TIETOTURVAN JOHTAMINEN JA RISKIENHALLINTA

Auditoinnin tavoite

Selvittää, johdetaanko tietoturvallisuutta tavoitteellisesti, vastuutetusti ja riskiperusteisesti sekä huomioidaanko tietoturvariskit yrityksen päätöksenteossa.

1. Onko yrityksellä hyväksytty ja ajantasainen tietoturvapolitiikka?

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

Todentava näyttö: tietoturvapolitiikka, hyväksymispäätös, julkaisukanava, versionhallintatiedot.

2. Onko tietoturvallisuuden johtamiselle määritelty tavoitteet ja mittarit?

Hyväksymiskriteeri: Tietoturvatavoitteet ovat mitattavia, liiketoiminnan tavoitteisiin kytkettyjä ja niiden toteutumista seurataan säännöllisesti.

Todentava näyttö: tietoturvatavoitteet, mittariraportit, johtoryhmän pöytäkirjat, seurantakatselmukset.

3. Onko tietoturvallisuuden vastuut ja valtuudet määritelty?

Hyväksymiskriteeri: Tietoturvan omistajuus, päätöksentekovaltuudet, operatiiviset vastuut ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: vastuumatriisi, tehtävänkuvat, yrityskaavio, nimityspäätökset.

4. Tunnistetaanko ja arvioidaanko tietoturvariskit säännöllisesti?

Hyväksymiskriteeri: Riskiarvioinnit toteutetaan määritellyllä menetelmällä, kattavat olennaiset tiedot, järjestelmät, palvelut ja riippuvuudet sekä päivitetään muutosten yhteydessä.

Todentava näyttö: riskienhallintamenetelmä, riskiarviot, riskirekisteri, katselmuspöytäkirjat.

5. Onko tunnistetuille tietoturvariskeille määritelty käsittelytoimenpiteet?

Hyväksymiskriteeri: Jokaiselle merkittävälle riskille on määritelty omistaja, käsittelytapa, määräaika ja tavoiteltu jäännösriskin taso.

Todentava näyttö: riskien käsittelysuunnitelma, toimenpiderekisteri, vastuuhenkilömerkinnät, hyväksynnät.

6. Hyväksytäänkö jäännösriskit määriteltyjen valtuuksien mukaisesti?

Hyväksymiskriteeri: Riskin hyväksyminen perustuu dokumentoituun arvioon, ja hyväksyjän toimivalta vastaa riskin vakavuutta ja liiketoimintavaikutusta.

Todentava näyttö: riskin hyväksymispäätökset, valtuusmatriisi, riskirekisteri, johdon pöytäkirjat.

7. Huomioidaanko lakisääteiset, sopimukselliset ja viranomaisvaatimukset tietoturvan johtamisessa?

Hyväksymiskriteeri: Yritys tunnistaa sitä koskevat tietoturvavaatimukset, ylläpitää vaatimusrekisteriä ja seuraa vaatimusten täyttymistä.

Todentava näyttö: vaatimusrekisteri, sopimukset, lakiseuranta, vaatimustenmukaisuusarviot.

8. Raportoidaanko tietoturvallisuuden tila johdolle säännöllisesti?

Hyväksymiskriteeri: Raportointi kattaa riskit, poikkeamat, haavoittuvuudet, mittarit, kehitystoimet ja päätöstä edellyttävät asiat ennalta määritellyllä aikataululla.

Todentava näyttö: johdon tietoturvaraportit, johtoryhmän aineistot, kokouspöytäkirjat, mittarikoosteet.

9. Arvioidaanko tietoturvariskit merkittävien muutosten ja hankkeiden yhteydessä?

Hyväksymiskriteeri: Uusien järjestelmien, palvelujen, toimittajien ja merkittävien muutosten tietoturvariskit arvioidaan ennen hyväksyntää tai käyttöönottoa.

Todentava näyttö: muutos- ja hankearviot, tietoturvakatselmukset, hyväksyntäportit, riskianalyysit.

10. Katselmoidaanko tietoturvan johtamisjärjestelmän toimivuus ja kehitystarpeet?

Hyväksymiskriteeri: Johto arvioi säännöllisesti tietoturvan tavoitteiden, kontrollien, resurssien ja kehitystoimien riittävyyden ja päättää tarvittavista muutoksista.

Todentava näyttö: johdon katselmuspöytäkirjat, auditointitulokset, kehityssuunnitelmat, päätökset.

KÄYTTÖOIKEUKSIEN HALLINTA

Auditoinnin tavoite

Selvittää, myönnetäänkö, muutetaanko, valvotaanko ja poistetaanko käyttöoikeudet hallitusti sekä rajataanko pääsy tietoihin ja järjestelmiin työtehtävien mukaisesti.

1. Onko käyttöoikeuksien hallintaprosessi dokumentoitu ja hyväksytty?

Hyväksymiskriteeri: Käyttöoikeuksien pyytäminen, hyväksyminen, myöntäminen, muuttaminen, katselmointi ja poistaminen on kuvattu vastuineen ja määräaikoineen.

Todentava näyttö: käyttöoikeusprosessi, työohjeet, vastuumatriisi, hyväksymismenettely.

2. Perustuvatko käyttöoikeudet työtehtävään ja vähimmän oikeuden periaatteeseen?

Hyväksymiskriteeri: Käyttäjälle myönnetään vain tehtävän suorittamiseen tarvittavat oikeudet, ja roolit perustuvat hyväksyttyihin tehtävä- tai roolikuvauksiin.

Todentava näyttö: roolimatriisi, tehtävänkuvat, käyttöoikeuspyynnöt, järjestelmäroolit.

3. Hyväksytäänkö käyttöoikeudet ennen niiden myöntämistä?

Hyväksymiskriteeri: Käyttöoikeuden hyväksyy tiedon, järjestelmän tai palvelun valtuutettu omistaja ennen teknistä toteutusta.

Todentava näyttö: käyttöoikeuspyynnöt, hyväksymismerkinnät, työnkulut, järjestelmälokit.

4. Ovatko käyttäjätunnukset henkilökohtaisia ja yksilöitävissä?

Hyväksymiskriteeri: Henkilökohtainen toiminta voidaan yhdistää yksittäiseen käyttäjään eikä yhteiskäyttöisiä tunnuksia käytetä ilman dokumentoitua perustetta ja lisäkontrolleja.

Todentava näyttö: käyttäjäluettelot, tunnuskäytännöt, poikkeusluvat, lokitiedot.

5. Hallitaanko pääkäyttäjä- ja muut korotetut käyttöoikeudet tehostetusti?

Hyväksymiskriteeri: Korotetut oikeudet ovat erillisiä, henkilökohtaisia, määräaikaisia tai tehtävään rajattuja, hyväksyttyjä ja valvottuja.

Todentava näyttö: pääkäyttäjäluettelo, PAM-järjestelmän tiedot, hyväksynnät, valvontalokit.

