ISO/IEC 27001:2022 + Amd 1:2024 Tietoturvallisuuden hallintajärjestelmät (ISMS)

Tietoturvallisuus, ISMS, sertifioitavissa maailmanlaajuisesti

181 vaatimusta. Tämän standardin mukainen sertifiointi on mahdollista akkreditoidussa sertifiointielimessä. Versio 07/2026.

ISO/IEC 27001 asettaa vaatimukset tietoturvallisuuden hallintajärjestelmälle: riskiperusteinen, dokumentoitu ja todennettavasti vaikuttava. Arviointi sitä vastaan on akkreditoitu sertifiointiauditointi kahdessa vaiheessa (asiakirjojen katselmointi ja sen jälkeen vaikuttavuuden arviointi paikan päällä), ja sen jälkeen tehdään vuosittaiset seuranta-auditoinnit sekä uudelleensertifiointi kolmen vuoden kuluttua.

Yritys	Päivämäärä	Täyttäjä

4 Organisaation toimintaympäristö 8

4.1-1 Ulkoiset ja sisäiset asiat, jotka vaikuttavat organisaation kykyyn saavuttaa ISMS:n aiotut tulokset, on määritetty ja ne ovat ajan tasalla.

Mistä sen tunnistaa: Näyttönä on toimintaympäristön analyysi joko omana asiakirjanaan tai ISMS-käsikirjan lukuna: markkinatilanne, asiakas- ja sopimustilanne, oikeudellinen kehys (GDPR, NIS2), käytettävät teknologiat, henkilöstömäärä ja riippuvuus pilvipalveluiden tarjoajista. Pienelle yritykselle riittää yhden sivun taulukko, jossa on päiväys ja katselmointiväli, kunhan johdon katselmus osoittaa, että sitä todella päivitetään.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

4.1-2 Organisaatio on määrittänyt, onko ilmastonmuutos sille merkityksellinen asia. Määritys on perusteltu riippumatta siitä, onko vastaus kyllä vai ei.

Mistä sen tunnistaa: Tämä vaatimus tuli mukaan muutoksella Amd 1:2024, ja auditoijat kysyvät sitä erikseen. Toimintaympäristön analyysissä on tälle oma rivinsä: helleajanjaksot ja niiden vaikutus palvelintiloihin ja saatavuuteen, sään ääri-ilmiöiden vaikutus pilvipalveluiden konesaleihin sekä sähköverkon vakaus. Perusteltu lopputulos ei merkityksellinen kelpaa, puuttuva merkintä ei kelpaa.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

4.2-1 ISMS:n kannalta merkitykselliset sidosryhmät on määritetty.

Mistä sen tunnistaa: Sidosryhmäluettelo, joka kattaa asiakkaat, henkilöstön, käsittelijät ja alikäsittelijät, valvontaviranomaiset, vakuuttajat, sertifiointielimen ja omistajat. Pienessä yrityksessä riittää taulukko, jossa on sidosryhmä, odotus ja odotuksen lähde.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

4.2-2 Näiden sidosryhmien merkitykselliset vaatimukset on määritetty, mukaan lukien mahdolliset ilmastonmuutokseen liittyvät vaatimukset.

Mistä sen tunnistaa: Jokaisen sidosryhmän kohdalla mainitaan konkreettinen lähde: sopimusehto, käsittelysopimus, asiakkaan kyselylomake tai lakisääteinen velvoite. Amd 1:2024 lisää huomautuksen, että sidosryhmillä voi olla ilmastonmuutokseen liittyviä vaatimuksia. Kyseessä ei ole erillinen velvoittava vaatimus, mutta auditoijat ottavat sen säännöllisesti esiin, esimerkiksi suuren asiakkaan toimittaja-auditoinnin kestävyyskysymyksinä. Yksi rivi sidosryhmätaulukossa tuloksineen riittää, myös silloin kun tulos on ei tällaisia vaatimuksia.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

4.2-3 On päätetty ja jäljitettävissä, mitkä näistä vaatimuksista hoidetaan ISMS:n kautta.

