STARATEGIA JA JOHTAMINEN

Auditoinnin tavoite

Selvittää, ovatko yrityksen strategia, johtamisjärjestelmä, päätöksenteko, vastuut ja turvallisuutta koskevat tavoitteet asianmukaisesti määriteltyjä ja toteutettuja.

1. Onko organisaatiolla hyväksytty ja ajantasainen strategia?

Hyväksymiskriteeri: Strategia on kirjallinen, johdon hyväksymä, voimassa oleva ja henkilöstön saatavilla.

Todentava näyttö: strategia-asiakirja, hyväksymispäätös, johtoryhmän pöytäkirja.

2. Onko strategiassa huomioitu toiminnan turvallisuus, jatkuvuus ja keskeiset riskit?

Hyväksymiskriteeri: Strategiassa tai sitä tukevissa suunnitelmissa on asetettu tavoitteita turvallisuudelle, jatkuvuudelle ja riskienhallinnalle.

Todentava näyttö: strategiset tavoitteet, turvallisuusohjelma, jatkuvuussuunnitelma.

3. Onko strategisille tavoitteille määritelty vastuuhenkilöt, mittarit ja aikataulut?

Hyväksymiskriteeri: Jokaisella keskeisellä tavoitteella on omistaja, seurattava mittari ja määräaika.

Todentava näyttö: tavoitekortit, toimintasuunnitelmat, tulosmittarit.

4. Seuraako johto strategian toteutumista säännöllisesti?

Hyväksymiskriteeri: Toteutumista käsitellään sovitun vuosikellon mukaisesti ja poikkeamiin reagoidaan.

Todentava näyttö: johtoryhmän pöytäkirjat, katselmukset, mittariraportit.

5. Ovatko päätöksentekovaltuudet ja hyväksymisrajat dokumentoitu?

Hyväksymiskriteeri: Päätös-, hankinta-, sopimus- ja talousvaltuudet on määritelty tehtävä- tai roolikohtaisesti.

Todentava näyttö: hallintosääntö, delegointipäätökset, hyväksymismatriisi.

6. Onko organisaation vastuunjako selkeä ja ajantasainen?

Hyväksymiskriteeri: Organisaatiorakenne, roolit, varahenkilöt ja raportointisuhteet on dokumentoitu.

Todentava näyttö: organisaatiokaavio, tehtävänkuvaukset, vastuunjakotaulukko.

7. [KRIITTINEN] Onko johto nimennyt vastuuhenkilöt tietoturvalle, riskienhallinnalle, tietosuojalle ja jatkuvuudelle?

Hyväksymiskriteeri: Keskeisille turvallisuus- ja valvontatehtäville on nimetty vastuuhenkilöt ja varahenkilöt.

Todentava näyttö: nimityspäätökset, tehtävänkuvaukset, vastuumatriisi.

8. Saako johto säännöllisesti tietoa merkittävistä riskeistä, poikkeamista ja turvallisuustapahtumista?

Hyväksymiskriteeri: Johdolle raportoidaan sovitulla tavalla merkittävät riskit, tapahtumat ja korjaavien toimenpiteiden tila.

Todentava näyttö: johdon raportit, tilannekuvat, poikkeamaraportit.

9. Onko esteellisyydet ja eturistiriidat huomioitu päätöksenteossa?

Hyväksymiskriteeri: Eturistiriitojen ilmoittamiselle, käsittelylle ja dokumentoinnille on määritelty menettely.

Todentava näyttö: esteellisyysperiaatteet, ilmoitukset, pöytäkirjamerkinnät.

10. [KRIITTINEN] Onko organisaatiolla menettely toiminnan jatkuvuuden johtamiseksi vakavassa häiriötilanteessa?

Hyväksymiskriteeri: Johtamisvastuut, päätöksenteko, varajärjestelyt ja viestintä on määritelty ja harjoiteltu.

Todentava näyttö: jatkuvuus- ja kriisijohtamissuunnitelmat, harjoitusraportit.

TALOUSHALLINTO

Auditoinnin tavoite

Selvittää, ovatko taloushallinnon menettelyt luotettavia, jäljitettäviä ja riittävästi suojattuja virheiltä, väärinkäytöksiltä ja tietojen menettämiseltä.