6. Poistetaanko käyttöoikeudet viipymättä työsuhteen tai tehtävän päättyessä?

Hyväksymiskriteeri: Poistumis- ja tehtävämuutosprosessi käynnistää oikeuksien poistamisen tai muuttamisen määritellyssä määräajassa kaikista olennaisista järjestelmistä.

Todentava näyttö: HR-ilmoitukset, poistumislistat, tunnusten sulkemislokit, tapausotos.

7. Katselmoidaanko käyttöoikeudet säännöllisesti?

Hyväksymiskriteeri: Järjestelmien ja tietojen omistajat tarkastavat käyttäjät, roolit ja korotetut oikeudet riskiperusteisin väliajoin ja poistavat tarpeettomat oikeudet.

Todentava näyttö: käyttöoikeuskatselmukset, hyväksyntäraportit, poistotoimenpiteet, poikkeamalistat.

8. Onko tehtävien eriyttäminen huomioitu käyttöoikeuksissa?

Hyväksymiskriteeri: Keskenään ristiriitaiset oikeudet on tunnistettu ja estetty tai niiden käyttöä valvotaan dokumentoiduilla korvaavilla kontrolleilla.

Todentava näyttö: SoD-matriisi, roolianalyysit, poikkeushyväksynnät, valvontaraportit.

9. Käytetäänkö vahvaa tunnistautumista riskialttiissa käyttötilanteissa?

Hyväksymiskriteeri: Monivaiheinen tunnistautuminen on käytössä etäyhteyksissä, ylläpitotunnuksilla, pilvipalveluissa ja muissa riskinarvioinnin edellyttämissä kohteissa.

Todentava näyttö: tunnistautumisasetukset, järjestelmäkonfiguraatiot, kirjautumislokit, tekniset testit.

10. Valvotaanko käyttöoikeuksien väärinkäyttöä ja poikkeavaa käyttöä?

Hyväksymiskriteeri: Epäonnistuneita kirjautumisia, epätavallisia käyttöaikoja, oikeuksien muutoksia ja korotettujen oikeuksien käyttöä seurataan ja poikkeamat tutkitaan.

Todentava näyttö: valvontasäännöt, hälytykset, lokiraportit, tutkintatapaukset.

TIETOJEN LUOKITTELU JA TURVALLINEN KÄSITTELY

Auditoinnin tavoite

Selvittää, tunnistetaanko tietojen suojaustarve ja käsitelläänkö, säilytetäänkö, siirretäänkö ja hävitetäänkö tiedot niiden luokituksen ja riskien mukaisesti.

1. Onko yrityksellä hyväksytty tietojen luokittelumalli?

Hyväksymiskriteeri: Luokittelutasot, niiden määräytymisperusteet ja kuhunkin tasoon liittyvät käsittelyvaatimukset on dokumentoitu ja hyväksytty.

Todentava näyttö: tiedonluokitteluohje, tietoturvapolitiikka, hyväksymispäätös, luokittelutaulukko.

2. Onko keskeisille tiedoille ja tietoaineistoille nimetty omistajat?

Hyväksymiskriteeri: Tietojen omistajat vastaavat luokittelusta, käyttöoikeuksista, säilytysajoista ja suojausvaatimuksista.

Todentava näyttö: tieto-omaisuusrekisteri, omistajaluettelo, vastuumatriisi, tehtävänkuvat.

3. Luokitellaanko tiedot niiden luottamuksellisuuden, eheyden ja saatavuuden perusteella?

Hyväksymiskriteeri: Luokittelu perustuu dokumentoituun vaikutusarvioon ja kattaa liiketoiminnan, henkilötietojen, sopimusten ja lakisääteisten velvoitteiden tarpeet.

Todentava näyttö: luokittelupäätökset, vaikutusarviot, tietoaineistoluettelo, käsittelyselosteet.

4. Merkitäänkö luokitellut tiedot yhdenmukaisesti?

Hyväksymiskriteeri: Asiakirjoissa, sähköposteissa, tallennuspaikoissa tai metatiedoissa käytetään sovittuja luokittelumerkintöjä, kun se on teknisesti ja toiminnallisesti mahdollista.

Todentava näyttö: asiakirjaotos, sähköpostimallit, metatiedot, luokittelutyökalun asetukset.

5. Säilytetäänkö tiedot vain hyväksytyissä tallennuspaikoissa?

Hyväksymiskriteeri: Tietojen luokitus määrittää sallitut järjestelmät, pilvipalvelut, päätelaitteet ja fyysiset säilytyspaikat.

Todentava näyttö: käsittelyohjeet, hyväksyttyjen palvelujen luettelo, järjestelmäasetukset, havainto-otos.

6. Suojataanko luottamukselliset tiedot siirron aikana?

Hyväksymiskriteeri: Luottamuksellisten tietojen sähköinen ja fyysinen siirto käyttää riskitason mukaisia salaus-, tunnistus-, pakkaus- ja luovutusmenettelyjä.

Todentava näyttö: salausasetukset, siirto-ohjeet, tiedostonsiirtopalvelun lokit, lähetysasiakirjat.

7. Rajoitetaanko tietojen kopiointia, tulostamista ja jakamista?

Hyväksymiskriteeri: Luokiteltujen tietojen kopiointi, tulostus, edelleenlähetys ja ulkoinen jakaminen on rajattu tarpeen mukaisesti ja tarvittaessa hyväksynnänvaraista.

Todentava näyttö: DLP-säännöt, tulostusasetukset, jakolinkkien asetukset, hyväksyntätiedot.

8. Noudatetaanko tiedoille määriteltyjä säilytysaikoja?

Hyväksymiskriteeri: Säilytysajat perustuvat liiketoiminta-, sopimus- ja lakivaatimuksiin, ja vanhentuneet tiedot poistetaan hallitusti.

Todentava näyttö: tiedonohjaussuunnitelma, säilytysaikataulu, poistopolitiikka, poistologit.

9. Hävitetäänkö tiedot ja tietovälineet turvallisesti?

Hyväksymiskriteeri: Tietojen ja välineiden hävitys estää tietojen palauttamisen luokituksen edellyttämällä tasolla ja hävitys voidaan tarvittaessa todentaa.

Todentava näyttö: hävitysohje, hävitystodistukset, tietovälinerekisteri, palveluntarjoajan raportit.

10. Seurataanko luokittelu- ja käsittelyvaatimusten noudattamista?

Hyväksymiskriteeri: Yritys tarkastaa säännöllisesti tiedon tallennuspaikkoja, jakamista, merkintöjä ja säilytysaikoja sekä korjaa havaitut poikkeamat.

Todentava näyttö: tarkastusraportit, DLP-hälytykset, auditointihavainnot, korjaavat toimenpiteet.