Mistä sen tunnistaa: Sidosryhmätaulukkoon lisätään sarake, joka osoittaa vaatimuksen hoitavaan sääntöön (politiikka, hallintakeino, sopimusliite). Tämä osoittaa, että vaatimuksia ei ole ainoastaan kerätty vaan myös käsitelty.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

4.3-1 **ISMS:n soveltamisala on määritetty, ja siinä otetaan huomioon kohdan 4.1 asiat, kohdan 4.2 vaatimukset sekä rajapinnat ja riippuvuudet kolmansien osapuolten suorittamiin toimintoihin.**

Mistä sen tunnistaa: Soveltamisala nimeää toimipaikat, organisaatioyksiköt, tuotteet, järjestelmät ja verkon rajat. Ulkoistetut osat (konesalipalvelu, maksunvälittäjät, tuki) kuvataan rajapintoina, joilla on selkeä vastuuraja. Keinotekoisesti kavennettu soveltamisala, joka jättää ydinprosessit ulkopuolelle, hylätään sertifiointielimissä.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

4.3-2 **Soveltamisala on saatavilla dokumentoituna tietona, ja se kertoo ISMS:n rajat yksiselitteisesti.** Asiakirja

Mistä sen tunnistaa: Hyväksytty soveltamisala-asiakirja, jossa on versio, päiväys ja ylimmän johdon hyväksyntä. Sen tarkka sanamuoto siirtyy myöhemmin sertifikaattiin, joten se muotoillaan täsmällisesti ja niin, että sen voi julkaista sellaisenaan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

4.4-1 **ISMS tarvittavine prosesseineen ja niiden vuorovaikutuksineen on laadittu ja otettu käyttöön, sitä ylläpidetään ja sitä parannetaan jatkuvasti.**

Mistä sen tunnistaa: Prosessikartta tai prosessiluettelo, joka yhdistää riskienhallinnan, häiriöiden käsittelyn, muutostenhallinnan, auditoinnin ja johdon katselmuksen omistajineen ja aikaväleineen. Elävä näyttö merkitsee enemmän kuin kaavio: tiketit, pöytäkirjat ja kalenterimerkinnät.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

5 Johtajuus 8

5.1-1 **Ylin johto ottaa vastuun ISMS:n vaikuttavuudesta ja varmistaa, että politiikka ja tavoitteet on laadittu ja että ne sopivat yhteen strategisen suunnan kanssa.**

Mistä sen tunnistaa: Näyttönä on allekirjoitetut hyväksynnät politiikalle, soveltamisalalle ja soveltuvuuslausunnolle, johdon katselmuksen pöytäkirjat sekä dokumentoidut budjettipäätökset. Hyvin pienessä yrityksessä ylin johto on usein sama henkilö kuin ISMS:n omistaja, mikä on hyväksyttävää, mutta se sanotaan avoimesti roolimäärittelyssä.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

5.1-2 **ISMS:n vaatimukset on liitetty osaksi liiketoimintaprosesseja, ja vaikuttavan tietoturvallisuuden merkityksestä viestitään.**

Mistä sen tunnistaa: Parhaiten tämä näkyy siellä, missä tietoturvallisuus ei ole erillinen kansio: tietoturvakriteeri valmiin määritelmässä, tietoturvatarkistus myynti- tai hankintaprosessissa ja toistuva tietoturva-aihe tiimipalaverin muistiossa.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

5.1-3 **Johto antaa tarvittavat resurssit, tukee henkilöitä, jotka edistävät ISMS:n vaikuttavuutta, ja edistää jatkuvaa parantamista.**

Mistä sen tunnistaa: Hyväksytty tietoturvabudjetti, koulutukseen varattu aika sekä ulkopuolisten auditoijien tai tunkeutumistestaajien käyttö. Parantamis- tai toimenpiderekisteri, jossa on merkintöjä usealta vuosineljännekseltä, osoittaa jatkuvuutta kertaponnistuksen sijaan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

5.2-1 **Tietoturvapolitiikka on laadittu, se sopii organisaation tarkoitukseen ja antaa kehyksen tietoturvatavoitteille.** Asiakirja

