soveltuva ja henkilöstön saatavilla.

Todentava näyttö: henkilöstöturvallisuusohje, hyväksymispäätös, julkaisukanava, versionhallintatiedot.

2. Onko turvallisuuteen liittyvät vastuut määritelty rekrytoinnin, työsuhteen ja päättämisen eri vaiheissa?

Hyväksymiskriteeri: Henkilöstöhallinnon, esihenkilöiden, tietohallinnon ja turvallisuudesta vastaavien tehtävät sekä määräajat on kuvattu.

Todentava näyttö: vastuumatriisi, prosessikuvaus, tehtävänkuvat, palvelutasot.

3. Arvioidaanko tehtävän turvallisuusvaatimukset ennen rekrytointia?

Hyväksymiskriteeri: Tehtävän luottamuksellisuus, käyttöoikeudet, pätevyysvaatimukset ja mahdolliset taustaselvitystarpeet määritellään ennen valintaa.

Todentava näyttö: tehtävänkuvat, rekrytointipyynnöt, riskiluokitus, hyväksynnät.

4. [KRIITTINEN] Tehdäänkö taustojen ja pätevyyksien tarkistukset lain ja tehtävän riskitason mukaisesti?

Hyväksymiskriteeri: Tarkistukset perustuvat kirjalliseen menettelyyn, suostumuksiin ja tehtäväkohtaiseen tarpeeseen, ja tulokset käsitellään luottamuksellisesti.

Todentava näyttö: tarkistusohje, suostumukset, tarkistusmerkinnät, poikkeuspäätökset.

5. Allekirjoittavatko työntekijät tarvittavat salassapito- ja turvallisuussitoumukset ennen pääsyn saamista?

Hyväksymiskriteeri: Sitoumukset vastaavat tehtävää ja ovat voimassa ennen luottamuksellisten tietojen, järjestelmien tai tilojen käyttöä.

Todentava näyttö: työsopimukset, salassapitositoumukset, perehdytyslista, allekirjoitusmerkinnät.

6. Saavatko uudet työntekijät turvallisuusperehdytyksen ennen itsenäistä työskentelyä?

Hyväksymiskriteeri: Perehdytys kattaa yrityksen keskeiset turvallisuusohjeet, poikkeamien ilmoittamisen ja työntekijän vastuut.

Todentava näyttö: perehdytysohjelma, koulutusmateriaali, osallistumismerkinnät, osaamisen varmistus.

7. Tarkistetaanko käyttö- ja kulkuoikeudet tehtävän muuttuessa tai pitkän poissaolon alkaessa?

Hyväksymiskriteeri: Oikeudet arvioidaan viipymättä uuden tehtävän ja vähimmän oikeuden periaatteen mukaisesti.

Todentava näyttö: HR-ilmoitukset, käyttöoikeuspyynnöt, kulkuoikeusraportit, muutoslokit.

8. [KRIITTINEN] Poistetaanko työsuhteen päättyessä käyttö- ja kulkuoikeudet sekä palautetaanko yrityksen omaisuus ajoissa?

Hyväksymiskriteeri: Päättämistoimet toteutetaan ennalta määritellyssä ajassa ja niiden valmistuminen varmennetaan ennen tai viimeistään työsuhteen päättyessä.

Todentava näyttö: päättämislista, tunnusten sulkemislokit, avain- ja laitepalautukset, hyväksyntä.

9. Hallitaanko avainhenkilöihin ja kriittiseen osaamiseen liittyvät riippuvuudet?

Hyväksymiskriteeri: Kriittiset tehtävät, varahenkilöt, osaamisen siirto ja poissaolojen varajärjestelyt on määritelty.

Todentava näyttö: osaamismatriisi, varahenkilöluettelo, jatkuvuussuunnitelma, koulutussuunnitelmat.

10. Seurataanko henkilöstöturvallisuuden toteutumista ja käsitelläänkö poikkeamat?

Hyväksymiskriteeri: Yritys seuraa sovittuja mittareita, tutkii poikkeamat ja toteuttaa korjaavat toimenpiteet määräajassa.

Todentava näyttö: mittariraportit, poikkeamarekisteri, juurisyyanalyysit, toimenpideseuranta.

TIETOSUOJAN HALLINTA

Auditoinnin tavoite

Selvittää, käsitteleekö yritys henkilötietoja lainmukaisesti, läpinäkyvästi, turvallisesti ja vain määriteltyihin tarkoituksiin.

1. Onko yrityksellä hyväksytty ja ajantasainen tietosuojapolitiikka?

Hyväksymiskriteeri: Tietosuojapolitiikka on kirjallinen, johdon hyväksymä, voimassa oleva, yrityksen toimintaan soveltuva ja henkilöstön saatavilla.

Todentava näyttö: tietosuojapolitiikka, hyväksymispäätös, julkaisukanava, versionhallintatiedot.

2. Onko henkilötietojen käsittelyn vastuut ja omistajuudet määritelty?

Hyväksymiskriteeri: Rekisterinpitäjän, prosessinomistajien, tietosuojavastaavan ja käsittelijöiden tehtävät sekä päätösvaltuudet on kuvattu.

Todentava näyttö: vastuumatriisi, tehtävänkuvat, nimityspäätökset, prosessikuvaukset.

3. Ylläpitääkö yritys ajantasaista luetteloa henkilötietojen käsittelytoimista?

Hyväksymiskriteeri: Luettelosta ilmenevät käsittelyn tarkoitus, tietoryhmät, rekisteröidyt, vastaanottajat, säilytysajat ja suojaustoimet.

Todentava näyttö: käsittelytoimien seloste, tietovirtakuvaukset, järjestelmäluettelo, päivityslokit.

4. Varmistetaanko jokaiselle henkilötietojen käsittelylle lainmukainen peruste ja käyttötarkoitus?

Hyväksymiskriteeri: Käsittelyperuste on dokumentoitu ennen käsittelyn aloittamista eikä tietoja käytetä yhteensopimattomiin tarkoituksiin.

Todentava näyttö: käsittelyperustearviot, suostumusmallit, sopimukset, tietosuojaselosteet.

5. [KRIITTINEN] Arvioidaanko korkean riskin henkilötietojen käsittelyn vaikutukset ennen käyttöönottoa?

Hyväksymiskriteeri: Tietosuojavaikutusten arviointi tehdään ennakolta, riskit käsitellään ja hyväksyntä dokumentoidaan.

Todentava näyttö: DPIA-arviot, riskirekisteri, hyväksymispäätökset, toimenpidesuunnitelmat.

6. Käsitelläänkö rekisteröityjen pyynnöt yhdenmukaisesti ja määräajassa?

Hyväksymiskriteeri: Pyynnöt tunnistetaan, kirjataan, henkilöllisyys varmistetaan ja vastaus annetaan sovellettavassa määräajassa.

Todentava näyttö: pyyntörekisteri, tunnistamisohje, vastausmallit, käsittelyajat.

7. Onko henkilötietojen säilytysajat ja turvallinen poistaminen määritelty?

Hyväksymiskriteeri: Säilytysajat perustuvat lakiin tai tarpeeseen, poistaminen on automatisoitu tai valvottu ja poikkeukset hyväksytään.

Todentava näyttö: säilytysaikataulu, poistopolitiikka, järjestelmäasetukset, poistoraportit.

8. Hallitaanko henkilötietojen luovutukset ja siirrot kolmansille osapuolille?

Hyväksymiskriteeri: Luovutuksille on peruste, vastaanottaja on arvioitu, sopimukset ovat voimassa ja kansainväliset siirrot suojataan.

Todentava näyttö: käsittelysopimukset, siirtoperustearviot, vastaanottajaluettelo, hyväksynnät.

9. [KRIITTINEN] Tunnistetaanko ja ilmoitetaanko henkilötietojen tietoturvaloukkaukset asianmukaisesti?

Hyväksymiskriteeri: Loukkaukset arvioidaan viipymättä, ilmoitusvelvollisuus ratkaistaan dokumentoidusti ja määräaikoja noudatetaan.

Todentava näyttö: poikkeamarekisteri, riskiarviot, viranomaisilmoitukset, rekisteröityjen ilmoitukset.

10. Seurataanko tietosuojan toteutumista ja koulutetaanko henkilöstöä säännöllisesti?

Hyväksymiskriteeri: Koulutus kattaa tehtäväkohtaiset velvoitteet, osaaminen varmistetaan ja tietosuojan tilasta raportoidaan johdolle.

Todentava näyttö: koulutusrekisteri, osaamistestit, auditointiraportit, johdon raportit.

OMAISUUDEN JA TIETOVARANTOJEN HALLINTA

Auditoinnin tavoite

Selvittää, tunnistaako, omistaako, luokitteleeko ja suojaako yritys laitteet, järjestelmät, ohjelmistot, tiedot ja muut kriittiset voimavarat koko elinkaaren ajan.

1. Onko yrityksellä hyväksytty omaisuuden ja tietovarantojen hallintaprosessi?

Hyväksymiskriteeri: Prosessin laajuus, vastuut, ylläpitotavat ja elinkaaren vaiheet on kirjattu ja hyväksytty.

Todentava näyttö: prosessikuvaus, omaisuudenhallintaohje, hyväksymispäätös, vastuumatriisi.

2. Ylläpidetäänkö yrityksen laitteista, järjestelmistä, ohjelmistoista ja tietovarannoista ajantasaista rekisteriä?

Hyväksymiskriteeri: Rekisteri kattaa kaikki olennaiset kohteet ja sisältää yksilöivän tunnisteen, omistajan, sijainnin, kriittisyyden ja tilan.