TEKNINEN SUOJAAMINEN

Auditoinnin tavoite

Selvittää, onko tietojärjestelmät, verkot, päätelaitteet ja palvelut suojattu tarkoituksenmukaisilla teknisillä kontrolleilla ja turvallisilla asetuksilla.

1. Onko teknisille tietoturvakontrolleille määritelty hyväksytty suojausarkkitehtuuri?

Hyväksymiskriteeri: Suojausarkkitehtuuri kuvaa keskeiset suojauskerrokset, verkkoalueet, luottamusrajat, kontrollit ja vastuut sekä vastaa tunnistettuja riskejä.

Todentava näyttö: tietoturva-arkkitehtuuri, verkkokaaviot, kontrollikuvaukset, hyväksymispäätökset.

2. Onko järjestelmille ja laitteille määritelty turvalliset perusasetukset?

Hyväksymiskriteeri: Käyttöjärjestelmien, palvelimien, verkkolaitteiden, pilvipalvelujen ja päätelaitteiden kovennusvaatimukset on dokumentoitu ja versioitu.

Todentava näyttö: kovennusstandardit, konfiguraatiomallit, MDM-asetukset, tekniset tarkastusraportit.

3. Onko verkot segmentoitu riskien ja käyttötarkoitusten mukaisesti?

Hyväksymiskriteeri: Kriittiset järjestelmät, käyttäjäverkot, vierasverkot, tuotantoympäristöt ja hallintaliikenne on eroteltu ja liikennettä rajoitetaan.

Todentava näyttö: verkkokaaviot, palomuurisäännöt, segmentointitestit, konfiguraatio-otokset.

4. Hallitaanko palomuuri- ja verkkoliikennesääntöjä hyväksytyllä menettelyllä?

Hyväksymiskriteeri: Sääntömuutokset perustuvat tarpeeseen, ne hyväksytään, testataan, dokumentoidaan ja vanhentuneet säännöt poistetaan säännöllisesti.

Todentava näyttö: muutospyynnöt, palomuurisääntöjen katselmukset, hyväksynnät, konfiguraatiolokit.

5. Suojataanko päätelaitteet haittaohjelmilta ja luvattomalta käytöltä?

Hyväksymiskriteeri: Päätelaitteissa on keskitetysti hallitut haittaohjelmasuojaukset, levynsalaus, näytön lukitus ja muut riskin mukaiset suojausasetukset.

Todentava näyttö: EDR- tai virustorjuntaraportit, MDM-raportit, salausasetukset, laiteotos.

6. Onko kriittinen tieto salattu tallennettuna?

Hyväksymiskriteeri: Luottamukselliset tiedot, varmuuskopiot, kannettavat laitteet ja muut riskialttiit tallennuskohteet salataan hyväksytyillä menetelmillä.

Todentava näyttö: salauspolitiikka, avainhallinnan tiedot, järjestelmäasetukset, tekniset testit.

7. Hallitaanko salausavaimet ja varmenteet turvallisesti?

Hyväksymiskriteeri: Avainten ja varmenteiden luonti, säilytys, käyttö, uusiminen, varmistaminen ja mitätöinti on vastuutettu ja suojattu.

Todentava näyttö: avainhallintaohje, varmennerekisteri, HSM- tai avainholvin lokit, uusimisaikataulut.

8. Rajoitetaanko ulkoisten laitteiden ja siirrettävien tietovälineiden käyttöä?

Hyväksymiskriteeri: USB-laitteiden, ulkoisten levyjen ja muiden siirrettävien välineiden käyttö on estetty tai rajattu hyväksyttyihin, salattuihin ja valvottuihin käyttötapauksiin.

Todentava näyttö: laitehallinta-asetukset, poikkeusluvat, lokit, tekniset testit.

9. Testataanko teknisten suojausten toimivuus säännöllisesti?

Hyväksymiskriteeri: Palomuurit, pääsynhallinta, haittaohjelmasuojaus, salaus ja muut keskeiset kontrollit testataan riskiperusteisesti ja puutteet korjataan.

Todentava näyttö: penetraatiotestit, kontrollitestit, tekniset auditoinnit, korjaussuunnitelmat.

10. Valvotaanko turvallisten asetusten säilymistä muutosten aikana?

Hyväksymiskriteeri: Konfiguraatiopoikkeamia havaitaan keskitetysti, luvattomat muutokset estetään tai hälytetään ja hyväksytyt perustasot palautetaan tarvittaessa.

Todentava näyttö: konfiguraationhallintaraportit, poikkeamahälytykset, muutospyynnöt, korjauslokit.

PÄIVITYS- JA HAAVOITTUVUUDENHALLINTA

Auditoinnin tavoite

Selvittää, tunnistetaanko järjestelmien ja palvelujen haavoittuvuudet, arvioidaanko niiden riskit ja toteutetaanko korjaukset hallitusti määritellyissä määräajoissa.

1. Onko päivitys- ja haavoittuvuudenhallintaprosessi dokumentoitu?

Hyväksymiskriteeri: Prosessi kattaa tietolähteet, skannaukset, riskiluokituksen, korjausajat, testauksen, poikkeukset, seurannan ja raportoinnin.

Todentava näyttö: prosessikuvaus, päivitysohje, haavoittuvuudenhallintaohje, vastuumatriisi.

2. Onko yrityksellä ajantasainen luettelo päivitettävistä laitteista, järjestelmistä ja ohjelmistoista?

Hyväksymiskriteeri: Omaisuus- ja ohjelmistoluettelot sisältävät omistajan, version, kriittisyyden, sijainnin ja tuen päättymistiedot.

Todentava näyttö: laite- ja ohjelmistorekisteri, CMDB, lisenssihallinnan raportit, inventaariot.

3. Seurataanko käytössä oleviin teknologioihin liittyviä haavoittuvuustiedotteita?

Hyväksymiskriteeri: Vastuuhenkilöt seuraavat valmistajien, viranomaisten ja luotettujen tietolähteiden ilmoituksia ja arvioivat niiden merkityksen viipymättä.

Todentava näyttö: tiedoteseuranta, tilaukset, uhkatiedusteluraportit, arviointimerkinnät.

4. Skannataanko järjestelmät haavoittuvuuksien varalta säännöllisesti?

Hyväksymiskriteeri: Sisäiset ja ulkoiset kohteet, pilviympäristöt ja sovellukset skannataan riskiperusteisin väliajoin sekä merkittävien muutosten jälkeen.

Todentava näyttö: skannaussuunnitelma, skannausraportit, kohdeluettelo, ajastustiedot.

5. Luokitellaanko haavoittuvuudet riskin ja liiketoimintavaikutuksen perusteella?

Hyväksymiskriteeri: Priorisointi huomioi teknisen vakavuuden, hyväksikäytettävyyden, altistumisen, kohteen kriittisyyden ja käytössä olevat suojaavat kontrollit.