Mistä sen tunnistaa: Lyhyt hyväksytty politiikka-asiakirja, kaksi tai kolme sivua riittää. Se nimeää suojaustavoitteet, soveltamisalan, vastuut ja riskiperusteisen lähestymistavan periaatteen. Yleinen mallipohjateksti, jolla ei ole yhteyttä todelliseen liiketoimintaan, erottuu auditoinnissa.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

5.2-2 **Politiikka sisältää sitoumuksen täyttää sovellettavat vaatimukset ja sitoumuksen ISMS:n jatkuvaan parantamiseen.** Asiakirja

Mistä sen tunnistaa: Molemmat sitoumukset esiintyvät politiikassa nimenomaisina lauseina, ja ne luetaan sanasta sanaan vaiheen 1 auditoinnissa. Lisäksi viitataan taustalla oleviin prosesseihin (lakirekisteri, parantamisrekisteri).

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

5.2-3 **Politiikasta viestitään organisaation sisällä, ja se on tarvittaessa sidosryhmien saatavilla.** Asiakirja

Mistä sen tunnistaa: Näyttönä voi olla intranetin tai wikin sivu lukuvelvoitteineen, perehdytyksen tarkistuslista kuittauksineen tai verkkosivuilla julkaistu tiivistelmä. Jakelulista kuittauksineen on yksinkertaisin kestävä näyttö.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

5.3-1 **Tietoturvan kannalta merkityksellisten roolien vastuut ja valtuudet on jaettu, ja niistä on viestitty organisaation sisällä.**

Mistä sen tunnistaa: Roolimatriisi (RACI), joka kattaa ISMS:n omistajan, riskien omistajat, suojattavien kohteiden omistajat, häiriöiden koordinaattorin ja tietosuojan yhteyshenkilön. Yhden hengen tai hyvin pienissä tiimeissä jokainen rooli osoitetaan nimetylle henkilölle, ja syntyvä roolien kasautuminen dokumentoidaan avoimesti sen piilottamisen sijaan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

5.3-2 **Valtuus varmistaa ISMS:n standardinmukaisuus ja raportoida ISMS:n suorituskyvystä ylimmälle johdolle on osoitettu tietylle roolille.**

Mistä sen tunnistaa: Nimityskirje tai roolikuvaus ISMS:n omistajalle, ja siinä raportointilinja johdolle on nimenomainen. Raportointilinja osoitetaan käytännössä johdon katselmuksen pöytäkirjoilla.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

6 Suunnittelu 21

6.1.1-1 **Kohdan 4.1 asioista ja kohdan 4.2 vaatimuksista lähtien on määritetty ne riskit ja mahdollisuudet, joihin on tarpeen vastata, jotta ISMS saavuttaa aiotut tuloksensa ja ei-toivotut vaikutukset estetään.**

Mistä sen tunnistaa: Rekisteri, joka yhdistää toimintaympäristön asiat riskeihin ja mahdollisuuksiin, joko erillisenä tai riskirekisterin osana. Ratkaisevaa on jäljitettävyys: jokainen toimintaympäristön analyysin asia johtaa näkyvästi arviointiin tai perusteltuun päätökseen jättää se huomiotta.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

6.1.1-2 **Toimenpiteet näihin riskeihin ja mahdollisuuksiin vastaamiseksi on suunniteltu ja liitetty ISMS:n prosesseihin, ja niiden vaikuttavuus arvioidaan.**

Mistä sen tunnistaa: Toimenpidesuunnitelma, jossa on vastuuhenkilö, määräaika ja vaikuttavuuskriteeri. Vaikuttavuuden arviointi säilytetään omana sarakkeenaan, muuten auditoinnista puuttuu näyttö siitä, että toimenpide on paitsi toteutettu myös todennettu.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

6.1.2-1 **Tietoturvariskien arviointiprosessi on määritelty ja käytössä, ja se sisältää riskin hyväksymiskriteerit sekä kriteerit riskin arviointien tekemiselle.** Asiakirja

Mistä sen tunnistaa: Riskienhallintapolitiikka, jossa on asteikot todennäköisyydelle ja vaikutukselle, määritelty riskimatriisi ja selkeä hyväksymisraja. Raja on luku tai matriisin alue, ei sanamuoto kuten oman harkintamme mukaan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