1. Ovatko taloushallinnon vastuut ja hyväksymisvaltuudet dokumentoitu?

Hyväksymiskriteeri: Maksamisen, kirjaamisen, hyväksymisen ja täsmäyttämisen vastuut on erotettu toisistaan.

Todentava näyttö: vastuumatriisi, hyväksymisrajat, käyttäjäroolit.

2. [KRIITTINEN] Toteutuuko tehtävien eriyttäminen maksuliikenteessä?

Hyväksymiskriteeri: Sama henkilö ei voi yksin luoda toimittajaa, muuttaa maksutietoja, hyväksyä laskua ja suorittaa maksua.

Todentava näyttö: järjestelmäroolit, maksuprosessin kuvaus, otanta maksutapahtumista.

3. Hyväksytäänkö ostolaskut määriteltyjen valtuuksien mukaisesti?

Hyväksymiskriteeri: Laskuilla on asianmukainen tarkastus, hyväksyntä ja tarvittaessa sopimus- tai tilaustieto.

Todentava näyttö: laskuotos, hyväksymiskierto, tilausviitteet.

4. [KRIITTINEN] Varmistetaanko pankki- ja maksutietojen muutokset riippumattomalla tavalla?

Hyväksymiskriteeri: Toimittajan tilinumeron muutos varmistetaan luotettavasta, aiemmin tunnetusta yhteystiedosta.

Todentava näyttö: muutoslokit, varmistusmerkinnät, ohjeistus.

5. Täsmäytetäänkö pankkitilit, pääkirja ja reskontrat säännöllisesti?

Hyväksymiskriteeri: Täsmäytykset tehdään määräajoin, dokumentoidaan ja poikkeamat käsitellään.

Todentava näyttö: täsmäytysraportit, hyväksynnät, poikkeamaselvitykset.

6. Onko budjetointi- ja ennustamisprosessi määritelty?

Hyväksymiskriteeri: Budjetin laadinta, hyväksyntä, seuranta ja ennusteiden päivittäminen on vastuutettu.

Todentava näyttö: budjetointiohje, vuosikello, raportit.

7. Seurataanko taloudellisia poikkeamia ja epätyypillisiä tapahtumia?

Hyväksymiskriteeri: Merkittävät ylitykset, poikkeavat maksut ja muut epätavalliset tapahtumat tutkitaan.

Todentava näyttö: poikkeamaraportit, analyysit, selvitykset.

8. Ovatko taloushallinnon järjestelmien käyttöoikeudet rajattu työtehtävien mukaisesti?

Hyväksymiskriteeri: Käyttöoikeudet myönnetään hyväksyntään perustuen ja tarkastetaan säännöllisesti.

Todentava näyttö: käyttäjäluettelot, käyttöoikeustarkastukset, lokit.

9. Säilytetäänkö kirjanpito- ja maksuaineistot hallitusti?

Hyväksymiskriteeri: Säilytysajat, suojaus, varmuuskopiointi ja hävittäminen on määritelty.

Todentava näyttö: tiedonhallintaohje, arkistointikäytäntö, varmistusraportit.

10. Onko taloushallinnon väärinkäytösten tunnistamiseen ja ilmoittamiseen menettely?

Hyväksymiskriteeri: Henkilöstö tietää, miten epäillyistä väärinkäytöksistä ilmoitetaan ja miten ilmoitukset tutkitaan.

Todentava näyttö: väärinkäytösohje, ilmoituskanava, käsittelyprosessi.

HENKILÖSTÖHALLINTO

Auditoinnin tavoite

Selvittää, hallitaanko henkilöstön elinkaari, henkilötiedot, käyttöoikeudet, osaaminen ja turvallisuusvastuut asianmukaisesti.

1. Onko rekrytointi- ja valintaprosessi dokumentoitu?

Hyväksymiskriteeri: Rekrytoinnin vastuut, hyväksynnät, arviointiperusteet ja dokumentointi on määritelty.

Todentava näyttö: rekrytointiohje, hakijadokumentit, hyväksymispäätökset.