Todentava näyttö: riskiluokittelumalli, haavoittuvuusraportit, uhkatiedot, priorisointipäätökset

.

6. Onko haavoittuvuuksille ja tietoturvapäivityksille määritelty korjausajat?

Hyväksymiskriteeri: Korjausajat on määritelty riskiluokittain, niiden toteutumista seurataan ja määräajan ylitykset eskaloidaan.

Todentava näyttö: palvelutasot, korjausaikataulut, mittariraportit, eskalointitiedot.

7. Testataanko päivitykset ennen tuotantoon asentamista?

Hyväksymiskriteeri: Päivitysten toimivuus, yhteensopivuus ja turvallisuusvaikutukset testataan riskiperusteisesti ja tarvittaessa määritellään palautusmenettely.

Todentava näyttö: testisuunnitelmat, testitulokset, muutospyynnöt, palautussuunnitelmat.

8. Varmistetaanko päivitysten onnistunut asentuminen?

Hyväksymiskriteeri: Asennusten kattavuus ja onnistuminen todennetaan keskitetystä hallinnasta tai teknisellä tarkastuksella, ja epäonnistuneet asennukset käsitellään.

Todentava näyttö: päivityshallinnan raportit, asennuslokit, poikkeamalistat, korjaustiketit.

9. Hallitaanko korjaamatta jätetyt haavoittuvuudet hyväksytyllä poikkeusmenettelyllä?

Hyväksymiskriteeri: Poikkeukselle on dokumentoitu peruste, riskinarvio, korvaavat kontrollit, omistaja, hyväksyntä ja määräaikainen uudelleenarviointi.

Todentava näyttö: poikkeusrekisteri, riskihyväksynnät, kompensoivien kontrollien kuvaukset, katselmukset.

10. Poistetaanko käytöstä tuen ulkopuolelle jääneet järjestelmät ja ohjelmistot?

Hyväksymiskriteeri: Elinkaaren päättymistä seurataan, korvaussuunnitelmat laaditaan ajoissa ja tukemattomien ratkaisujen käyttö on poikkeuksellista ja riskihyväksyttyä.

Todentava näyttö: elinkaariraportit, poistumissuunnitelmat, projektisuunnitelmat, poikkeusluvat.

LOKIENHALLINTA JA TIETOTURVAVALVONTA

Auditoinnin tavoite

Selvittää, kerätäänkö, suojataanko ja analysoidaanko tietoturvan kannalta olennaisia tapahtumatietoja siten, että poikkeamat voidaan havaita ja tapahtumat jäljittää.

1. Onko lokienhallinnalle ja tietoturvavalvonnalle määritelty hyväksytty toimintamalli?

Hyväksymiskriteeri: Toimintamalli määrittelee lokilähteet, vastuut, valvonta-ajat, hälytykset, käsittelymenettelyt, säilytysajat ja eskaloinnin.

Todentava näyttö: lokienhallintapolitiikka, valvontaprosessi, vastuumatriisi, palvelukuvaus.

2. Onko tietoturvan kannalta olennaiset lokilähteet tunnistettu?

Hyväksymiskriteeri: Lokitus kattaa vähintään tunnistautumisen, käyttöoikeusmuutokset, ylläpitotoimet, kriittiset järjestelmät, verkkolaitteet ja tietoturvaratkaisut.

Todentava näyttö: lokilähdeluettelo, järjestelmäarkkitehtuuri, SIEM-integraatiot, lokikattavuusraportti.

3. Sisältävätkö lokit riittävät tiedot tapahtumien jäljittämiseksi?

Hyväksymiskriteeri: Lokimerkinnöistä käyvät ilmi vähintään tapahtuma, ajankohta, käyttäjä tai laite, kohde, lähde ja tulos riskin edellyttämällä tarkkuudella.

Todentava näyttö: lokinäytteet, lokitusvaatimukset, järjestelmäasetukset, tekniset testit.

4. Onko järjestelmien kellonaika synkronoitu luotettavaan aikalähteeseen?

Hyväksymiskriteeri: Keskeiset järjestelmät käyttävät hyväksyttyä aikapalvelua ja merkittävät aikaerot havaitaan sekä korjataan.

Todentava näyttö: NTP-asetukset, aikapalvelun lokit, konfiguraatio-otokset, valvontahälytykset.

5. Suojataanko lokit luvattomalta muuttamiselta ja poistamiselta?

Hyväksymiskriteeri: Lokien käyttöoikeudet on rajattu, lokit siirretään tarvittaessa keskitettyyn ympäristöön ja eheys sekä säilyminen varmistetaan.

Todentava näyttö: käyttöoikeusluettelot, SIEM-asetukset, muuttumattoman tallennuksen asetukset, auditointilokit.

6. Noudatetaanko lokeille määriteltyjä säilytysaikoja?

Hyväksymiskriteeri: Lokien säilytysajat perustuvat riskeihin, tutkintatarpeisiin, sopimuksiin ja lainsäädäntöön, ja toteutuminen on teknisesti varmistettu.

Todentava näyttö: säilytyspolitiikka, järjestelmäasetukset, kapasiteettiraportit, poistologit.

7. Onko keskeisille tietoturvatapahtumille määritelty valvonta- ja hälytyssäännöt?

Hyväksymiskriteeri: Hälytykset kattavat esimerkiksi luvattomat kirjautumisyritykset, haittaohjelmahavainnot, oikeuksien muutokset ja poikkeavan tietoliikenteen.

Todentava näyttö: SIEM-säännöt, käyttötapausluettelo, hälytysasetukset, testitulokset.

8. Käsitelläänkö tietoturvahälytykset määriteltyjen prioriteettien ja vasteaikojen mukaisesti?

Hyväksymiskriteeri: Hälytykset luokitellaan, osoitetaan vastuuhenkilölle, tutkitaan, dokumentoidaan ja eskaloidaan riskin mukaisessa ajassa.

Todentava näyttö: hälytystiketit, palvelutasoraportit, tutkintamuistiot, eskalointilokit.

9. Testataanko valvontasääntöjen ja hälytysten toimivuus säännöllisesti?

Hyväksymiskriteeri: Hälytysten syntyminen, välittyminen, käsittely ja eskalointi testataan suunnitellusti sekä muutosten jälkeen.

Todentava näyttö: testisuunnitelmat, simulaatiot, testihälytykset, korjaavat toimenpiteet.

10. Arvioidaanko valvonnan kattavuutta ja tehokkuutta säännöllisesti?

Hyväksymiskriteeri: Katvealueet, käsittelemättömät hälytykset, väärät positiiviset havainnot ja tutkintojen tulokset analysoidaan ja valvontaa kehitetään.

Todentava näyttö: kattavuusraportit, hälytysstatistiikka, kehitysjono, katselmuspöytäkirjat.