6.1.2-2 **Prosessi varmistaa, että toistetut riskin arvioinnit tuottavat yhdenmukaisia, päteviä ja vertailukelpoisia tuloksia.**

Mistä sen tunnistaa: Näyttönä on kiinteä menetelmä määriteltyine asteikkoineen ja kahden arviointiversion vertailu: samat riskit, sama luokittelulogiikka ja selitettävissä olevat erot. Viime vuoden riskirekisterin päivätty versio on tässä vahvin näyttö.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.1.2-3 **Tietoturvariskit on tunnistettu, jotta luottamuksellisuuden, eheyden ja saatavuuden menetykset soveltamisalan sisällä havaitaan, ja jokaiselle riskille on osoitettu riskin omistaja.**

Mistä sen tunnistaa: Riskirekisteri, joka viittaa suojattaviin kohteisiin tai prosesseihin, kolmeen suojaustavoitteeseen ja nimettyyn riskin omistajaan. Riskin omistajalla on valtuus hyväksyä riski, ja pienessä yrityksessä tämä on tavallisesti toimitusjohtaja.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.1.2-4 **Tunnistetut riskit on analysoitu: mahdolliset seuraukset, realistinen todennäköisyys ja niistä syntyvä riskitaso on määritetty.**

Mistä sen tunnistaa: Sarakkeet vaikutukselle, todennäköisyydelle ja syntyvälle riskitasolle, kussakin lyhyt perustelu. Yksi perustelulause riskiä kohti estää yleisimmän auditointihavainnon eli luvut ilman päättelyä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.1.2-5 **Riskejä verrataan hyväksymiskriteereihin, ja ne on asetettu käsittelyjärjestykseen.**

Mistä sen tunnistaa: Riskirekisteristä käy ilmi, mitkä riskit ylittävät hyväksymisrajan ja missä järjestyksessä ne käsitellään. Lajiteltu näkymä tai prioriteettisarake riittää.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.1.2-6 **Riskin arviointiprosessi on saatavilla dokumentoituna tietona.** Asiakirja

Mistä sen tunnistaa: Menetelmä itsessään on pakollinen asiakirja, ei ainoastaan sen tuotos. Hyväksytty politiikka, jossa on versio ja hyväksymispäivä, linkitettynä ISMS:n asiakirjaluetteloon.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.1.3-1 **Jokaiselle hyväksymisrajan ylittävälle riskille on valittu sopiva käsittelyvaihtoehto (pienentäminen, välttäminen, siirtäminen tai hyväksyminen).**

Mistä sen tunnistaa: Käsittelyvaihtoehdon sarake riskirekisterissä. Kun riski hyväksytään, kirjataan perustelu ja riskin omistajan muodollinen hyväksyntä, ja kun riski siirretään, nimetään sopimus tai vakuutus.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.1.3-2 **Kaikki hallintakeinot, jotka ovat tarpeen valittujen riskin käsittelyvaihtoehtojen toteuttamiseksi, on määritetty.**

Mistä sen tunnistaa: Hallintakeinot muotoillaan konkreettisesti ja todennettavasti, vastuuhenkilöineen ja määräaikoineen. Viittaus jo käynnissä olevaan tekniseen työhön (MFA:n käyttöönotto, varmuuskopion palautustesti) kelpaa, kunhan se osoittaa tikettiin tai konfiguraatiotuotokseen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.1.3-3 **Määritettyjä hallintakeinoja verrataan liitteen A hallintakeinoihin sen todentamiseksi, ettei tarpeellinen hallintakeino ole jäänyt huomaamatta.**

Mistä sen tunnistaa: Vertailu on erillinen, jäljitettävä vaihe eikä sivutuote. Näyttönä on riskirekisterin kohdistussarake, joka viittaa liitteen A numeroihin, sekä vertailusta laadittu päivätty muistio.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.1.3-4 **Soveltuvuuslausunto (SoA) on olemassa. Siinä arvioidaan kaikki 93 liitteen A hallintakeinoa erikseen, ja siinä ilmoitetaan jokaisen hallintakeinon soveltuvuus perusteluineen, toteutustilanne sekä perustelu jokaiselle poissulkemiselle.** Asiakirja