Todentava näyttö: omaisuusrekisteri, järjestelmäluettelo, ohjelmistoluettelo, tietovarantorekisteri.

3. Onko jokaiselle kriittiselle omaisuuserälle ja tietovarannolle nimetty omistaja?

Hyväksymiskriteeri: Omistaja vastaa luokituksesta, käyttöehdoista, suojaamisesta, katselmoinnista ja elinkaaripäätöksistä.

Todentava näyttö: omistajaluettelo, tehtävänkuvat, hyväksynnät, katselmuspöytäkirjat.

4. Luokitellaanko tiedot ja omaisuus niiden luottamuksellisuuden, eheyden, saatavuuden ja kriittisyyden perusteella?

Hyväksymiskriteeri: Luokitteluperusteet ovat kirjalliset ja luokitus ohjaa käsittelyä, suojausta, säilytystä ja hävittämistä.

Todentava näyttö: luokitteluohje, luokitusmerkinnät, tietomallit, käsittelyohjeet.

5. [KRIITTINEN] Varmistetaanko, että vain hyväksytyt laitteet, ohjelmistot ja palvelut ovat käytössä?

Hyväksymiskriteeri: Käyttöönotto edellyttää hyväksyntää, vaatimusten tarkistusta ja rekisteröintiä; luvattomat kohteet havaitaan ja poistetaan.

Todentava näyttö: hyväksymispyynnöt, laitehallintaraportit, ohjelmistoinventaario, poikkeamarekisteri.

6. Hallitaanko yrityksen omaisuuden luovutus työntekijöille ja ulkopuolisille jäljitettävästi?

Hyväksymiskriteeri: Luovutus, haltija, käyttötarkoitus, ehdot ja palautusvelvollisuus dokumentoidaan.

Todentava näyttö: luovutuslomakkeet, laiterekisteri, kuittaukset, sopimusehdot.

7. Tarkastetaanko omaisuusrekisterien oikeellisuus säännöllisesti?

Hyväksymiskriteeri: Fyysisiä ja teknisiä inventointeja verrataan rekistereihin ja erot selvitetään määräajassa.

Todentava näyttö: inventointiraportit, poikkeamalistat, täsmäytykset, korjausmerkinnät.

8. Hallitaanko ohjelmistolisenssit ja käyttöehdot?

Hyväksymiskriteeri: Lisenssien määrä, voimassaolo, käyttörajoitukset ja vastuut tunnetaan, ja alikäyttö tai luvaton käyttö käsitellään.

Todentava näyttö: lisenssirekisteri, ostotositteet, käyttöraportit, sopimukset.

9. [KRIITTINEN] Poistetaanko käytöstä poistettavista laitteista ja tietovälineistä tiedot turvallisesti?

Hyväksymiskriteeri: Poistomenetelmä vastaa tietojen luokitusta, toteutus voidaan todentaa ja hävitysketju on hallittu.

Todentava näyttö: poistotodistukset, ylikirjoitusraportit, hävityssopimukset, luovutusketju.

10. Seurataanko omaisuuden elinkaarta, kuntoa ja vanhentumisriskejä?

Hyväksymiskriteeri: Takuu-, tuki-, päivitys- ja elinkaaritiedot tunnetaan ja korvaamiselle on suunnitelma ennen tuen päättymistä.

Todentava näyttö: elinkaariraportit, uusimissuunnitelmat, budjetit, riskirekisteri.

KÄYTTÖVALTUUS- JA IDENTITEETINHALLINTA

Auditoinnin tavoite

Selvittää, myönnetäänkö, muutetaanko, katselmoidaanko ja poistetaanko käyttäjien sekä teknisten tunnusten oikeudet hallitusti ja tehtävien mukaisesti.

1. Onko yrityksellä hyväksytty käyttövaltuus- ja identiteetinhallinnan prosessi?

Hyväksymiskriteeri: Prosessi kattaa tunnusten elinkaaren, hyväksynnät, roolit, katselmoinnit, poikkeukset ja poistamisen.

Todentava näyttö: prosessikuvaus, käyttövaltuusohje, hyväksymispäätös, vastuumatriisi.

2. Perustetaanko käyttäjätunnukset vain yksilöidyn ja hyväksytyn pyynnön perusteella?

Hyväksymiskriteeri: Pyynnöstä ilmenevät käyttäjä, tehtävä, tarvittavat oikeudet, omistajan hyväksyntä ja voimassaoloaika.

Todentava näyttö: käyttöoikeuspyynnöt, hyväksymismerkinnät, tiketit, tunnusrekisteri.

3. Myönnetäänkö käyttöoikeudet vähimmän oikeuden ja tehtäväperusteisuuden mukaisesti?

Hyväksymiskriteeri: Käyttäjä saa vain työn edellyttämät oikeudet ennalta määriteltyjen roolien perusteella.

Todentava näyttö: roolikuvaus, käyttöoikeusmatriisi, käyttäjäotos, hyväksynnät.

4. [KRIITTINEN] Suojataanko pääkäyttäjä- ja muut korotetut oikeudet erityismenettelyillä?

Hyväksymiskriteeri: Korotetut oikeudet ovat henkilökohtaisia, määräaikaisia tarvittaessa, vahvasti tunnistettuja, valvottuja ja hyväksyttyjä.

Todentava näyttö: pääkäyttäjäluettelo, PAM-raportit, MFA-asetukset, istuntolokit.

5. Eriytetäänkö vaaralliset tehtävä- ja oikeusyhdistelmät?

Hyväksymiskriteeri: Ristiriitaiset roolit on määritelty SoD-matriisissa, poikkeukset hyväksytään ja korvaavat kontrollit toteutetaan.

Todentava näyttö: SoD-matriisi, ristiriitaraportit, poikkeuspäätökset, valvontaraportit.

6. Katselmoidaanko käyttäjien käyttöoikeudet säännöllisesti?

Hyväksymiskriteeri: Omistajat tarkistavat oikeuksien tarpeellisuuden riskiperusteisesti ja tarpeettomat oikeudet poistetaan määräajassa.

Todentava näyttö: katselmointiraportit, hyväksyntämerkinnät, poistotiketit, seurantamittarit.

7. Hallitaanko palvelu-, integraatio- ja yhteiskäyttötunnukset erikseen?

Hyväksymiskriteeri: Tunnuksilla on omistaja, rajattu käyttötarkoitus, suojatut salaisuudet, säännöllinen tarkastus ja tarvittaessa määräaika.

Todentava näyttö: teknisten tunnusten rekisteri, avainholvin tiedot, salasanakierto, käyttölogit.

8. [KRIITTINEN] Poistetaanko tai muutetaanko oikeudet viipymättä tehtävämuutoksissa ja työsuhteen päättyessä?

Hyväksymiskriteeri: HR-ilmoitus käynnistää hallitun työnkulun ja oikeuksien sulkeminen varmennetaan sovitussa määräajassa.

Todentava näyttö: HR-ilmoitukset, päättämistiketit, sulkemislokit, poikkeamaraportit.

9. Valvotaanko epäonnistuneita kirjautumisia ja poikkeavaa tunnusten käyttöä?

Hyväksymiskriteeri: Hälytysrajat on määritelty, tapahtumat yhdistetään lokivalvontaan ja poikkeamat tutkitaan.

Todentava näyttö: kirjautumislokit, SIEM-hälytykset, tutkintaraportit, estolistat.

10. Seurataanko käyttövaltuushallinnan laatua ja tehokkuutta?

Hyväksymiskriteeri: Yritys mittaa esimerkiksi käsittelyaikoja, vanhentuneita oikeuksia, ristiriitoja ja katselmointien kattavuutta.

Todentava näyttö: mittariraportit, poikkeamalistat, johdon raportit, kehitystoimenpiteet.

TOIMITTAJA- JA ULKOISTUSPALVELUJEN TURVALLISUUDENHALLINTA

Auditoinnin tavoite

Selvittää, hallitseeko yritys toimittajiin, alihankkijoihin ja ulkoistettuihin palveluihin liittyvät turvallisuus-, jatkuvuus- ja vaatimustenmukaisuusriskit.

1. Onko yrityksellä hyväksytty toimittaja- ja ulkoistuspalvelujen turvallisuudenhallintaprosessi?

Hyväksymiskriteeri: Prosessi kattaa valinnan, riskinarvioinnin, sopimukset, valvonnan, poikkeamat ja yhteistyön päättämisen.

Todentava näyttö: prosessikuvaus, hankintaohje, turvallisuusvaatimukset, hyväksymispäätös.

2. Luokitellaanko toimittajat palvelun kriittisyyden ja käsiteltävien tietojen perusteella?

Hyväksymiskriteeri: Luokitus ohjaa ennakkoarvioinnin laajuutta, sopimusehtoja, valvontaa ja jatkuvuusvaatimuksia.

Todentava näyttö: toimittajaluettelo, kriittisyysluokitus, riskikriteerit, hyväksynnät.

3. Arvioidaanko toimittajan turvallisuus ja jatkuvuus ennen sopimuksen tekemistä?

Hyväksymiskriteeri: Arviointi kattaa kyvykkyyden, referenssit, tekniset kontrollit, taloudellisen tilanteen, alihankinnat ja palautumisen.

Todentava näyttö: ennakkoarvioinnit, auditointiraportit, sertifikaatit, riskipäätökset.

4. [KRIITTINEN] Sisältyvätkö sopimuksiin riittävät turvallisuus-, tietosuoja- ja jatkuvuusehdot?