TIETOTURVAPOIKKEAMIEN HALLINTA

Auditoinnin tavoite

Selvittää, tunnistetaanko, ilmoitetaanko, rajataanko, tutkitaanko ja korjataanko tietoturvapoikkeamat hallitusti sekä opitaanko tapahtumista.

1. Onko tietoturvapoikkeamien hallintaprosessi dokumentoitu ja hyväksytty?

Hyväksymiskriteeri: Prosessi kuvaa ilmoittamisen, vastaanoton, luokittelun, eskaloinnin, rajaamisen, tutkinnan, palautumisen ja jälkiarvioinnin.

Todentava näyttö: poikkeamaprosessi, toimintaohjeet, vastuumatriisi, hyväksymispäätös.

2. Onko henkilöstölle ja sidosryhmille määritelty selkeät ilmoituskanavat?

Hyväksymiskriteeri: Tietoturvahavainnoista voi ilmoittaa helposti, kanavat ovat tiedossa ja ilmoituksia vastaanotetaan tarvittaessa myös normaalin työajan ulkopuolella.

Todentava näyttö: ilmoitusohje, intranet-sivu, palvelukanavat, koulutusmateriaali.

3. Luokitellaanko poikkeamat vakavuuden ja vaikutuksen perusteella?

Hyväksymiskriteeri: Luokittelu huomioi tiedon luottamuksellisuuden, eheyden, saatavuuden, laajuuden, liiketoimintavaikutuksen ja mahdolliset lakivelvoitteet.

Todentava näyttö: luokittelumalli, tapausotokset, vaikutusarviot, prioriteettimerkinnät.

4. Onko vakaville poikkeamille määritelty nopeutettu eskalointi ja päätöksenteko?

Hyväksymiskriteeri: Vakavien tapausten vastuuhenkilöt, yhteystiedot, päätösvaltuudet ja johtamisen käytännöt ovat ajantasaisia ja nopeasti käytettävissä.

Todentava näyttö: vakavan poikkeaman ohje, päivystyslista, kriisiryhmän tiedot, tapausraportit.

5. Rajataanko tietoturvapoikkeamat viipymättä lisävahinkojen estämiseksi?

Hyväksymiskriteeri: Rajaamistoimet perustuvat hyväksyttyihin toimintamalleihin, ne dokumentoidaan ja niiden vaikutukset liiketoimintaan arvioidaan.

Todentava näyttö: toimintakortit, tapauslokit, eristämistoimet, päätösmerkinnät.

6. Säilytetäänkö tutkinnassa tarvittava todistusaineisto asianmukaisesti?

Hyväksymiskriteeri: Lokit, laitekuvat, viestit ja muut todisteet kerätään, suojataan ja käsitellään siten, että niiden eheys, alkuperä ja käsittelyketju voidaan osoittaa.

Todentava näyttö: todisteiden käsittelyohje, chain of custody -lomakkeet, lokikopiot, tutkintaraportit.

7. Arvioidaanko poikkeamiin liittyvät ilmoitusvelvollisuudet?

Hyväksymiskriteeri: Tietosuoja-, viranomais-, asiakas-, vakuutus- ja sopimusperusteiset ilmoitusvelvollisuudet arvioidaan määräajoissa ja päätökset dokumentoidaan.

Todentava näyttö: ilmoitusarviot, viranomaisilmoitukset, asiakasviestit, päätöspöytäkirjat.

8. Viestitäänkö poikkeamista hallitusti sisäisille ja ulkoisille sidosryhmille?

Hyväksymiskriteeri: Viestinnän vastuut, hyväksynnät, kohderyhmät ja viestipohjat on määritelty, ja julkaistut tiedot ovat oikeita ja yhdenmukaisia.

Todentava näyttö: viestintäsuunnitelma, tiedotteet, hyväksyntämerkinnät, sidosryhmälistat.

9. Tehdäänkö merkittävistä poikkeamista juurisyyanalyysi?

Hyväksymiskriteeri: Analyysi tunnistaa tekniset, organisatoriset ja inhimilliset perussyyt sekä määrittelee korjaavat ja ehkäisevät toimenpiteet.

Todentava näyttö: juurisyyanalyysit, tutkintaraportit, toimenpiderekisteri, vastuuhenkilömerkinnät.

10. Harjoitellaanko tietoturvapoikkeamien hallintaa säännöllisesti?

Hyväksymiskriteeri: Harjoitukset kattavat relevantteja skenaarioita, vastuut ja päätöksenteon, ja havainnot johtavat dokumentoituihin parannuksiin.

Todentava näyttö: harjoitussuunnitelmat, osallistujaluettelot, harjoitusraportit, kehitystoimet.

VARMUUSKOPIOINTI JA PALAUTUMINEN

Auditoinnin tavoite

Selvittää, varmistetaanko kriittiset tiedot ja järjestelmät suunnitellusti sekä voidaanko ne palauttaa eheästi ja tavoiteajassa häiriö- tai vahinkotilanteessa.

1. Onko yrityksellä hyväksytty varmuuskopiointi- ja palautuspolitiikka?

Hyväksymiskriteeri: Politiikka määrittelee vastuut, varmistettavat kohteet, varmistustiheydet, säilytysajat, suojaustavat ja palautustestauksen.

Todentava näyttö: varmuuskopiointipolitiikka, tekniset ohjeet, hyväksymispäätös, vastuumatriisi.

2. Onko varmistettavat tiedot ja järjestelmät tunnistettu liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Varmuuskopioinnin kattavuus perustuu järjestelmien ja tietojen kriittisyyteen, palautuspistetavoitteisiin ja riippuvuuksiin.

Todentava näyttö: järjestelmäluettelo, kriittisyysluokitus, RPO-määrittelyt, varmistuskohdeluettelo.

3. Toteutetaanko varmuuskopiot määriteltyjen aikataulujen mukaisesti?

Hyväksymiskriteeri: Automaattisten ja manuaalisten varmistusten toteutumista valvotaan ja epäonnistumiset käsitellään määritellyssä ajassa.

Todentava näyttö: varmistusajot, valvontaraportit, virhelokit, korjaustiketit.

4. Säilytetäänkö varmuuskopioita erillään tuotantoympäristöstä?

Hyväksymiskriteeri: Vähintään yksi palautuskelpoinen kopio on suojattu tuotantoympäristön häiriöiltä, ylläpitotunnusten väärinkäytöltä ja kiristyshaittaohjelmilta.

Todentava näyttö: varmistusarkkitehtuuri, eriytysasetukset, offline- tai immutable-kopioiden tiedot, tekniset testit.

5. Suojataanko varmuuskopiot luvattomalta käytöltä ja muuttamiselta?

Hyväksymiskriteeri: Varmuuskopioiden käyttöoikeudet on rajattu, tiedot salataan tarpeen mukaan ja poistaminen tai muuttaminen on valvottua.

Todentava näyttö: käyttöoikeusluettelo, salausasetukset, hallintalokit, pääkäyttäjäraportit.