Mistä sen tunnistaa: Soveltuvuuslausunto on keskeinen pakollinen asiakirja ja koko auditoinnin kartta. Se on kattava: myös ne hallintakeinot, jotka eivät sovellu, esiintyvät siinä perusteluineen eivätkä koskaan tyhjänä rivinä. Suositellut sarakkeet: hallintakeinon numero, otsikko, soveltuu kyllä tai ei, perustelu, toteutustilanne, viittaus politiikkaan tai näyttöön ja yhteys riskiin. Versio ja johdon hyväksyntä ovat pakollisia, koska soveltuvuuslausuntoa verrataan todellisuuteen jokaisessa seuranta-auditoinnissa.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.1.3-5 **Riskin käsittelysuunnitelma on tuotettu, ja se kokoaa yhteen hallintakeinot, vastuut, määräajat ja tarvittavat resurssit.** Asiakirja

Mistä sen tunnistaa: Tämä voi olla riskitaulukon välilehti tai projektitaulu. Ratkaisevaa on, että päivämäärät ovat realistisia ja että ylittyneet määräajat on näkyvästi suunniteltu uudelleen, koska juuri sitä auditoija katsoo.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.1.3-6 **Riskien omistajat ovat hyväksyneet riskin käsittelysuunnitelman ja hyväksyneet muodollisesti jäljelle jäävät jäännösriskit.** Asiakirja

Mistä sen tunnistaa: Allekirjoitus, sähköinen hyväksyntä tai päivätty päätös pöytäkirjassa. Yksi rivi johdon katselmuksen pöytäkirjassa, joka viittaa rekisterin versioon, riittää, kunhan versio on yksiselitteinen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.1.3-7 **Riskin käsittelyprosessi on saatavilla dokumentoituna tietona.** Asiakirja

Mistä sen tunnistaa: Tavallisesti tämä katetaan samassa politiikka-asiakirjassa kuin riskin arviointi. Kulku arvioinnista vaihtoehdon valinnan kautta jäännösriskin hyväksymiseen kuvataan siinä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.2-1 **Tietoturvatavoitteet on laadittu merkityksellisille toiminnoille ja tasoille, ne ovat yhdenmukaisia politiikan kanssa ja ne ovat mitattavia silloin kun se on käytännössä mahdollista.**

Mistä sen tunnistaa: Tavoitetaulukko, jossa on kolmesta kuuteen tavoitetta, kussakin mittari, lähtötaso, tavoitearvo ja määräaika. Esimerkiksi MFA:lla suojattujen järjestelmien osuus nostetaan 80 prosentista 100 prosenttiin vuosineljänneksen loppuun mennessä. Tavoite ilman lukua ei ole mitattava.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.2-2 **Tavoitteissa otetaan huomioon sovellettavat tietoturvavaatimukset sekä riskin arvioinnin ja riskin käsittelyn tulokset.**

Mistä sen tunnistaa: Tavoitetaulukkoon lisätään alkuperäsarake: mistä riskistä, mistä asiakasvaatimuksesta tai mistä lakisääteisestä velvoitteesta tavoite on peräisin. Tämä estää tavoitteet, jotka näyttävät sattumanvaraisilta.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.2-3 **Tavoitteita seurataan, niistä viestitään ja niitä päivitetään tarvittaessa.**

Mistä sen tunnistaa: Neljännesvuosittainen edistymisen seuranta tavoitetaulukossa sekä viestintä tiimille, esimerkiksi lyhyt merkintä wikiin tai kohta tiimipalaverin asialistalla. Aiemmat versiot osoittavat, että päivityksiä todella tehdään.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.2-4 **Tietoturvatavoitteet ovat saatavilla dokumentoituna tietona.** Asiakirja

Mistä sen tunnistaa: Hyväksytty tavoiteasiakirja päiväyksineen riittää. Se voi olla osa johdon katselmusta, mutta siellä se on omana haettavana osionaan.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.2-5 **Jokaisesta tavoitteesta on suunniteltu, mitä tehdään, mitä resursseja tarvitaan, kuka vastaa, milloin se valmistuu ja miten tulokset arvioidaan.**