Hyväksymiskriteeri: Sopimuksessa määritellään vaatimukset, ilmoitusvelvollisuudet, auditointioikeus, alihankinta, tietojen palautus ja vastuut.

Todentava näyttö: sopimusmallit, allekirjoitetut sopimukset, tietojenkäsittelyehdot, palvelutasot.

5. Hallitaanko toimittajien käyttö- ja etäyhteysoikeudet?

Hyväksymiskriteeri: Oikeudet ovat hyväksyttyjä, yksilöllisiä, rajattuja, määräaikaisia ja valvottuja, ja ne poistetaan tarpeen päättyessä.

Todentava näyttö: käyttöoikeuspyynnöt, etäyhteysraportit, lokit, päättämistiketit.

6. Tunnetaanko kriittisten toimittajien alihankintaketjut ja tietojen käsittelypaikat?

Hyväksymiskriteeri: Alihankkijat ja käsittelypaikat on ilmoitettu, muutokset hyväksytään ja samat vaatimukset ulotetaan ketjuun.

Todentava näyttö: alihankkijaluettelot, sijaintitiedot, sopimusehdot, muutosilmoitukset.

7. Seurataanko toimittajien palvelutasoa, turvallisuutta ja korjaavia toimenpiteitä?

Hyväksymiskriteeri: Sovittuja mittareita ja poikkeamia seurataan säännöllisesti, ja puutteille asetetaan omistaja sekä määräaika.

Todentava näyttö: palveluraportit, katselmuspöytäkirjat, poikkeamarekisteri, toimenpideseuranta.

8. [KRIITTINEN] Ilmoittavatko toimittajat turvallisuuspoikkeamista ja merkittävistä häiriöistä viipymättä?

Hyväksymiskriteeri: Ilmoitusajat, sisältö, yhteyshenkilöt ja yhteistyö tutkinnassa on määritelty ja testattu.

Todentava näyttö: sopimusehdot, poikkeamailmoitukset, yhteystietolistat, harjoitusraportit.

9. Onko kriittisille ulkoistuspalveluille määritelty jatkuvuus- ja irtautumissuunnitelmat?

Hyväksymiskriteeri: Yritys pystyy siirtämään palvelun, palauttamaan tiedot ja jatkamaan kriittistä toimintaa toimittajan häiriössä tai vaihdossa.

Todentava näyttö: irtautumissuunnitelma, varajärjestelyt, tietojen palautusmenettely, testitulokset.

10. Päätetäänkö toimittajayhteistyö hallitusti?

Hyväksymiskriteeri: Oikeudet poistetaan, omaisuus ja tiedot palautetaan tai hävitetään, salassapito jatkuu ja avoimet velvoitteet suljetaan.

Todentava näyttö: päättämislista, poistotodistukset, käyttöoikeuslokit, loppukatselmus.

JATKUVUUDEN- JA VALMIUDENHALLINTA

Auditoinnin tavoite

Selvittää, pystyykö yritys jatkamaan kriittistä toimintaa häiriöissä sekä palautumaan hyväksyttävässä ajassa ja hyväksyttävälle tasolle.

1. Onko yrityksellä hyväksytty jatkuvuuden- ja valmiudenhallinnan toimintamalli?

Hyväksymiskriteeri: Toimintamalli määrittelee tavoitteet, vastuut, suunnittelun, harjoittelun, ylläpidon ja raportoinnin.

Todentava näyttö: jatkuvuuspolitiikka, prosessikuvaus, hyväksymispäätös, vastuumatriisi.

2. Onko yrityksen kriittiset prosessit, palvelut, resurssit ja riippuvuudet tunnistettu?

Hyväksymiskriteeri: Tunnistaminen perustuu liiketoimintavaikutusten arviointiin ja kattaa henkilöt, tilat, tiedot, järjestelmät sekä toimittajat.

Todentava näyttö: BIA-raportti, prosessikartta, riippuvuuskuvaukset, kriittisyysluokitus.

3. Onko kriittisille toiminnoille määritelty palautumistavoitteet?

Hyväksymiskriteeri: Sallitut keskeytysajat, palautumisajat, tietojen palautuspisteet ja vähimmäispalvelutasot on hyväksytty.

Todentava näyttö: RTO- ja RPO-tavoitteet, palvelutasot, johdon hyväksynnät, järjestelmäluettelo.

4. [KRIITTINEN] Onko kriittisille toiminnoille laadittu ajantasaiset jatkuvuus- ja palautumissuunnitelmat?

Hyväksymiskriteeri: Suunnitelmat sisältävät käynnistyskriteerit, vastuut, yhteystiedot, varamenettelyt, viestinnän ja palautumisen.

Todentava näyttö: jatkuvuussuunnitelmat, palautumisohjeet, yhteystietolistat, versionhallinta.

5. Onko kriisijohtamisen päätöksenteko ja tilannekuvan muodostaminen määritelty?

Hyväksymiskriteeri: Kriisiryhmän roolit, koollekutsuminen, päätösloki, tilannekuva ja eskalointitasot on kuvattu.

Todentava näyttö: kriisijohtamisohje, roolikortit, päätöslokipohja, yhteystiedot.

6. Onko kriisiviestintä suunniteltu henkilöstölle, asiakkaille, toimittajille ja viranomaisille?

Hyväksymiskriteeri: Viestintävastuut, hyväksynnät, kanavat, varakanavat ja valmiit viestipohjat on määritelty.

Todentava näyttö: kriisiviestintäsuunnitelma, viestipohjat, yhteystietoluettelot, harjoitusraportit.

7. Onko kriittisille henkilöstö-, tila-, teknologia- ja toimittajariippuvuuksille varajärjestelyt?

Hyväksymiskriteeri: Varajärjestelyt ovat realistisia, resursoituja, sopimuksin tuettuja ja dokumentoituja.

Todentava näyttö: varahenkilöluettelo, varatilasopimukset, varayhteydet, toimittajasopimukset.

8. [KRIITTINEN] Testataanko jatkuvuus- ja palautumismenettelyjä säännöllisesti?

Hyväksymiskriteeri: Harjoitukset kattavat olennaiset skenaariot, tavoitteet mitataan ja puutteet korjataan määräajassa.

Todentava näyttö: harjoitussuunnitelma, testitulokset, palautumisajat, korjaavat toimet.

9. Päivitetäänkö suunnitelmat muutosten, poikkeamien ja harjoitusten jälkeen?

Hyväksymiskriteeri: Omistajat katselmoivat suunnitelmat säännöllisesti ja aina olennaisen muutoksen tai havainnon jälkeen.

Todentava näyttö: katselmuspöytäkirjat, muutoshistoria, poikkeamaraportit, päivitetyt suunnitelmat.

10. Raportoidaanko jatkuvuuskyvystä johdolle?

Hyväksymiskriteeri: Raportointi sisältää valmiustason, harjoitusten tulokset, avoimet riskit, resurssitarpeet ja päätösehdotukset.

Todentava näyttö: johdon raportit, mittarit, riskirekisteri, päätöspöytäkirjat.

HÄIRIÖ- JA POIKKEAMANHALLINTA

Auditoinnin tavoite

Selvittää, tunnistaako, käsitteleekö ja ehkäiseekö yritys toiminnalliset, turvallisuus- ja tietosuojapoikkeamat yhdenmukaisesti ja oikea-aikaisesti.

1. Onko yrityksellä hyväksytty häiriö- ja poikkeamanhallintaprosessi?

Hyväksymiskriteeri: Prosessi kattaa ilmoittamisen, kirjaamisen, luokittelun, eskaloinnin, tutkinnan, viestinnän ja sulkemisen.

Todentava näyttö: prosessikuvaus, poikkeamaohje, hyväksymispäätös, vastuumatriisi.

2. Onko henkilöstöllä helppo ja tunnettu tapa ilmoittaa häiriöistä ja poikkeamista?

Hyväksymiskriteeri: Ilmoituskanavat ovat saavutettavia, ohjeistetut ja käytettävissä myös normaalin työajan ulkopuolella.

Todentava näyttö: ilmoitusohje, palvelukanavat, koulutusmateriaali, ilmoitusmäärät.

3. Kirjataanko kaikki olennaiset häiriöt ja poikkeamat keskitetysti ja jäljitettävästi?

Hyväksymiskriteeri: Tapauksella on tunniste, omistaja, aikaleimat, vaikutus, käsittelyhistoria ja sulkemispäätös.

Todentava näyttö: poikkeamarekisteri, tikettijärjestelmä, lokit, tapausotos.

4. Luokitellaanko tapaukset vaikutuksen, kiireellisyyden ja lakisääteisten velvoitteiden perusteella?

Hyväksymiskriteeri: Luokittelu ohjaa prioriteettia, vasteaikaa, resursointia, eskalointia ja ilmoituksia.

Todentava näyttö: luokitteluohje, prioriteettimatriisi, palvelutasot, tapausotos.

5. [KRIITTINEN] Onko vakaville poikkeamille ympärivuorokautinen eskalointi- ja johtamismenettely?

Hyväksymiskriteeri: Vastuut, yhteystiedot, päätösvaltuudet, tilannekuva ja viestintä toimivat myös työajan ulkopuolella.

Todentava näyttö: vakavan poikkeaman ohje, päivystyslista, hälytyslokit, tapausraportit.

6. Rajataanko poikkeaman vaikutukset ja turvataanko todistusaineisto viipymättä?

Hyväksymiskriteeri: Rajaamistoimet ovat valtuutettuja, dokumentoituja ja säilyttävät tutkinnan kannalta olennaiset tiedot.

Todentava näyttö: toimintakortit, forensiikkaohje, eristyslokit, todistusaineistorekisteri.