2. Tehdäänkö tehtävän edellyttämät tausta- ja kelpoisuustarkastukset?

Hyväksymiskriteeri: Tarkastukset perustuvat tehtävän riskeihin ja sovellettaviin vaatimuksiin.

Todentava näyttö: tarkastusmerkinnät, suostumukset, riskiluokittelu.

3. Ovatko työsopimukset ja salassapitovelvoitteet asianmukaisesti dokumentoitu?

Hyväksymiskriteeri: Sopimukset ovat hyväksyttyjä, allekirjoitettuja ja turvallisesti säilytettyjä.

Todentava näyttö: sopimusotos, salassapitositoumukset, säilytyskäytäntö.

4. Saavatko uudet työntekijät perehdytyksen turvallisuuteen ja tietosuojaan?

Hyväksymiskriteeri: Perehdytys suoritetaan ennen itsenäisen työskentelyn aloittamista ja suoritus dokumentoidaan.

Todentava näyttö: perehdytyslistat, koulutusmateriaalit, suoritusmerkinnät.

5. Onko tehtävien ja käyttöoikeuksien myöntäminen hyväksyttyä ja rooliperusteista?

Hyväksymiskriteeri: Käyttöoikeudet vastaavat työtehtäviä eikä tarpeettomia oikeuksia myönnetä.

Todentava näyttö: käyttöoikeuspyynnöt, hyväksynnät, roolikuvaukset.

6. Tarkastetaanko henkilöstön käyttöoikeudet tehtävien muuttuessa?

Hyväksymiskriteeri: Roolimuutokset käynnistävät käyttöoikeuksien tarkistamisen ja tarpeettomien oikeuksien poistamisen.

Todentava näyttö: muutosilmoitukset, tarkastusraportit, lokit.

7. [KRIITTINEN] Poistetaanko työsuhteen päättyessä käyttöoikeudet ja kulkuoikeudet viipymättä?

Hyväksymiskriteeri: Poistaminen tapahtuu ennalta määritellyssä ajassa ja kattaa kaikki järjestelmät, laitteet ja tilat.

Todentava näyttö: päättämislista, tunnusten sulkemisajat, laitepalautukset.

8. Koulutetaanko henkilöstöä säännöllisesti turvallisuuteen ja toimintaperiaatteisiin?

Hyväksymiskriteeri: Koulutukset ovat rooliperusteisia, toistuvia ja niiden suorittamista seurataan.

Todentava näyttö: koulutusrekisteri, osallistumistiedot, osaamistestit.

9. Suojataanko henkilöstö- ja palkkatiedot asianmukaisesti?

Hyväksymiskriteeri: Tietoihin pääsevät vain tehtävänsä vuoksi niitä tarvitsevat henkilöt.

Todentava näyttö: käyttöoikeudet, lokit, säilytys- ja salauskäytännöt.

10. Onko epäasiallisen toiminnan, häirinnän ja turvallisuuspoikkeamien ilmoittamiseen luottamuksellinen menettely?

Hyväksymiskriteeri: Ilmoituskanavat, käsittelijät, suojaaminen ja jatkotoimenpiteet on määritelty.

Todentava näyttö: toimintaohje, ilmoituskanava, anonymisoidut käsittelytiedot.

SOPIMUS JA DOKUMENTINHALLINTA

Auditoinnin tavoite

Selvittää, ovatko sopimukset ja asiakirjat hallittuja koko niiden elinkaaren ajan ja suojattuja luvattomalta käytöltä, muuttamiselta tai häviämiseltä.

1. Onko sopimusten laatimiselle, tarkastamiselle ja hyväksymiselle määritelty prosessi?

Hyväksymiskriteeri: Vastuut, tarkastusvaiheet, hyväksymisvaltuudet ja allekirjoitusmenettelyt on dokumentoitu.

Todentava näyttö: sopimusprosessi, mallipohjat, hyväksymismatriisi.

2. [KRIITTINEN] Allekirjoittavatko sopimukset vain siihen valtuutetut henkilöt?

Hyväksymiskriteeri: Allekirjoitusoikeus voidaan todentaa eikä valtuuksia ylitetä.

Todentava näyttö: nimenkirjoitusoikeudet, delegoinnit, sopimusotos.