6. Noudatetaanko varmuuskopioille määriteltyjä säilytysaikoja?

Hyväksymiskriteeri: Päivittäiset, viikoittaiset, kuukausittaiset ja pitkäaikaiset kopiot säilytetään hyväksytyn aikataulun mukaisesti ja poistetaan hallitusti.

Todentava näyttö: säilytysaikataulu, varmistusjärjestelmän asetukset, raportit, poistologit.

7. Testataanko tietojen ja järjestelmien palauttamista säännöllisesti?

Hyväksymiskriteeri: Palautustestit tehdään riskiperusteisesti, kattavat kokonaiset palveluketjut ja osoittavat tietojen eheyden sekä tavoiteaikojen saavuttamisen.

Todentava näyttö: palautustestisuunnitelmat, testiraportit, palautusajat, virhe- ja korjauslistat.

8. Onko palautusmenettelyt dokumentoitu ja vastuuhenkilöiden saatavilla?

Hyväksymiskriteeri: Ohjeet sisältävät palautusjärjestyksen, riippuvuudet, käyttöoikeudet, yhteystiedot, tarkistukset ja päätöksenteon.

Todentava näyttö: palautusohjeet, toimintakortit, yhteystietoluettelot, dokumenttien jakelutiedot.

9. Valvotaanko varmuuskopiointikapasiteettia ja teknistä toimintakykyä?

Hyväksymiskriteeri: Tallennustila, suorituskyky, varmistusikkunat, lisenssit ja laitteiston kunto seurataan ennakoivasti.

Todentava näyttö: kapasiteettiraportit, valvontahälytykset, ylläpitoraportit, ennusteet.

10. Käsitelläänkö varmuuskopioinnin ja palautusten poikkeamat järjestelmällisesti?

Hyväksymiskriteeri: Toistuvien epäonnistumisten syyt selvitetään, korjaustoimille asetetaan omistaja ja määräaika, ja vaikuttavuus varmistetaan.

Todentava näyttö: poikkeamarekisteri, juurisyyanalyysit, toimenpidelista, uusintatestit.

JATKUVUUDENHALLINTA

Auditoinnin tavoite

Selvittää, onko yritys tunnistanut kriittiset palvelut ja riippuvuudet sekä varautunut ylläpitämään tai palauttamaan toimintansa hyväksytyssä ajassa häiriötilanteissa.

1. Onko yrityksellä hyväksytty jatkuvuudenhallintapolitiikka ja toimintamalli?

Hyväksymiskriteeri: Jatkuvuudenhallinnan tavoitteet, laajuus, vastuut, suunnitelmat, harjoittelu ja katselmointi on dokumentoitu ja johdon hyväksymä.

Todentava näyttö: jatkuvuuspolitiikka, toimintamalli, hyväksymispäätös, vastuumatriisi.

2. Onko liiketoiminnan kriittiset prosessit ja palvelut tunnistettu?

Hyväksymiskriteeri: Kriittisyys perustuu dokumentoituun liiketoimintavaikutusten arviointiin, jossa huomioidaan asiakas-, talous-, turvallisuus- ja lakivaikutukset.

Todentava näyttö: liiketoimintavaikutusten analyysi, prosessiluettelo, kriittisyysluokitus, haastattelumuistiot.

3. Onko kriittisille palveluille määritelty palautumistavoitteet?

Hyväksymiskriteeri: Palautumisaika-, palautuspiste- ja palvelutasotavoitteet on hyväksytty liiketoiminnan tarpeiden perusteella ja ne ovat teknisesti toteuttamiskelpoisia.

Todentava näyttö: RTO- ja RPO-määrittelyt, palvelutasot, hyväksynnät, tekniset arviot.

4. Onko kriittiset resurssit ja riippuvuudet tunnistettu?

Hyväksymiskriteeri: Henkilöstö, tilat, järjestelmät, tiedot, tietoliikenne, toimittajat, laitteet ja muut keskeiset riippuvuudet on dokumentoitu.

Todentava näyttö: riippuvuuskartat, palvelukuvaukset, resurssiluettelot, arkkitehtuurikuvat.

5. Onko kriittisille resursseille määritelty varajärjestelyt?

Hyväksymiskriteeri: Avainhenkilöille, tiloille, järjestelmille, yhteyksille, laitteille ja palveluntarjoajille on riskin mukaiset vaihtoehtoiset ratkaisut.

Todentava näyttö: varahenkilöluettelot, varatilasopimukset, tekniset vararatkaisut, vaihtoehtoiset toimittajat.

6. Onko jatkuvuus- ja palautumissuunnitelmat dokumentoitu ja ajantasaisia?

Hyväksymiskriteeri: Suunnitelmat sisältävät käynnistyskriteerit, vastuut, yhteystiedot, toimintavaiheet, prioriteetit, viestinnän ja paluun normaalitoimintaan.

Todentava näyttö: jatkuvuussuunnitelmat, toimintakortit, yhteystietoluettelot, versionhallintatiedot.

7. Ovatko jatkuvuussuunnitelmat käytettävissä myös normaalien järjestelmien häiriötilanteessa?

Hyväksymiskriteeri: Ajantasaiset suunnitelmat ja yhteystiedot ovat saatavilla suojatussa vaihtoehtoisessa muodossa tai sijainnissa.

Todentava näyttö: offline-kopiot, varajakelukanava, dokumenttirekisteri, saatavuustesti.

8. Harjoitellaanko jatkuvuus- ja palautumismenettelyjä säännöllisesti?

Hyväksymiskriteeri: Harjoitukset kattavat kriittiset skenaariot, riippuvuudet ja päätöksenteon sekä osoittavat palautumistavoitteiden toteutumisen.

Todentava näyttö: harjoitussuunnitelmat, osallistujaluettelot, harjoitusraportit, mitatut palautumisajat.

9. Päivitetäänkö suunnitelmat harjoitusten, poikkeamien ja muutosten perusteella?

Hyväksymiskriteeri: Havaitut puutteet kirjataan, vastuutetaan ja korjataan, ja suunnitelmat katselmoidaan merkittävien muutosten jälkeen.

Todentava näyttö: kehitystoimenpiteet, päivitetyt suunnitelmat, muutoslokit, jälkikatselmukset.

10. Raportoidaanko jatkuvuusvalmiuden tila johdolle?

Hyväksymiskriteeri: Johto saa säännöllisesti tiedon kriittisistä puutteista, harjoitustuloksista, palautumistavoitteista ja resursointitarpeista.

Todentava näyttö: jatkuvuusraportit, johdon katselmukset, riskiraportit, päätöspöytäkirjat.

HENKILÖSTÖN TIETOTURVAOSAAMINEN JA -KOULUTUS

Auditoinnin tavoite

Selvittää, tunnistaako henkilöstö tietoturvavastuunsa, saako se tehtäviensä edellyttämän koulutuksen ja osaako se toimia turvallisesti sekä ilmoittaa poikkeamista.