7. Täytetäänkö viranomaisille, asiakkaille ja muille osapuolille tehtävät ilmoitusvelvollisuudet?

Hyväksymiskriteeri: Ilmoitustarve, määräaika, sisältö, hyväksyntä ja lähettäminen ratkaistaan dokumentoidusti.

Todentava näyttö: ilmoitusarviot, viranomaisilmoitukset, asiakasviestit, päätöslokit.

8. [KRIITTINEN] Selvitetäänkö vakavien ja toistuvien poikkeamien juurisyyt?

Hyväksymiskriteeri: Analyysi tunnistaa tekniset, inhimilliset ja johtamiseen liittyvät perussyyt sekä estävät toimenpiteet.

Todentava näyttö: juurisyyanalyysit, tutkintaraportit, haastattelumuistiot, tekniset havainnot.

9. Seurataanko korjaavien ja ehkäisevien toimenpiteiden toteutumista ja vaikuttavuutta?

Hyväksymiskriteeri: Toimilla on omistaja, määräaika ja hyväksymiskriteeri, ja niiden vaikutus varmennetaan.

Todentava näyttö: toimenpiderekisteri, seurantakokoukset, uusintatestit, sulkemishyväksynnät.

10. Hyödynnetäänkö poikkeamatietoa koulutuksessa, riskienhallinnassa ja prosessien kehittämisessä?

Hyväksymiskriteeri: Trendejä analysoidaan, opit jaetaan ja vastaavat riskit käsitellään muissa kohteissa.

Todentava näyttö: trendiraportit, koulutusmateriaalit, riskirekisterin muutokset, kehityspäätökset.

JÄRJESTELMÄHANKINTA JA KÄYTTÖÖNOTTO

Auditoinnin tavoite

Selvittää, huomioidaanko järjestelmähankinnoissa liiketoiminta-, turvallisuus-, tietosuoja-, integraatio- ja jatkuvuusvaatimukset ennen käyttöönottoa.

1. Onko yrityksellä hyväksytty järjestelmähankinnan ja käyttöönoton prosessi?

Hyväksymiskriteeri: Prosessi kattaa tarpeen, vaatimukset, arvioinnin, hankintapäätöksen, testauksen, hyväksynnän ja luovutuksen ylläpitoon.

Todentava näyttö: prosessikuvaus, hankintaohje, projektimalli, hyväksymispäätös.

2. Määritelläänkö järjestelmälle omistaja, käyttötarkoitus ja liiketoimintavaatimukset ennen hankintaa?

Hyväksymiskriteeri: Omistaja, käyttäjät, tavoitteet, rajaukset, tiedot, integraatiot ja kriittisyys on dokumentoitu.

Todentava näyttö: hankintaesitys, vaatimusmäärittely, omistajapäätös, prosessikuvaus.

3. Tunnistetaanko turvallisuus-, tietosuoja- ja jatkuvuusvaatimukset hankinnan alkuvaiheessa?

Hyväksymiskriteeri: Vaatimukset perustuvat riskiluokkaan ja sisältyvät tarjouspyyntöihin, arviointiin ja sopimukseen.

Todentava näyttö: turvallisuusvaatimukset, tietosuojavaatimukset, jatkuvuusvaatimukset, tarjouspyyntö.

4. Arvioidaanko vaihtoehtojen soveltuvuus ja toimittajan kyvykkyys dokumentoidusti?

Hyväksymiskriteeri: Arviointi kattaa toiminnallisuuden, turvallisuuden, elinkaaren, kustannukset, toimittajariskin ja irtautumisen.

Todentava näyttö: vertailumatriisi, toimittaja-arviointi, riskianalyysi, hankintapäätös.

5. [KRIITTINEN] Tehdäänkö korkean riskin järjestelmälle turvallisuus- ja tietosuojavaikutusten arviointi ennen päätöstä?

Hyväksymiskriteeri: Merkittävät riskit käsitellään, jäännösriskit hyväksytään ja tarvittavat kontrollit sisällytetään toteutukseen.

Todentava näyttö: riskinarviointi, DPIA, käsittelysuunnitelma, hyväksymispäätös.

6. Sisältävätkö sopimukset riittävät palvelu-, turvallisuus-, tuki- ja jatkuvuusehdot?

Hyväksymiskriteeri: Sopimuksissa määritellään vastuut, palvelutasot, tietojen omistus, poikkeamailmoitukset, auditointioikeus ja päättäminen.

Todentava näyttö: sopimus, palvelutasoliite, tietojenkäsittelyehdot, turvallisuusliite.

7. Testataanko järjestelmä erillisessä ympäristössä ennen tuotantokäyttöä?

Hyväksymiskriteeri: Toiminnallisuus, integraatiot, käyttöoikeudet, lokitus, suorituskyky, palautuminen ja turvallisuus testataan hyväksytyllä suunnitelmalla.

Todentava näyttö: testisuunnitelma, testitulokset, haavoittuvuustestit, poikkeamalista.

8. [KRIITTINEN] Hyväksytäänkö järjestelmä tuotantoon vasta, kun kriittiset vaatimukset ja puutteet on käsitelty?

Hyväksymiskriteeri: Käyttöönotolla on omistajan, turvallisuuden ja ylläpidon hyväksyntä, eikä avoimia estäviä puutteita ole.

Todentava näyttö: käyttöönottopäätös, hyväksymispöytäkirja, avoimet puutteet, riskihyväksynnät.

9. Dokumentoidaanko järjestelmä ja siirretäänkö vastuu ylläpidolle hallitusti?

Hyväksymiskriteeri: Arkkitehtuuri, asetukset, integraatiot, käyttöohjeet, varmistukset, yhteystiedot ja tukivastuut luovutetaan.

Todentava näyttö: järjestelmädokumentaatio, ylläpitosopimus, luovutuspöytäkirja, koulutusmerkinnät.

10. Tehdäänkö käyttöönoton jälkeen jälkiarviointi?

Hyväksymiskriteeri: Toteutuneet hyödyt, häiriöt, turvallisuus, käyttäjäpalaute ja jatkotoimet arvioidaan sovitun ajan kuluttua.

Todentava näyttö: jälkiarviointiraportti, mittarit, käyttäjäpalaute, kehitystoimenpiteet.

TURVALLINEN OHJELMISTOKEHITYS

Auditoinnin tavoite

Selvittää, rakennetaanko ja ylläpidetäänkö yrityksen ohjelmistot turvallisesti koko kehityksen elinkaaren ajan vaatimuksista tuotantoon ja korjauksiin.

1. Onko yrityksellä hyväksytty turvallisen ohjelmistokehityksen toimintamalli?

Hyväksymiskriteeri: Malli kattaa vaatimukset, suunnittelun, toteutuksen, testauksen, julkaisemisen, ylläpidon ja käytöstä poistamisen.

Todentava näyttö: kehitysmalli, turvallisen koodauksen ohje, hyväksymispäätös, vastuumatriisi.

2. Määritelläänkö turvallisuus- ja tietosuojavaatimukset ennen toteutusta?

Hyväksymiskriteeri: Vaatimukset ovat testattavia, riskiperusteisia ja jäljitettävissä suunnittelusta hyväksyntään.

Todentava näyttö: vaatimusmäärittely, käyttäjätarinat, hyväksymiskriteerit, jäljitettävyysmatriisi.

3. Tehdäänkö merkittäville ratkaisuille uhkamallinnus tai vastaava suunnittelun turvallisuusarviointi?

Hyväksymiskriteeri: Tietovirrat, luottamusrajat, hyökkäystavat ja suojaustoimet arvioidaan ennen toteutuspäätöksiä.

Todentava näyttö: uhkamallit, arkkitehtuurikatselmukset, riskirekisteri, suunnittelupäätökset.

4. Eristetäänkö kehitys-, testi- ja tuotantoympäristöt toisistaan?

Hyväksymiskriteeri: Ympäristöillä on erilliset käyttöoikeudet, tiedot, salaisuudet ja julkaisureitit; tuotantotietojen käyttö on rajattu.

Todentava näyttö: ympäristökuvaukset, käyttöoikeudet, verkkosäännöt, testidatan ohjeet.

5. Hallitaanko lähdekoodi, muutokset ja katselmoinnit jäljitettävästi?

Hyväksymiskriteeri: Koodi säilytetään hyväksytyssä versionhallinnassa, muutokset vertaisarvioidaan ja suojatut haarat estävät luvattomat julkaisut.

Todentava näyttö: versionhallintalokit, yhdistämispyynnöt, katselmointimerkinnät, haarasäännöt.

6. [KRIITTINEN] Tarkastetaanko koodi ja riippuvuudet automaattisesti haavoittuvuuksien ja salaisuuksien varalta?

Hyväksymiskriteeri: SAST-, riippuvuus- ja salaisuusskannaukset kuuluvat kehitysputkeen, ja kriittiset löydökset estävät julkaisun.

Todentava näyttö: skannausraportit, CI/CD-asetukset, estorajat, korjaustiketit.

7. Testataanko sovelluksen turvallisuus ennen tuotantoon julkaisemista?

Hyväksymiskriteeri: Testaus kattaa riskitason mukaisesti esimerkiksi käyttöoikeudet, syötteet, istunnot, rajapinnat ja haavoittuvuudet.

Todentava näyttö: turvallisuustestisuunnitelma, DAST-raportit, penetraatiotesti, hyväksyntä.

8. Suojataanko kehitys- ja julkaisuympäristöjen salaisuudet sekä allekirjoitusavaimet?

Hyväksymiskriteeri: Salaisuuksia ei tallenneta lähdekoodiin, ne säilytetään avainholvissa ja käyttöä valvotaan.