3. Sisältävätkö sopimukset tarvittavat turvallisuus-, salassapito- ja tietosuojavaatimukset?

Hyväksymiskriteeri: Sopimusehdot vastaavat käsiteltävien tietojen, palvelun ja toimittajan riskitasoa.

Todentava näyttö: sopimuspohjat, sopimusotos, tietojenkäsittelyehdot.

4. Onko voimassa olevista sopimuksista keskitetty ja ajantasainen rekisteri?

Hyväksymiskriteeri: Rekisteristä ilmenevät omistaja, vastapuoli, voimassaolo, irtisanomisaika ja keskeiset velvoitteet.

Todentava näyttö: sopimusrekisteri, otanta ja vertailu alkuperäisiin sopimuksiin.

5. Seurataanko sopimusten määräaikoja ja velvoitteita?

Hyväksymiskriteeri: Uusimisista, irtisanomisajoista ja tarkastuspäivistä syntyy ennakoiva ilmoitus.

Todentava näyttö: hälytykset, vuosikello, seurantaluettelo.

6. Onko dokumenteille määritelty omistajat, versiot ja hyväksymistila?

Hyväksymiskriteeri: Käytössä oleva versio voidaan tunnistaa eikä vanhentuneita versioita käytetä vahingossa.

Todentava näyttö: dokumenttirekisteri, versiohistoria, hyväksymismerkinnät.

7. Ovatko dokumenttien käyttöoikeudet tiedon luokittelun mukaiset?

Hyväksymiskriteeri: Luottamuksellisiin asiakirjoihin on pääsy vain valtuutetuilla käyttäjillä.

Todentava näyttö: käyttöoikeusluettelot, luokittelumerkinnät, lokit.

8. Voidaanko dokumentteihin tehdyt muutokset jäljittää?

Hyväksymiskriteeri: Järjestelmä tallentaa tekijän, ajankohdan ja muutoksen tai säilyttää versiohistorian.

Todentava näyttö: auditointiloki, versiohistoria, muutosmerkinnät.

9. Onko asiakirjoille määritelty säilytys- ja hävittämisajat?

Hyväksymiskriteeri: Säilytys perustuu toiminnalliseen, sopimukselliseen tai sovellettavaan vaatimukseen.

Todentava näyttö: tiedonohjaussuunnitelma, säilytysaikataulu, hävittämisraportit.

10. [KRIITTINEN] Onko keskeiset sopimukset ja dokumentit varmistettu ja palautettavissa?

Hyväksymiskriteeri: Aineistosta on suojatut varmuuskopiot ja palauttamista on testattu.

Todentava näyttö: varmistusraportit, palautustestit, jatkuvuussuunnitelma.

TIETOHALLINTO JA TIETOTURVA

Auditoinnin tavoite

Selvittää, hallitaanko järjestelmiä, laitteita, käyttöoikeuksia, tietoja ja turvallisuuspoikkeamia niiden riskien edellyttämällä tavalla.

1. Onko tietohallinnon ja tietoturvan johtamismalli dokumentoitu?

Hyväksymiskriteeri: Vastuut, päätöksenteko, resurssit ja raportointisuhteet on määritelty.

Todentava näyttö: tietohallintomalli, tietoturvapolitiikka, vastuumatriisi.

2. Onko organisaatiolla ajantasainen järjestelmä-, laite- ja tietovarantojen luettelo?

Hyväksymiskriteeri: Omaisuudelle on nimetty omistaja, luokitus, sijainti ja elinkaaritila.

Todentava näyttö: CMDB, laiteluettelo, järjestelmärekisteri.

3. [KRIITTINEN] Käytetäänkö vahvaa tunnistautumista kriittisissä ja etäkäyttöä mahdollistavissa järjestelmissä?

Hyväksymiskriteeri: Monivaiheinen tunnistautuminen on käytössä riskiperusteisesti ja poikkeamat on hyväksytty.

Todentava näyttö: järjestelmäasetukset, käyttäjäotos, poikkeusluettelo.

4. Myönnetäänkö käyttöoikeudet vähimmän oikeuden periaatteella?

Hyväksymiskriteeri: Oikeudet perustuvat tehtävään, ovat hyväksyttyjä ja määräaikaiset oikeudet vanhenevat automaattisesti.