1. Onko henkilöstön tietoturvakoulutukselle hyväksytty suunnitelma?

Hyväksymiskriteeri: Koulutussuunnitelma määrittelee kohderyhmät, sisällöt, aikataulut, vastuut, uusintakoulutukset ja osaamisen seurannan.

Todentava näyttö: koulutussuunnitelma, vuosikello, vastuuhenkilöluettelo, hyväksymispäätös.

2. Saavatko uudet työntekijät tietoturvaperehdytyksen ennen tai heti työtehtävien alkaessa?

Hyväksymiskriteeri: Perehdytys kattaa keskeiset säännöt, salassapidon, hyväksyttävän käytön, tietojen käsittelyn ja poikkeamien ilmoittamisen.

Todentava näyttö: perehdytysmateriaali, suoritusrekisteri, perehdytyslistat, työntekijäotos.

3. Suorittaako koko henkilöstö säännöllisen tietoturvan kertauskoulutuksen?

Hyväksymiskriteeri: Pakollinen koulutus uusitaan määritellyin väliajoin, suorittamista seurataan ja puuttuvat suoritukset eskaloidaan.

Todentava näyttö: koulutusrekisteri, suoritusraportit, muistutukset, eskalointitiedot.

4. Onko erityisrooleille määritelty tehtäväkohtainen tietoturvakoulutus?

Hyväksymiskriteeri: Pääkäyttäjät, kehittäjät, johto, asiakaspalvelu, taloushallinto ja muut riskialttiit roolit saavat tehtäviinsä soveltuvan lisäkoulutuksen.

Todentava näyttö: roolikohtaiset koulutuspolut, osallistujaluettelot, pätevyysvaatimukset, koulutusmateriaalit.

5. Testataanko henkilöstön kykyä tunnistaa tietojenkalastelu ja muu sosiaalinen manipulointi?

Hyväksymiskriteeri: Simulaatioita tai muita harjoituksia toteutetaan suunnitellusti, tulokset analysoidaan ja riskiryhmille järjestetään lisäohjausta.

Todentava näyttö: kalastelusimulaatioiden raportit, tulosanalyysit, lisäkoulutukset, kehitystoimet.

6. Onko henkilöstölle ohjeistettu turvallinen etä- ja hybridityö?

Hyväksymiskriteeri: Ohjeistus kattaa laitteet, verkkoyhteydet, työtilan yksityisyyden, paperiaineistot, matkustamisen ja poikkeamista ilmoittamisen.

Todentava näyttö: etätyöohje, matkustusturvaohje, henkilöstöviestit, koulutusmateriaali.

7. Ovatko tietoturvaohjeet henkilöstön helposti saatavilla ja ymmärrettäviä?

Hyväksymiskriteeri: Ajantasaiset ohjeet ovat keskitetysti saatavilla, niitä viestitään säännöllisesti ja olennaiset muutokset tuodaan henkilöstön tietoon.

Todentava näyttö: intranet, ohjerekisteri, tiedotteet, versionhallinta, henkilöstökyselyt.

8. Ymmärtääkö henkilöstö velvollisuutensa ilmoittaa tietoturvahavainnoista?

Hyväksymiskriteeri: Ilmoituskynnys on matala, kanavat tunnetaan ja henkilöstö osaa tunnistaa esimerkkejä ilmoitettavista tilanteista.

Todentava näyttö: koulutustulokset, henkilöstökyselyt, ilmoitusohje, harjoitushavainnot.

9. Käsitelläänkö tietoturvaohjeiden rikkomukset yhdenmukaisesti?

Hyväksymiskriteeri: Tahattomat virheet, huolimattomuus ja tahallinen väärinkäyttö tutkitaan dokumentoidulla menettelyllä ja seuraamukset ovat oikeasuhtaisia.

Todentava näyttö: rikkomusten käsittelyohje, HR-prosessi, anonymisoidut tapausraportit, päätökset.

10. Arvioidaanko koulutuksen vaikuttavuutta ja kehitetäänkö sisältöä tulosten perusteella?

Hyväksymiskriteeri: Vaikuttavuutta seurataan osaamistesteillä, simulaatioilla, poikkeamatiedoilla ja palautteella, ja havaintoihin reagoidaan.

Todentava näyttö: testitulokset, poikkeamatrendit, palautekyselyt, päivitetyt koulutusmateriaalit.

TOIMITTAJIEN JA KUMPPANEIDEN TIETOTURVAN HALLINTA

Auditoinnin tavoite

Selvittää, arvioidaanko ulkoisiin toimittajiin ja kumppaneihin liittyvät tietoturvariskit ennen yhteistyötä, sopimuksen aikana ja yhteistyön päättyessä.

1. Onko toimittajien tietoturvan hallintaprosessi dokumentoitu?

Hyväksymiskriteeri: Prosessi kattaa riskiluokituksen, ennakkoarvioinnin, sopimusvaatimukset, seurannan, poikkeamat, muutokset ja yhteistyön päättämisen.

Todentava näyttö: toimittajahallintaprosessi, hankintaohje, tietoturvaohje, vastuumatriisi.

2. Luokitellaanko toimittajat palvelun, tietojen ja käyttöoikeuksien riskin perusteella?

Hyväksymiskriteeri: Luokittelu huomioi palvelun kriittisyyden, käsiteltävät tiedot, järjestelmäpääsyn, alihankinnan, sijainnin ja jatkuvuusvaikutukset.

Todentava näyttö: toimittajaluokittelu, riskikyselyt, palvelukuvaukset, kriittisyysarviot.

3. Arvioidaanko toimittajan tietoturvallisuus ennen sopimuksen tekemistä?

Hyväksymiskriteeri: Riskitasoon nähden riittävä arviointi tehdään ennen valintaa ja havaitut puutteet käsitellään ennen palvelun käyttöönottoa.

Todentava näyttö: toimittaja-arvioinnit, auditointiraportit, sertifikaatit, korjaussuunnitelmat.

4. Sisältyvätkö sopimuksiin tarvittavat tietoturvavaatimukset?

Hyväksymiskriteeri: Sopimus määrittelee vähintään tietojen suojauksen, käyttöoikeudet, poikkeamailmoitukset, auditointioikeudet, jatkuvuuden ja yhteistyön päättymisen.

Todentava näyttö: sopimukset, tietoturvaliitteet, sopimusmallit, lakikatselmukset.

5. Onko toimittajien tietoturvapoikkeamille määritelty ilmoitus- ja yhteistyömenettely?

Hyväksymiskriteeri: Toimittajan on ilmoitettava sovitussa ajassa poikkeamista, osallistuttava tutkintaan ja toimitettava tarvittavat tiedot sekä korjaustoimet.