Todentava näyttö: avainholvin asetukset, salaisuusskannaukset, HSM-lokit, käyttöoikeusraportit.

9. [KRIITTINEN] Korjataanko julkaistujen ohjelmistojen haavoittuvuudet riskiperusteisissa määräajoissa?

Hyväksymiskriteeri: Haavoittuvuudet luokitellaan, omistetaan, korjataan, testataan ja tarvittaessa tiedotetaan asiakkaille.

Todentava näyttö: haavoittuvuusrekisteri, korjausjulkaisut, testitulokset, asiakastiedotteet.

10. Ylläpidetäänkö ohjelmistokomponenttien ja riippuvuuksien luetteloa?

Hyväksymiskriteeri: Yritys pystyy tunnistamaan käytetyt komponentit, versiot, lisenssit ja tunnetuille haavoittuvuuksille altistuvat tuotteet.

Todentava näyttö: SBOM, riippuvuusluettelo, lisenssiraportit, haavoittuvuushaku.

MUUTOSTEN- JA JULKAISUJENHALLINTA

Auditoinnin tavoite

Selvittää, suunnitellaanko, arvioidaanko, hyväksytäänkö, testataanko ja toteutetaanko järjestelmä- ja palvelumuutokset hallitusti.

1. Onko yrityksellä hyväksytty muutosten- ja julkaisujenhallintaprosessi?

Hyväksymiskriteeri: Prosessi kattaa normaalit, vakio- ja hätämuutokset sekä arvioinnin, hyväksynnän, testauksen, toteutuksen ja jälkiarvioinnin.

Todentava näyttö: prosessikuvaus, muutosohje, hyväksymispäätös, vastuumatriisi.

2. Kirjataanko kaikki tuotantoon vaikuttavat muutokset ennen toteutusta?

Hyväksymiskriteeri: Muutospyynnöllä on tunniste, omistaja, kuvaus, kohde, aikataulu, vaikutus ja tila.

Todentava näyttö: muutosrekisteri, tiketit, julkaisukalenteri, tapausotos.

3. Arvioidaanko muutoksen vaikutukset palveluun, turvallisuuteen, tietosuojaan ja jatkuvuuteen?

Hyväksymiskriteeri: Arviointi kattaa riippuvuudet, riskit, kapasiteetin, käyttökatkon, asiakasvaikutukset ja sääntelyvelvoitteet.

Todentava näyttö: vaikutusarvio, riskianalyysi, arkkitehtuurikatselmus, sidosryhmälausunnot.

4. Hyväksytäänkö muutokset valtuuksien ja riskitason mukaisesti?

Hyväksymiskriteeri: Hyväksyjä on riippumaton toteuttajasta tarvittaessa, ja merkittävät muutokset käsitellään muutosryhmässä.

Todentava näyttö: hyväksymismatriisi, CAB-pöytäkirjat, sähköiset hyväksynnät, muutosotos.

5. Testataanko muutokset ennen tuotantoon vientiä?

Hyväksymiskriteeri: Testaus vastaa muutoksen riskiä ja kattaa toiminnallisuuden, integraatiot, turvallisuuden ja palautettavuuden.

Todentava näyttö: testisuunnitelma, testitulokset, hyväksymismerkinnät, poikkeamalista.

6. [KRIITTINEN] Onko merkittävillä muutoksilla toteutus-, viestintä- ja palautussuunnitelma?

Hyväksymiskriteeri: Suunnitelmassa ovat vaiheet, vastuut, valvonta, keskeytysrajat, palautusmenettely ja sidosryhmäviestintä.

Todentava näyttö: toteutussuunnitelma, palautussuunnitelma, viestintäsuunnitelma, tarkistuslista.

7. Eriytetäänkö muutoksen kehittäminen, hyväksyminen ja tuotantoon vieminen riittävästi?

Hyväksymiskriteeri: Vaaralliset tehtäväyhdistelmät on estetty tai niihin kohdistuu hyväksytty korvaava valvonta.

Todentava näyttö: SoD-matriisi, käyttöoikeusraportit, julkaisulokit, poikkeuspäätökset.

8. [KRIITTINEN] Hallitaanko hätämuutokset nopeutetulla mutta valvotulla menettelyllä?

Hyväksymiskriteeri: Hätämuutos dokumentoidaan, valtuutetaan, testataan mahdollisuuksien mukaan ja katselmoidaan jälkikäteen.

Todentava näyttö: hätämuutostiketit, hyväksyntälokit, toteutuslokit, jälkikatselmukset.

9. Varmistetaanko muutoksen onnistuminen ja palvelun tila toteutuksen jälkeen?

Hyväksymiskriteeri: Seuranta, tekniset tarkistukset ja käyttäjä- tai palveluomistajan hyväksyntä tehdään ennen muutoksen sulkemista.

Todentava näyttö: valvontaraportit, käyttöönottotarkistus, hyväksyntä, häiriöraportit.

10. Analysoidaanko epäonnistuneita ja häiriöitä aiheuttaneita muutoksia?

Hyväksymiskriteeri: Syyt, vaikutukset ja opit dokumentoidaan ja toimintamallia tai teknisiä kontrolleja parannetaan.

Todentava näyttö: jälkiarvioinnit, juurisyyanalyysit, muutosmittarit, kehitystoimenpiteet.

PILVIPALVELUJEN HALLINTA

Auditoinnin tavoite

Selvittää, valitseeko, määrittääkö, käyttääkö, valvooko ja päättääkö yritys pilvipalvelut turvallisesti ja hallitusti.

1. Onko yrityksellä hyväksytty pilvipalvelujen hallintamalli?

Hyväksymiskriteeri: Malli määrittelee hyväksytyt palvelut, vastuut, riskiluokat, käyttöönoton, valvonnan ja poistumisen.

Todentava näyttö: pilvipolitiikka, prosessikuvaus, hyväksyttyjen palvelujen luettelo, hyväksymispäätös.

2. Hyväksytäänkö pilvipalvelut ennen käyttöönottoa?

Hyväksymiskriteeri: Palvelun omistaja, käyttötarkoitus, käsiteltävät tiedot, kustannukset, riskit ja sopimukset arvioidaan.

Todentava näyttö: pilvipalvelupyyntö, riskinarviointi, tietosuojaselvitys, hankintapäätös.

3. Onko yrityksen ja pilvipalveluntarjoajan vastuunjako dokumentoitu?

Hyväksymiskriteeri: Teknisten asetusten, tietojen, käyttöoikeuksien, lokituksen, varmistusten, poikkeamien ja jatkuvuuden vastuut ovat selvät.

Todentava näyttö: vastuunjakomatriisi, palvelukuvaus, sopimus, arkkitehtuurikuvaus.

4. Arvioidaanko tietojen sijainti, siirrot ja palvelun alihankkijat?

Hyväksymiskriteeri: Tietojen käsittelymaat, siirtoperusteet ja alihankintaketju hyväksytään ennen käyttöä ja muutoksia valvotaan.

Todentava näyttö: sijaintitiedot, käsittelysopimus, alihankkijaluettelo, siirtoperustearvio.

5. [KRIITTINEN] Määritetäänkö pilvipalvelut hyväksyttyjen turvallisuusasetusten mukaisesti?

Hyväksymiskriteeri: Käytössä ovat turvalliset perusasetukset, vahva tunnistaminen, vähimmät oikeudet, salaus ja julkisuuden estot.

Todentava näyttö: konfiguraatiostandardi, CSPM-raportit, asetustarkastus, poikkeusluvat.

6. Hallitaanko pilvipalvelujen käyttäjä-, ylläpito- ja palvelutunnukset keskitetysti?

Hyväksymiskriteeri: Tunnukset kytketään yrityksen identiteetinhallintaan, korotetut oikeudet suojataan ja tekniset salaisuudet hallitaan.

Todentava näyttö: SSO-asetukset, käyttöoikeusraportit, PAM-raportit, avainholvin tiedot.

7. Kerätäänkö pilvipalveluista riittävät lokit ja valvontatiedot?

Hyväksymiskriteeri: Hallinta-, käyttö-, tietoturva- ja tietovirtalokit ovat käytössä, suojattuja ja yhdistettyjä valvontaan.

Todentava näyttö: pilvilokit, SIEM-integraatio, hälytyssäännöt, säilytysasetukset.

8. [KRIITTINEN] Onko pilvipalvelujen varmuuskopiointi, palautuminen ja jatkuvuus varmistettu?

Hyväksymiskriteeri: Palveluntarjoajan ja yrityksen vastuut, palautumistavoitteet, varmistukset ja alueelliset riippuvuudet on arvioitu ja testattu.

Todentava näyttö: jatkuvuussuunnitelma, varmistusraportit, palautustestit, palvelutasot.

9. Seurataanko pilvipalvelujen kustannuksia, käyttöä, turvallisuutta ja sopimusehtojen toteutumista?

Hyväksymiskriteeri: Poikkeamat, käyttämättömät resurssit, julkiset kohteet, vanhentuneet oikeudet ja palvelutaso raportoidaan.

Todentava näyttö: kustannusraportit, CSPM-havainnot, palveluraportit, katselmuspöytäkirjat.

10. Päätetäänkö pilvipalvelun käyttö hallitusti?

Hyväksymiskriteeri: Tiedot palautetaan tai siirretään, tunnukset ja resurssit poistetaan, säilytysvelvoitteet täytetään ja poistaminen todennetaan.