Todentava näyttö: käyttöoikeuspyynnöt, roolit, tarkastusraportit.

5. Tarkastetaanko käyttöoikeudet ja pääkäyttäjäoikeudet säännöllisesti?

Hyväksymiskriteeri: Omistajat vahvistavat oikeuksien tarpeellisuuden ja ylimääräiset oikeudet poistetaan.

Todentava näyttö: käyttöoikeuskatselmukset, poistot, pääkäyttäjäluettelo.

6. [KRIITTINEN] Päivitetäänkö käyttöjärjestelmät, sovellukset ja verkkolaitteet hallitusti?

Hyväksymiskriteeri: Tietoturvapäivityksille on määräajat, seuranta ja dokumentoitu poikkeuskäsittely.

Todentava näyttö: päivitysraportit, haavoittuvuusskannaukset, poikkeushyväksynnät.

7. Onko muutostenhallinta käytössä tuotantojärjestelmissä?

Hyväksymiskriteeri: Muutokset arvioidaan, testataan, hyväksytään ja niille on palautussuunnitelma.

Todentava näyttö: muutospyynnöt, testausnäyttö, hyväksynnät.

8. [KRIITTINEN] Ovatko varmuuskopiot suojattuja ja onko palauttamista testattu?

Hyväksymiskriteeri: Varmuuskopiot ovat erillään tuotannosta, suojattuja muuttamiselta ja palautettavissa tavoiteajassa.

Todentava näyttö: varmistuslokit, palautustestit, palautumisaikatavoitteet.

9. Valvotaanko järjestelmiä ja tietoturvatapahtumia?

Hyväksymiskriteeri: Keskeiset lokit kerätään, suojataan ja poikkeaviin tapahtumiin reagoidaan.

Todentava näyttö: lokiasetukset, hälytykset, valvontaraportit.

10. [KRIITTINEN] Onko tietoturvapoikkeamien käsittelyprosessi määritelty ja harjoiteltu?

Hyväksymiskriteeri: Havaitseminen, ilmoittaminen, rajaaminen, tutkinta, palautuminen ja jälkiarviointi on määritelty.

Todentava näyttö: poikkeamaprosessi, harjoitusraportit, tapausrekisteri.

RISKIENHALLINTA JA COMPLIANCE

Auditoinnin tavoite

Selvittää, tunnistaako organisaatio toimintansa riskit ja velvoitteet sekä käsitteleekö ja seuraako se niitä järjestelmällisesti.

1. Onko organisaatiolla hyväksytty riskienhallintapolitiikka?

Hyväksymiskriteeri: Politiikka määrittelee tavoitteet, vastuut, arviointimenetelmän ja raportoinnin.

Todentava näyttö: riskienhallintapolitiikka, hyväksymispäätös.

2. Onko riskien tunnistaminen osa keskeisiä prosesseja ja päätöksentekoa?

Hyväksymiskriteeri: Riskejä arvioidaan esimerkiksi muutoksissa, hankinnoissa, projekteissa ja uusissa palveluissa.

Todentava näyttö: riskinarvioinnit, projektidokumentit, päätösesitykset.

3. Onko organisaatiolla ajantasainen riskirekisteri?

Hyväksymiskriteeri: Rekisterissä ovat riskin kuvaus, omistaja, vaikutus, todennäköisyys, käsittely ja määräaika.

Todentava näyttö: riskirekisteri, päivityshistoria.

4. [KRIITTINEN] Onko merkittäville riskeille nimetty omistajat ja käsittelytoimenpiteet?

Hyväksymiskriteeri: Jokaiselle merkittävälle riskille on hyväksytty käsittelysuunnitelma ja vastuuhenkilö.

Todentava näyttö: riskien käsittelysuunnitelmat, johdon hyväksynnät.

5. Onko organisaation riskinottohalu ja hyväksyttävä riskitaso määritelty?

Hyväksymiskriteeri: Johto on määritellyt, millaisia riskejä voidaan hyväksyä ja milloin asia on eskaloitava.

Todentava näyttö: riskikriteerit, päätökset, eskalointimalli.