Todentava näyttö: sopimusehdot, poikkeamamenettely, yhteystietoluettelo, tapausraportit.

6. Hallitaanko toimittajien ja huoltohenkilöstön käyttöoikeudet turvallisesti?

Hyväksymiskriteeri: Ulkoiset oikeudet ovat henkilökohtaisia, rajattuja, määräaikaisia, hyväksyttyjä ja valvottuja sekä poistetaan tarpeen päättyessä.

Todentava näyttö: toimittajatunnusten luettelo, hyväksynnät, pääsylokit, oikeuksien poistotiedot.

7. Valvotaanko kriittisten toimittajien tietoturvan tasoa sopimuskauden aikana?

Hyväksymiskriteeri: Seuranta perustuu riskitasoon ja hyödyntää esimerkiksi raportointia, katselmuksia, auditointeja, sertifikaatteja ja poikkeamatietoja.

Todentava näyttö: toimittajakatselmukset, auditointiraportit, palveluraportit, sertifikaatit.

8. Hallitaanko toimittajan käyttämät alihankkijat ja palveluketjut?

Hyväksymiskriteeri: Alihankkijoiden käyttö on läpinäkyvää, hyväksyttyä tai ilmoitettua, ja samat olennaiset tietoturvavaatimukset ulotetaan palveluketjuun.

Todentava näyttö: alihankkijaluettelot, sopimusehdot, hyväksynnät, toimitusketjun riskiarviot.

9. Onko kriittisten toimittajien jatkuvuus ja korvattavuus arvioitu?

Hyväksymiskriteeri: Toimittajariippuvuudet, varajärjestelyt, palvelun siirrettävyys, varatoimittajat ja exit-suunnitelmat on arvioitu.

Todentava näyttö: jatkuvuusarviot, exit-suunnitelmat, vaihtoehtoisten toimittajien luettelo, harjoitusraportit.

10. Poistetaanko toimittajan pääsyt ja palautetaanko tai hävitetäänkö tiedot yhteistyön päättyessä?

Hyväksymiskriteeri: Sopimuksen päättyessä tunnukset suljetaan, aineistot palautetaan tai hävitetään, laitteet palautetaan ja toimenpiteet todennetaan.

Todentava näyttö: päättämistarkastuslista, tunnusten sulkemislokit, palautus- ja hävitystodistukset, sopimuspäätös.

AUDITOINNIT, VAATIMUSTENMUKAISUUS JA JATKUVA KEHITTÄMINEN

Auditoinnin tavoite

Selvittää, arvioidaanko tietoturvakontrollien toimivuutta riippumattomasti, seurataanko vaatimustenmukaisuutta ja toteutetaanko havaitut kehitystoimet järjestelmällisesti.

1. Onko tietoturva-auditoinneille laadittu riskiperusteinen auditointiohjelma?

Hyväksymiskriteeri: Auditointiohjelma kattaa keskeiset prosessit, järjestelmät, toimittajat ja vaatimukset määritellyllä aikavälillä ja perustuu riskeihin.

Todentava näyttö: auditointiohjelma, auditointisuunnitelma, riskiarviot, hyväksymispäätös.

2. Ovatko auditointien tavoitteet, laajuus ja arviointikriteerit määritelty etukäteen?

Hyväksymiskriteeri: Jokaiselle auditoinnille on dokumentoitu kohde, tavoitteet, rajaukset, viitevaatimukset, menetelmät ja vastuuhenkilöt.

Todentava näyttö: auditointitoimeksianto, auditointisuunnitelma, tarkastuslista, viitekehys.

3. Ovatko auditoijat riittävän päteviä ja riippumattomia arvioitavasta toiminnasta?

Hyväksymiskriteeri: Auditoijilla on tehtävään soveltuva osaaminen, eikä heillä ole sellaista vastuuta arvioitavasta kohteesta, joka vaarantaisi puolueettomuuden.

Todentava näyttö: pätevyystiedot, koulutusrekisteri, auditoijaluettelo, riippumattomuusarvio.

4. Perustuvatko auditointitulokset riittävään ja todennettavaan näyttöön?

Hyväksymiskriteeri: Johtopäätökset perustuvat asiakirjoihin, järjestelmätietoihin, haastatteluihin, havaintoihin ja tarkoituksenmukaiseen otantaan.

Todentava näyttö: auditointimuistiinpanot, näyttöluettelo, otantatiedot, haastattelut, lokiotteet.

5. Luokitellaanko auditointihavainnot vakavuuden ja riskin perusteella?

Hyväksymiskriteeri: Havainnot luokitellaan yhtenäisin perustein, ja luokittelu ohjaa korjausaikaa, eskalointia ja raportointia.

Todentava näyttö: havaintoluokittelu, auditointiraportit, riskiperusteet, eskalointiohje.

6. Määritelläänkö havainnoille korjaavat toimenpiteet, omistajat ja määräajat?

Hyväksymiskriteeri: Jokaisella olennaisella havainnolla on hyväksytty toimenpide, vastuuhenkilö, määräaika ja seurattava tila.

Todentava näyttö: toimenpiderekisteri, vastuuhenkilömerkinnät, hyväksynnät, määräaikaseuranta.

7. Varmistetaanko korjaavien toimenpiteiden valmistuminen ja vaikuttavuus?

Hyväksymiskriteeri: Toimenpiteen toteutus todennetaan näytöllä ja arvioidaan, onko havaittu puute poistunut ja riski pienentynyt hyväksyttävälle tasolle.

Todentava näyttö: sulkemisnäyttö, uusintatarkastus, jälkiauditointi, päivitetty riskiarvio.

8. Seurataanko lakien, viranomaisvaatimusten, sopimusten ja standardien muutoksia?

Hyväksymiskriteeri: Vaatimusten muutoksille on nimetty seuranta, vaikutukset arvioidaan ja tarvittavat prosessi- tai kontrollimuutokset toteutetaan.

Todentava näyttö: vaatimusrekisteri, lakiseurantaraportit, vaikutusarviot, muutosprojektit.

9. Raportoidaanko auditointien ja vaatimustenmukaisuuden tila johdolle?

Hyväksymiskriteeri: Raportointi sisältää merkittävät havainnot, avoimet toimenpiteet, määräaikojen ylitykset, toistuvat puutteet ja päätöstarpeet.

Todentava näyttö: johdon raportit, auditointiyhteenvedot, johtoryhmän pöytäkirjat, mittariraportit.

10. Hyödynnetäänkö auditointi-, poikkeama- ja mittaritietoa jatkuvassa parantamisessa?

Hyväksymiskriteeri: Yritys tunnistaa trendejä ja juurisyitä, priorisoi kehityshankkeet ja seuraa, että tietoturvan kypsyys ja riskitaso kehittyvät tavoitteiden mukaisesti.

Todentava näyttö: kehitysohjelma, trendianalyysit, kypsyysarviot, tiekartta, johdon katselmukset.