Todentava näyttö: irtautumissuunnitelma, tietojen vientiraportti, poistotodistus, päättämistarkistus.

VARMUUSKOPIOINTI JA PALAUTTAMINEN

Auditoinnin tavoite

Selvittää, varmistetaanko yrityksen kriittiset tiedot ja järjestelmät luotettavasti sekä voidaanko ne palauttaa määritellyssä ajassa

.

1. Onko yrityksellä hyväksytty varmuuskopiointi- ja palautuspolitiikka?

Hyväksymiskriteeri: Politiikka määrittelee kohteet, vastuut, menetelmät, säilytyksen, suojauksen, testauksen ja poikkeamien käsittelyn.

Todentava näyttö: varmuuskopiointipolitiikka, hyväksymispäätös, vastuumatriisi, versionhallinta.

2. Onko varmuuskopioitavat tiedot, järjestelmät ja määritykset tunnistettu?

Hyväksymiskriteeri: Kattavuus perustuu kriittisyyteen, palautumistavoitteisiin ja omistajan hyväksymään luetteloon.

Todentava näyttö: varmistuskohdeluettelo, järjestelmärekisteri, BIA, omistajahyväksynnät.

3. Vastaavatko varmuuskopiointitiheydet ja säilytysajat liiketoiminnan sekä lain vaatimuksia?

Hyväksymiskriteeri: Aikataulut täyttävät hyväksytyt palautuspistetavoitteet ja säilytysvelvoitteet ilman tarpeetonta säilyttämistä.

Todentava näyttö: varmistusaikataulut, RPO-tavoitteet, säilytysaikataulu, järjestelmäasetukset.

4. [KRIITTINEN] Eristetäänkö ja suojataanko varmuuskopiot tuotantoympäristöstä ja luvattomalta muuttamiselta?

Hyväksymiskriteeri: Käytössä on erillisiä tai muuttumattomia kopioita, rajatut oikeudet, vahva tunnistaminen ja salaus.

Todentava näyttö: arkkitehtuurikuvaus, immutability-asetukset, käyttöoikeusraportit, salausasetukset.

5. Valvotaanko varmuuskopiointien onnistumista päivittäin tai riskitason mukaisesti?

Hyväksymiskriteeri: Epäonnistumiset havaitaan, eskaloidaan, korjataan ja niiden vaikutus arvioidaan viipymättä.

Todentava näyttö: varmistusraportit, hälytykset, tiketit, poikkeamaseuranta.

6. Suojataanko varmuuskopioiden siirto, säilytys ja avaimet?

Hyväksymiskriteeri: Tiedot salataan siirrossa ja levossa, avaimet hallitaan erillään ja fyysiset kopiot kuljetetaan turvallisesti.

Todentava näyttö: salausasetukset, avainhallintalokit, kuljetusketju, säilytystilan tarkastus.

7. [KRIITTINEN] Testataanko tietojen ja järjestelmien palauttamista säännöllisesti?

Hyväksymiskriteeri: Testit kattavat kriittiset kohteet, mittaavat palautusajan ja varmistavat tiedon käyttökelpoisuuden.

Todentava näyttö: palautustestisuunnitelma, testiraportit, RTO-tulokset, hyväksyntä.

8. Onko laajalle häiriölle tai kiristyshaittaohjelmalle määritelty palautusjärjestys?

Hyväksymiskriteeri: Kriittisten palvelujen riippuvuudet, puhtaan palautuksen vaiheet, päätöksenteko ja viestintä on kuvattu.

Todentava näyttö: katastrofipalautussuunnitelma, riippuvuuskartta, toimintakortit, harjoitusraportti.

9. Hallitaanko varmuuskopioiden poistaminen ja tietovälineiden hävittäminen?

Hyväksymiskriteeri: Poistaminen noudattaa säilytysaikoja ja tietojen luokitusta, ja toteutus voidaan todentaa.

Todentava näyttö: poistolokit, hävitystodistukset, säilytysasetukset, hyväksynnät.

10. Raportoidaanko varmuuskopioinnin kattavuus ja palautuskyky johdolle sekä omistajille?

Hyväksymiskriteeri: Raportointi sisältää onnistumisasteen, puuttuvat kohteet, testitulokset, poikkeamat ja korjaavat toimet.

Todentava näyttö: mittariraportit, palvelukatselmukset, riskirekisteri, toimenpideseuranta.

RISKIENHALLINTA

Auditoinnin tavoite

Selvittää, tunnistaako, arvioiko, käsitteleekö ja seuraako yritys tavoitteitaan uhkaavia riskejä johdonmukaisesti ja päätöksenteon tukena.

1. Onko yrityksellä hyväksytty ja ajantasainen riskienhallintapolitiikka?

Hyväksymiskriteeri: Politiikka on kirjallinen, johdon hyväksymä, yrityksen toimintaan soveltuva ja henkilöstön saatavilla.

Todentava näyttö: riskienhallintapolitiikka, hyväksymispäätös, julkaisukanava, versionhallintatiedot.

2. Onko riskienhallinnan vastuut, omistajuudet ja raportointisuhteet määritelty?

Hyväksymiskriteeri: Hallitus tai johto, riskien omistajat, prosessinomistajat ja valvontatoiminnot tietävät tehtävänsä ja valtuutensa.

Todentava näyttö: vastuumatriisi, tehtävänkuvat, hallintosääntö, raportointimalli.

3. Onko yrityksellä yhtenäiset riskien tunnistamis- ja arviointikriteerit?

Hyväksymiskriteeri: Todennäköisyys, vaikutus, riskitaso, aikajänne ja hyväksyttävä riskitaso on kuvattu ja yhdenmukaisesti käytössä.

Todentava näyttö: riskimenetelmä, arviointiasteikot, riskimatriisi, ohjeistus.

4. Tunnistetaanko riskit säännöllisesti ja olennaisten muutosten yhteydessä?

Hyväksymiskriteeri: Arviointi kattaa strategiset, taloudelliset, toiminnalliset, turvallisuus-, sääntely- ja toimittajariskit.

Todentava näyttö: riskityöpajojen aineistot, muutosarviot, riskirekisteri, haastattelut.

5. Onko jokaiselle merkittävälle riskille nimetty omistaja?

Hyväksymiskriteeri: Omistaja vastaa riskin arvioinnista, käsittelystä, seurannasta ja raportoinnista.

Todentava näyttö: riskirekisteri, omistajaluettelo, hyväksymismerkinnät, seurantapöytäkirjat.

6. [KRIITTINEN] Käsitelläänkö hyväksyttävän tason ylittävät riskit määräajassa?

Hyväksymiskriteeri: Riskille valitaan välttäminen, pienentäminen, siirtäminen tai hyväksyminen, ja toimenpiteet resursoidaan.

Todentava näyttö: riskinkäsittelysuunnitelma, budjetti, toimenpiderekisteri, seurantatiedot.

7. [KRIITTINEN] Hyväksytäänkö jäännösriskit valtuuksien mukaisesti?

Hyväksymiskriteeri: Hyväksyjä ymmärtää riskin vaikutuksen, perustelut, voimassaoloajan ja mahdolliset lisäehdot.

Todentava näyttö: riskihyväksyntä, päätöspöytäkirja, poikkeuslupa, määräaikaseuranta.

8. Huomioidaanko riskit hankkeissa, hankinnoissa, muutoksissa ja päätöksenteossa?

Hyväksymiskriteeri: Riskinarviointi on osa päätösportteja ja merkittävät riskit esitetään päätöksentekijälle ennen sitoutumista.

Todentava näyttö: projektipäätökset, hankinta-arviot, muutospyynnöt, päätösesitykset.

9. Seurataanko riskien muutoksia ja käsittelytoimien vaikuttavuutta?

Hyväksymiskriteeri: Riskitasot päivitetään sovitusti ja kontrollien toimivuus varmennetaan mittareilla tai testeillä.

Todentava näyttö: riskikatselmukset, kontrollitestit, mittarit, päivitetty riskirekisteri.

10. Raportoidaanko yrityksen riskit johdolle ymmärrettävästi ja oikea-aikaisesti?

Hyväksymiskriteeri: Raportointi näyttää merkittävimmät riskit, trendit, riippuvuudet, avoimet toimet ja päätöstarpeet.

Todentava näyttö: riskiraportit, johtoryhmän pöytäkirjat, riskikartat, päätösseuranta.

VAATIMUSTENMUKAISUUDEN HALLINTA

Auditoinnin tavoite

Selvittää, tunnistaako ja täyttääkö yritys toimintaansa koskevat lait, viranomaisvaatimukset, sopimukset, standardit ja sisäiset velvoitteet.

1. Onko yrityksellä hyväksytty vaatimustenmukaisuuden hallintaprosessi?

Hyväksymiskriteeri: Prosessi kattaa vaatimusten tunnistamisen, tulkinnan, vastuutuksen, toimeenpanon, seurannan ja raportoinnin.

Todentava näyttö: prosessikuvaus, compliance-ohje, hyväksymispäätös, vastuumatriisi.

2. Ylläpitääkö yritys ajantasaista rekisteriä sovellettavista vaatimuksista?

Hyväksymiskriteeri: Rekisterissä ovat lait, viranomaispäätökset, sopimusehdot, standardit, asiakkaiden vaatimukset ja sisäiset sitoumukset.

Todentava näyttö: vaatimusrekisteri, lakiseuranta, sopimusluettelo, standardiluettelo.

3. Onko jokaiselle merkittävälle vaatimukselle nimetty vastuuhenkilö?

Hyväksymiskriteeri: Vastuuhenkilö seuraa muutoksia, tulkitsee vaikutukset ja varmistaa toimeenpanon.