6. Tunnistetaanko organisaatiota koskevat lait, määräykset, sopimusvelvoitteet ja sisäiset vaatimukset?

Hyväksymiskriteeri: Velvoitteista ylläpidetään rekisteriä, jossa on vastuuhenkilöt ja seuranta.

Todentava näyttö: velvoite- tai compliance-rekisteri, vastuuluettelo.

7. Arvioidaanko vaatimustenmukaisuuden toteutumista säännöllisesti?

Hyväksymiskriteeri: Toteutumista arvioidaan katselmuksilla, tarkastuksilla tai itsearvioinneilla.

Todentava näyttö: compliance-arvioinnit, tarkastusraportit, seurantasuunnitelmat.

8. Onko rikkomusten ja epäiltyjen väärinkäytösten ilmoittamiseen suojattu kanava?

Hyväksymiskriteeri: Ilmoitukset voidaan tehdä luottamuksellisesti ja ne käsitellään puolueettomasti.

Todentava näyttö: ilmoituskanava, käsittelyohje, käsittelijöiden valtuutukset.

9. Seurataanko korjaavia toimenpiteitä niiden valmistumiseen saakka?

Hyväksymiskriteeri: Toimenpiteillä on vastuuhenkilöt, määräajat ja vaikutusten tarkistus.

Todentava näyttö: toimenpiderekisteri, seurantapöytäkirjat.

10. Raportoidaanko merkittävät riskit ja vaatimustenmukaisuuspoikkeamat johdolle?

Hyväksymiskriteeri: Raportointi on säännöllistä, riittävän kattavaa ja johtaa tarvittaessa päätöksiin.

Todentava näyttö: johdon raportit, pöytäkirjat, päätökset.

HANKINTA- JA TOIMITTAJAHALLINTA

Auditoinnin tavoite

Selvittää, valitaanko, arvioidaanko ja valvotaanko toimittajia asianmukaisesti koko hankinnan ja sopimuksen elinkaaren ajan.

1. Onko hankintaprosessi ja siihen liittyvät valtuudet dokumentoitu?

Hyväksymiskriteeri: Tarpeen määrittely, kilpailutus, valinta, hyväksyntä ja vastaanotto on kuvattu.

Todentava näyttö: hankintaohje, hyväksymisrajat, prosessikuvaus.

2. Toteutetaanko hankinnat hyväksyttyjen periaatteiden ja menettelyjen mukaisesti?

Hyväksymiskriteeri: Hankinnasta voidaan todentaa tarve, vertailu, päätösperusteet ja hyväksyntä.

Todentava näyttö: hankintaotos, tarjoukset, vertailut, päätökset.

3. Arvioidaanko toimittajan taloudellinen, toiminnallinen ja turvallisuuteen liittyvä soveltuvuus ennen valintaa?

Hyväksymiskriteeri: Arviointi vastaa hankinnan kriittisyyttä ja käsiteltävän tiedon riskejä.

Todentava näyttö: due diligence -arvioinnit, kyselyt, referenssit.

4. [KRIITTINEN] Sisältävätkö kriittisten toimittajien sopimukset turvallisuus- ja jatkuvuusvaatimukset?

Hyväksymiskriteeri: Sopimuksissa on vaatimukset tietoturvasta, ilmoitusajoista, jatkuvuudesta, alihankinnasta ja tarkastusoikeuksista.

Todentava näyttö: sopimusotos, turvallisuusliitteet, palvelutasosopimukset.

5. Onko toimittajat luokiteltu niiden kriittisyyden ja riskien perusteella?

Hyväksymiskriteeri: Luokittelu ohjaa arviointia, seurantaa, sopimusehtoja ja jatkuvuusvaatimuksia.

Todentava näyttö: toimittajarekisteri, kriittisyysluokitus.

6. Seurataanko toimittajien suorituskykyä ja palvelutasoa?

Hyväksymiskriteeri: Laatua, toimitusvarmuutta, poikkeamia ja palvelutasoa seurataan sovituilla mittareilla.

Todentava näyttö: palveluraportit, toimittajakatselmukset, mittarit.

7. Seurataanko toimittajien tietoturva- ja muita poikkeamia?

Hyväksymiskriteeri: Toimittajan on ilmoitettava poikkeamista sovitussa ajassa, ja tapahtumat käsitellään organisaatiossa.