Todentava näyttö: vastuuluettelo, tehtävänkuvat, vaatimusrekisteri, seurantamerkinnät.

4. Seurataanko vaatimusten muutoksia järjestelmällisesti?

Hyväksymiskriteeri: Luotettavat seurantakanavat, arviointitiheys ja muutosten käsittelymenettely on määritelty.

Todentava näyttö: lakiseurantapalvelu, uutiskirjeet, muutosarviot, katselmuspöytäkirjat.

5. Arvioidaanko uusien tai muuttuneiden vaatimusten vaikutukset yrityksen toimintaan?

Hyväksymiskriteeri: Vaikutus prosesseihin, järjestelmiin, sopimuksiin, resursseihin, koulutukseen ja määräaikoihin dokumentoidaan.

Todentava näyttö: vaikutusarviot, toimeenpanosuunnitelmat, budjettipäätökset, projektit.

6. [KRIITTINEN] Toteutetaanko lakisääteiset ja sopimukselliset velvoitteet määräajassa?

Hyväksymiskriteeri: Toimenpiteillä on omistaja, aikataulu ja hyväksymiskriteeri, ja viivästykset eskaloidaan.

Todentava näyttö: toimenpiderekisteri, viranomaisilmoitukset, sopimusraportit, seurantatiedot.

7. Varmistetaanko henkilöstön tietoisuus tehtäviin liittyvistä vaatimuksista?

Hyväksymiskriteeri: Koulutus ja ohjeistus kohdistetaan rooleittain, ja osaaminen varmistetaan tarvittaessa.

Todentava näyttö: koulutusrekisteri, työohjeet, osaamistestit, tiedotteet.

8. Arvioidaanko vaatimustenmukaisuutta tarkastuksilla ja kontrollitestauksella?

Hyväksymiskriteeri: Arvioinnit ovat riskiperusteisia, riippumattomia tarvittaessa ja kattavat käytännön toteutuksen.

Todentava näyttö: auditointiohjelma, tarkastusraportit, kontrollitestit, otantatulokset.

9. [KRIITTINEN] Käsitelläänkö vaatimustenvastaisuudet ja viranomaisasiat hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, vaikutukset arvioidaan, viranomaisyhteistyö vastuutetaan ja korjaavat toimet seurataan.

Todentava näyttö: poikkeamarekisteri, viranomaiskirjeenvaihto, juurisyyanalyysi, toimenpideseuranta.

10. Raportoidaanko vaatimustenmukaisuuden tila johdolle?

Hyväksymiskriteeri: Raportointi sisältää merkittävät muutokset, puutteet, seuraamusriskit, avoimet toimet ja tarvittavat päätökset.

Todentava näyttö: compliance-raportit, johdon pöytäkirjat, riskirekisteri, päätösseuranta.

DOKUMENTTIEN JA TALLENTEIDEN HALLINTA

Auditoinnin tavoite

Selvittää, laaditaanko, hyväksytäänkö, julkaistaanko, säilytetäänkö ja hävitetäänkö yrityksen asiakirjat ja tallenteet hallitusti sekä jäljitettävästi.

1. Onko yrityksellä hyväksytty dokumenttien ja tallenteiden hallintaprosessi?

Hyväksymiskriteeri: Prosessi kattaa laatimisen, tarkastamisen, hyväksymisen, julkaisemisen, muuttamisen, säilyttämisen ja hävittämisen.

Todentava näyttö: prosessikuvaus, dokumentinhallintaohje, hyväksymispäätös, vastuumatriisi.

2. Onko dokumenttityypeille määritelty omistajat ja hyväksyjät?

Hyväksymiskriteeri: Omistaja vastaa sisällön oikeellisuudesta, ajantasaisuudesta, luokituksesta ja määräaikaisesta katselmoinnista.

Todentava näyttö: dokumenttirekisteri, omistajaluettelo, hyväksymismatriisi, tehtävänkuvat.

3. Käytetäänkö hyväksyttyjä asiakirjapohjia, tunnisteita ja metatietoja?

Hyväksymiskriteeri: Dokumentista ilmenevät nimi, omistaja, versio, hyväksyjä, voimassaolo, luokitus ja tarvittaessa säilytysaika.

Todentava näyttö: asiakirjapohjat, metatietomalli, dokumenttiotos, ohjeistus.

4. Tarkastetaanko ja hyväksytäänkö dokumentit ennen julkaisemista?

Hyväksymiskriteeri: Sisällön oikeellisuus, soveltuvuus ja vaatimustenmukaisuus varmennetaan valtuutetulla hyväksymisellä.

Todentava näyttö: hyväksymistyönkulut, tarkastusmerkinnät, päätöslokit, dokumenttiotos.

5. Varmistetaanko, että käyttäjillä on saatavilla vain voimassa olevat ohjeet?

Hyväksymiskriteeri: Julkaisukanavat ovat hallittuja, vanhat versiot poistetaan käytöstä ja voimassa oleva versio on tunnistettavissa.

Todentava näyttö: intranet, dokumentinhallintajärjestelmä, versiohistoria, työpisteotos.

6. Hallitaanko dokumenttien muutokset ja versiot jäljitettävästi?

Hyväksymiskriteeri: Muutoksen tekijä, sisältö, ajankohta, peruste ja hyväksyntä voidaan todentaa.

Todentava näyttö: muutoshistoria, versionhallintalokit, hyväksynnät, vertailuversiot.

7. [KRIITTINEN] Suojataanko luottamukselliset dokumentit ja tallenteet luvattomalta käytöltä ja muuttamiselta?

Hyväksymiskriteeri: Pääsy perustuu tehtävään, tiedot salataan tarvittaessa ja eheyttä sekä käyttöä valvotaan.

Todentava näyttö: käyttöoikeusraportit, salausasetukset, lokit, luokitusmerkinnät.

8. Onko tallenteille määritelty säilytysajat ja säilytysmuodot?

Hyväksymiskriteeri: Säilytys perustuu lakiin, sopimukseen ja liiketoiminnan tarpeeseen, ja tiedot säilyvät luettavina koko ajan.

Todentava näyttö: säilytysaikataulu, arkistointiohje, tiedostomuotovaatimukset, arkisto-otos.

9. [KRIITTINEN] Hävitetäänkö vanhentuneet dokumentit ja tallenteet turvallisesti?

Hyväksymiskriteeri: Hävittäminen on valtuutettua, tietojen luokituksen mukaista, tarvittaessa keskeytettävissä ja todennettavissa.

Todentava näyttö: hävityslokit, poistotodistukset, oikeudellinen säilytyskielto, hyväksynnät.

10. Katselmoidaanko dokumenttien ajantasaisuus ja hallintaprosessin toimivuus?

Hyväksymiskriteeri: Vanhentuneet, puuttuvat ja käyttämättömät dokumentit tunnistetaan ja korjaavat toimet seurataan.

Todentava näyttö: katselmointiraportit, vanhenemishälytykset, auditointihavainnot, toimenpiderekisteri.

SISÄISET AUDITOINNIT

Auditoinnin tavoite

Selvittää, suunnitteleeko ja toteuttaako yritys sisäiset auditoinnit riippumattomasti, riskiperusteisesti ja tavalla, joka tukee jatkuvaa parantamista.

1. Onko yrityksellä hyväksytty sisäisen auditoinnin toimintamalli?

Hyväksymiskriteeri: Toimintamalli määrittelee tarkoituksen, toimivallan, riippumattomuuden, suunnittelun, toteutuksen ja raportoinnin.

Todentava näyttö: auditointipolitiikka, auditointiohje, hyväksymispäätös, toimintasääntö.

2. Laaditaanko riskiperusteinen monivuotinen tai vuosittainen auditointiohjelma?

Hyväksymiskriteeri: Ohjelma kattaa yrityksen merkittävät riskit, prosessit, velvoitteet ja aiemmat havainnot.

Todentava näyttö: auditointiohjelma, riskiperustelut, johdon hyväksyntä, kattavuusanalyysi.

3. Määritelläänkö jokaiselle auditoinnille tavoite, laajuus, kriteerit ja aikataulu?

Hyväksymiskriteeri: Toimeksianto on kirjallinen ja osapuolten tiedossa ennen auditoinnin aloittamista.

Todentava näyttö: auditointisuunnitelma, toimeksianto, kokouskutsu, kriteeriluettelo.

4. Ovatko auditoijat päteviä ja riittävän riippumattomia arvioitavasta toiminnasta?

Hyväksymiskriteeri: Pätevyys, kokemus, esteettömyys ja mahdolliset eturistiriidat arvioidaan ja dokumentoidaan.

Todentava näyttö: pätevyysrekisteri, koulutustodistukset, esteellisyysilmoitukset, nimeämispäätökset.

5. Perustuvatko auditointihavainnot riittävään ja todennettavaan näyttöön?

Hyväksymiskriteeri: Näyttö koostuu asiakirjoista, järjestelmätiedoista, havainnoista, haastatteluista ja tarkoituksenmukaisesta otannasta.

Todentava näyttö: auditointimuistiinpanot, otantalista, liitteet, haastattelut.

6. Luokitellaanko havainnot yhdenmukaisilla kriteereillä?

Hyväksymiskriteeri: Poikkeamien, huomioiden ja kehitysehdotusten merkitys, näyttö ja vaatimusperuste kirjataan selkeästi.

Todentava näyttö: luokitteluohje, havaintorekisteri, raporttiotos, laadunvarmistus.

7. [KRIITTINEN] Raportoidaanko merkittävät ja kriittiset havainnot viipymättä oikealle johdolle?

Hyväksymiskriteeri: Vakavat puutteet eskaloidaan ennen loppuraporttia, jos ne edellyttävät välittömiä toimia.

Todentava näyttö: eskalointiohje, ilmoitukset, johtoryhmän pöytäkirjat, välittömät toimet.

8. Hyväksytäänkö auditointiraportti ja toimitetaanko se sovituille vastaanottajille?

Hyväksymiskriteeri: Raportti on selkeä, tasapuolinen, näyttöön perustuva ja julkaistu sovitussa määräajassa.

Todentava näyttö: auditointiraportti, hyväksymismerkintä, jakelulista, julkaisuloki.

9. [KRIITTINEN] Seurataanko korjaavien toimenpiteiden toteutumista ja vaikuttavuutta?

Hyväksymiskriteeri: Havainnoilla on omistaja, määräaika ja sulkemiskriteeri, ja sulkeminen perustuu todennettuun näyttöön.

Todentava näyttö: toimenpiderekisteri, seurantakokoukset, sulkemisnäyttö, uusinta-auditointi.

10. Arvioidaanko sisäisen auditoinnin toimivuutta ja kattavuutta?

Hyväksymiskriteeri: Yritys seuraa suunnitelman toteutumista, havaintojen laatua, asiakaspalautetta ja auditoinnin tuottamaa hyötyä.

Todentava näyttö: auditointimittarit, palautekyselyt, laadunarvioinnit, kehityssuunnitelma.

JOHDON KATSELMUKSET

Auditoinnin tavoite

Selvittää, arvioiko yrityksen johto säännöllisesti johtamisjärjestelmien, riskien, turvallisuuden, laadun ja jatkuvuuden tilaa sekä tekee tarvittavat päätökset.

1. Onko yrityksellä hyväksytty menettely johdon katselmusten toteuttamiseen?

Hyväksymiskriteeri: Menettely määrittelee tiheyden, osallistujat, lähtötiedot, päätökset, pöytäkirjat ja seurannan.

Todentava näyttö: katselmusohje, vuosikello, hyväksymispäätös, kokouspohjat.

2. Pidetäänkö johdon katselmukset suunnitelluin väliajoin?

Hyväksymiskriteeri: Katselmukset toteutuvat vähintään määritellyllä tiheydellä ja olennaisten muutosten tai kriisien jälkeen tarvittaessa.

Todentava näyttö: kokouskalenteri, pöytäkirjat, osallistujaluettelot, vuosikello.

3. Osallistuvatko katselmukseen päätösvaltaiset ja aiheiden kannalta oikeat henkilöt?

Hyväksymiskriteeri: Johto, prosessinomistajat ja tarvittavat asiantuntijat ovat edustettuina ja sijaisjärjestelyt toimivat.

Todentava näyttö: osallistujaluettelo, roolikuvaukset, kutsut, pöytäkirjat.

4. Saako johto riittävät ja luotettavat lähtötiedot ennen katselmusta?

Hyväksymiskriteeri: Aineisto kattaa tavoitteet, mittarit, riskit, auditoinnit, poikkeamat, asiakkaat, vaatimukset, resurssit ja muutokset.

Todentava näyttö: katselmusaineisto, mittariraportit, riskiraportit, auditointiyhteenvedot.

5. Arvioidaanko tavoitteiden saavuttaminen ja prosessien suorituskyky?

Hyväksymiskriteeri: Poikkeamat tavoitearvoista, trendit, syyt ja vaikutukset käsitellään päätöksenteon pohjaksi.

Todentava näyttö: tavoiteraportit, trendikaaviot, poikkeama-analyysit, pöytäkirjat.

6. [KRIITTINEN] Käsitelläänkö merkittävät riskit, poikkeamat ja vaatimustenvastaisuudet?

Hyväksymiskriteeri: Johto arvioi vaikutukset, hyväksyy välittömät ja pitkäaikaiset toimet sekä tarvittaessa riskin.

Todentava näyttö: riskiraportti, poikkeamayhteenveto, päätökset, riskihyväksynnät.

7. Arvioidaanko resurssien, osaamisen ja teknologian riittävyys?

Hyväksymiskriteeri: Johto käsittelee henkilöstön, budjetin, kapasiteetin, työkalujen ja toimittajien kyvykkyyden suhteessa tavoitteisiin.

Todentava näyttö: resurssiraportit, budjetti, kapasiteettianalyysi, osaamiskartoitus.

8. Tehdäänkö katselmuksessa selkeät päätökset ja nimetäänkö toimenpiteille vastuuhenkilöt?

Hyväksymiskriteeri: Päätöksestä ilmenevät tehtävä, omistaja, määräaika, resurssi ja tavoiteltu tulos.

Todentava näyttö: päätöspöytäkirja, toimenpidelista, vastuutus, määräajat.

9. [KRIITTINEN] Seurataanko johdon päätösten toteutumista?

Hyväksymiskriteeri: Avoimet toimet käsitellään seuraavissa kokouksissa ja viivästykset eskaloidaan.

Todentava näyttö: päätösseuranta, tilaraportit, muistutukset, sulkemismerkinnät.

10. Säilytetäänkö katselmusten aineisto ja päätökset jäljitettävästi?

Hyväksymiskriteeri: Pöytäkirjat, liitteet, hyväksynnät ja päätöshistoria säilytetään suojatusti määritellyn ajan.

Todentava näyttö: pöytäkirja-arkisto, käyttöoikeudet, versionhallinta, säilytysaikataulu.

MITTAAMINEN JA RAPORTOINTI

Auditoinnin tavoite

Selvittää, tuottaako yritys luotettavaa ja tarkoituksenmukaista tietoa prosessien suorituskyvystä, riskeistä, turvallisuudesta ja kehityksestä päätöksenteon tueksi.

1. Onko yrityksellä hyväksytty mittaamisen ja raportoinnin toimintamalli?

Hyväksymiskriteeri: Malli määrittelee tavoitteet, vastuut, tietolähteet, mittarit, raportointitiheyden, laadunvarmistuksen ja jakelun.

Todentava näyttö: mittauspolitiikka, raportointiohje, hyväksymispäätös, vastuumatriisi.

2. Johdetaanko mittarit yrityksen tavoitteista, riskeistä ja vaatimuksista?

Hyväksymiskriteeri: Jokaisella mittarilla on selkeä käyttötarkoitus ja yhteys päätökseen, tavoitteeseen tai kontrolliin.

Todentava näyttö: tavoitekartta, mittariluettelo, riskirekisteri, vaatimusmatriisi.

3. Onko jokaiselle mittarille määritelty omistaja, laskentatapa ja tietolähde?

Hyväksymiskriteeri: Määritelmä sisältää kaavan, rajaukset, lähdejärjestelmän, päivitystiheyden, tavoitearvon ja vastuut.

Todentava näyttö: mittarikortit, tietomallit, omistajaluettelo, laskentasäännöt.

4. Varmistetaanko mittaustiedon oikeellisuus, eheys ja ajantasaisuus?

Hyväksymiskriteeri: Tietolähteet ovat hyväksyttyjä, muutokset jäljitettäviä ja poikkeavat tai puuttuvat tiedot tarkistetaan.

Todentava näyttö: tietolähdeluettelo, täsmäytysraportit, laaduntarkastukset, muutoslokit.

5. Ovatko tavoite-, varoitus- ja kriittiset raja-arvot määritelty?

Hyväksymiskriteeri: Raja-arvot perustuvat liiketoiminnan tarpeeseen ja ohjaavat ennalta määriteltyjä toimenpiteitä.

Todentava näyttö: mittarikortit, tavoitepäätökset, hälytysrajat, eskalointiohje.

6. [KRIITTINEN] Reagoidaanko kriittisiin mittaripoikkeamiin oikea-aikaisesti?

Hyväksymiskriteeri: Poikkeama eskaloidaan, vaikutus arvioidaan, välittömät toimet tehdään ja omistaja nimetään.

Todentava näyttö: hälytykset, poikkeamaraportit, päätöslokit, toimenpideseuranta.

7. Raportoidaanko eri kohderyhmille tarkoituksenmukaisella tasolla?

Hyväksymiskriteeri: Johto saa tiiviin päätöksentekonäkymän ja asiantuntijat riittävän yksityiskohtaiset toiminta- ja analyysitiedot.

Todentava näyttö: johtoraportit, prosessiraportit, kojelaudat, jakelulistat.

8. Esitetäänkö raporteissa trendit, vertailut ja syyt pelkkien hetkellisten arvojen lisäksi?

Hyväksymiskriteeri: Raportointi mahdollistaa kehityksen, toistuvien ongelmien ja poikkeamien juurisyiden tunnistamisen.

Todentava näyttö: trendikaaviot, vertailuraportit, analyysit, kommentit.

9. Suojataanko raportit niiden sisältämän tiedon luokituksen mukaisesti?

Hyväksymiskriteeri: Pääsy, jakelu, säilytys ja mahdollinen anonymisointi on rajattu raportin luottamuksellisuuden perusteella.

Todentava näyttö: käyttöoikeudet, jakelulistat, luokitusmerkinnät, säilytysasetukset.

10. Katselmoidaanko mittareiden hyödyllisyys ja raportoinnin tehokkuus säännöllisesti?

Hyväksymiskriteeri: Tarpeettomat mittarit poistetaan, puutteita korjataan ja uusia mittareita lisätään muuttuvien tavoitteiden perusteella.

Todentava näyttö: mittarikatselmukset, käyttäjäpalaute, muutoshistoria, kehityspäätökset.