Todentava näyttö: poikkeamailmoitukset, sopimusehdot, käsittelyraportit.

8. Hallitaanko toimittajien ja alihankkijoiden pääsyä organisaation tietoihin ja järjestelmiin?

Hyväksymiskriteeri: Pääsy on hyväksyttyä, rajattua, valvottua ja poistetaan tarpeen päättyessä.

Todentava näyttö: toimittajatunnukset, käyttöoikeudet, lokit, poistot.

9. Onko toimittajan vaihtamiseen tai palvelun päättymiseen suunnitelma?

Hyväksymiskriteeri: Tietojen palautus, siirto, poistaminen, tunnusten sulkeminen ja jatkuvuus on määritelty.

Todentava näyttö: exit-suunnitelma, sopimusehdot, siirtomenettelyt.

10. [KRIITTINEN] Onko kriittisten toimittajien häiriöihin varauduttu?

Hyväksymiskriteeri: Organisaatiolla on vaihtoehtoiset toimintatavat, varajärjestelyt tai hyväksytty riskipäätös.

Todentava näyttö: jatkuvuussuunnitelma, vaihtoehtoisten toimittajien arviointi, harjoitukset.

VIESTINTÄ JA RAPORTOINTI

Auditoinnin tavoite

Selvittää, tuotetaanko ja välitetäänkö oikeaa tietoa oikeille vastaanottajille turvallisesti, oikea-aikaisesti ja ymmärrettävässä muodossa.

1. Onko sisäisen ja ulkoisen viestinnän vastuut määritelty?

Hyväksymiskriteeri: Viestintävastuut, hyväksymiskäytännöt ja sijaisjärjestelyt on dokumentoitu.

Todentava näyttö: viestintäohje, vastuumatriisi, organisaatiokaavio.

2. Onko johdon raportoinnille määritelty sisältö, aikataulu ja vastuuhenkilöt?

Hyväksymiskriteeri: Raportit sisältävät päätöksenteon kannalta olennaiset tiedot ja poikkeamat.

Todentava näyttö: raportointikalenteri, raporttipohjat, toteutuneet raportit.

3. Varmistetaanko raportoitavien tietojen oikeellisuus ennen julkaisemista?

Hyväksymiskriteeri: Tiedot tarkastetaan, hyväksytään ja tarvittaessa täsmäytetään lähdejärjestelmiin.

Todentava näyttö: hyväksymismerkinnät, täsmäytykset, tarkastuslistat.

4. Luokitellaanko viestittävä tieto sen luottamuksellisuuden perusteella?

Hyväksymiskriteeri: Luottamuksellisen tiedon käsittelylle ja jakamiselle on selkeät säännöt.

Todentava näyttö: tiedonluokitteluohje, asiakirjaotos, jakeluoikeudet.

5. [KRIITTINEN] Käytetäänkö luottamuksellisen tiedon välittämiseen hyväksyttyjä ja suojattuja kanavia?

Hyväksymiskriteeri: Arkaluonteisia tietoja ei lähetetä suojaamattomilla tai hyväksymättömillä välineillä.

Todentava näyttö: viestintäohje, tekniset asetukset, lähetysotos.

6. Onko raporttien ja tiedotteiden vastaanottajajoukko rajattu asianmukaisesti?

Hyväksymiskriteeri: Jakelu perustuu työtehtävään ja vastaanottajaluettelot tarkastetaan ennen lähettämistä.

Todentava näyttö: jakelulistat, käyttöoikeudet, lähetysprosessit.

7. Onko kriisi- ja häiriöviestintä suunniteltu?

Hyväksymiskriteeri: Viestintävastuut, kohderyhmät, varakanavat ja hyväksymismenettelyt on määritelty.

Todentava näyttö: kriisiviestintäsuunnitelma, yhteystietoluettelo, viestipohjat.

8. [KRIITTINEN] Onko kriittisten viestintäkanavien toimivuutta testattu?

Hyväksymiskriteeri: Hälytys-, yhteydenpito- ja varaviestintäkanavat testataan säännöllisesti.

Todentava näyttö: testiraportit, harjoitukset, korjaavat toimenpiteet.

9. Korjataanko virheellinen tai vanhentunut tieto hallitusti?

Hyväksymiskriteeri: Korjaukset hyväksytään, vastaanottajille ilmoitetaan ja tarvittaessa virheellinen versio poistetaan.

Todentava näyttö: korjausmerkinnät, versionhallinta, tiedotteet.

10. Säilytetäänkö päätöksenteon ja raportoinnin kannalta olennaiset viestit?

Hyväksymiskriteeri: Säilytys on hallittua, määräaikaista ja hakukelpoista.

Todentava näyttö: arkistointiohje, säilytyskäytäntö, järjestelmäasetukset.

LAADUNHALLINTA JA JATKUVA KEHITTÄMINEN

Auditoinnin tavoite

Selvittää, tunnistetaanko toiminnan laatuun liittyvät vaatimukset ja kehitystarpeet sekä johdetaanko korjaavia ja ehkäiseviä toimenpiteitä järjestelmällisesti.

1. Onko organisaatiolla määritelty laadunhallinnan toimintamalli?

Hyväksymiskriteeri: Laatutavoitteet, vastuut, prosessit ja seuranta on dokumentoitu.

Todentava näyttö: laatupolitiikka, laatukäsikirja, prosessikuvaukset.

2. Ovatko keskeiset prosessit kuvattuja ja omistettuja?

Hyväksymiskriteeri: Prosesseilla on omistajat, tavoitteet, syötteet, tuotokset, vastuut ja mittarit.

Todentava näyttö: prosessikartta, prosessikuvaukset, omistajaluettelo.

3. Onko prosesseille määritelty laadun ja turvallisuuden mittarit?

Hyväksymiskriteeri: Mittarit ovat tarkoituksenmukaisia, luotettavia ja niitä seurataan säännöllisesti.

Todentava näyttö: mittariluettelo, raportit, tavoitearvot.

4. Kerätäänkö asiakas-, henkilöstö- ja sidosryhmäpalautetta?

Hyväksymiskriteeri: Palautteet kirjataan, luokitellaan, käsitellään ja hyödynnetään kehittämisessä.

Todentava näyttö: palauterekisteri, kyselytulokset, käsittelypöytäkirjat.

5. Onko poikkeamien ja laatuhavaintojen ilmoittamiseen yhtenäinen menettely?

Hyväksymiskriteeri: Havainto voidaan ilmoittaa matalalla kynnyksellä ja sille nimetään käsittelijä.

Todentava näyttö: poikkeamajärjestelmä, ilmoitusohje, tapausotos.

6. [KRIITTINEN] Selvitetäänkö merkittävien poikkeamien juurisyyt?

Hyväksymiskriteeri: Merkittävissä tapauksissa tunnistetaan perimmäinen syy eikä korjata vain näkyvää seurausta.

Todentava näyttö: juurisyyanalyysit, tutkintaraportit.

7. Onko korjaaville toimenpiteille määritelty vastuuhenkilöt ja määräajat?

Hyväksymiskriteeri: Toimenpiteet kirjataan, priorisoidaan ja seurataan päätökseen asti.

Todentava näyttö: toimenpiderekisteri, seurantakatselmukset.

8. Arvioidaanko korjaavien toimenpiteiden vaikuttavuus?

Hyväksymiskriteeri: Valmistumisen lisäksi varmistetaan, että toimenpide poisti tai pienensi ongelman.

Todentava näyttö: vaikuttavuusarvioinnit, uusintamittaukset, jälkiauditoinnit.

9. Toteutetaanko sisäisiä auditointeja riskiperusteisen suunnitelman mukaisesti?

Hyväksymiskriteeri: Auditointiohjelma kattaa keskeiset prosessit ja riippumattomuus on varmistettu.

Todentava näyttö: auditointiohjelma, raportit, auditoijien pätevyydet.

10. Käsitteleekö johto laadunhallinnan tulokset säännöllisessä katselmuksessa?

Hyväksymiskriteeri: Johto arvioi tavoitteet, mittarit, poikkeamat, auditoinnit, palautteet ja resurssitarpeet.

Todentava näyttö: johdon katselmuksen pöytäkirja, päätökset ja toimenpiteet.