Mistä sen tunnistaa: Nämä viisi kohtaa ovat erikseen todennettavissa, ja niitä kysytään auditoinnissa erikseen. Ne asetetaan tavoitetaulukkoon viideksi sarakkeeksi, jolloin vaatimustenmukaisuus näkyy yhdellä silmäyksellä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

6.3-1 **Kun organisaatio toteaa, että ISMS:ään tarvitaan muutoksia, muutokset toteutetaan suunnitellulla tavalla.**

Mistä sen tunnistaa: Näyttönä on muutospyynnöt, pöytäkirjat tai tiketit, joista käy ilmi käynnistävä syy, vaikutusten arviointi, hyväksyntä ja toteutus. Tyypillisiä käynnistäviä syitä pienessä yrityksessä ovat pilvipalvelun toimittajan vaihto, uudet toimipaikat ja ensimmäinen palkkaus.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7 Tukitoiminnot 15

7.1-1 **ISMS:n laatimiseen, käyttöönottoon, ylläpitoon ja jatkuvaan parantamiseen tarvittavat resurssit on määritetty ja annettu käyttöön.**

Mistä sen tunnistaa: Tietoturvan budjettirivi, työkalulisenssit (salasanojen hallinta, MDM, lokialusta), suunnitellut henkilötyöpäivät ISMS:n ylläpitoon ja ulkoiset auditointipalvelut. Lasku tai budjetin hyväksyntä osoittaa tämän nopeammin kuin mikään sanallinen kuvaus.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.2-1 **Niiden henkilöiden tarvittava pätevyys, joiden työ vaikuttaa tietoturvallisuuden suorituskykyyn, on määritetty.**

Mistä sen tunnistaa: Pätevyysmatriisi tai rooliprofiilit, joissa luetellaan kussakin roolissa tarvittava osaaminen, esimerkiksi turvallinen kehittäminen kehittäjille ja häiriöiden käsittely koordinaattorille. Hyvin pienissä tiimeissä riittää yksi rivi henkilöä kohti.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.2-2 **Pätevyys varmistetaan soveltuvan koulutuksen, perehdytyksen tai kokemuksen perusteella.**

Mistä sen tunnistaa: Todistukset, kurssivahvistukset, ansioluettelot tai dokumentoitu käytännön kokemus. Itseopiskelu kelpaa, jos siitä on näyttö, esimerkiksi verkkokurssien suoritusmerkinnät tai hyväksytysti suoritetut sisäiset osaamistestit.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.2-3 **Kun pätevyydessä on aukkoja, niiden sulkemiseksi on tehty toimenpiteitä ja näiden toimenpiteiden vaikuttavuus on arvioitu.**

Mistä sen tunnistaa: Koulutussuunnitelma, jossa on tavoitteen ja toteuman vertailu sekä vaikuttavuuden tarkistus, esimerkiksi testin tulos, tietojenkalastelusimulaation klikkausosuus tai havainnointi työn ääressä. Vaikuttavuuden tarkistus unohtuu usein ja on klassinen lievä poikkeama.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.2-4 **Pätevyydestä on näyttönä saatavilla asianmukainen dokumentoitu tieto.** Asiakirja

Mistä sen tunnistaa: Pätevyys- tai koulutuskansio henkilöä kohti, näyttöineen ja päiväyksineen. Pienessä yrityksessä riittää hakemisto, johon PDF-tallenteet on koottu, sekä yhteenvetotaulukko.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.3-1 **Soveltamisalan sisällä työskentelevät henkilöt tuntevat tietoturvapolitiikan.**

Mistä sen tunnistaa: Kuittaus perehdytyksessä ja jokaisen politiikan muutoksen jälkeen, päiväyksineen ja versioineen. Wikin lukukuittaustoiminto tai allekirjoitettu lista riittää.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.3-2 **Henkilöt tietävät oman osuutensa ISMS:n vaikuttavuudessa ja paremman tietoturvallisuuden suorituskyvyn hyödyt.**

Mistä sen tunnistaa: Koulutusaineisto ja osallistujalistat, joissa yhteys henkilön omaan työhön näkyy. Auditoijat haastattelevat henkilöstöä suoraan, joten koulutus rakennetaan konkreettisille arjen esimerkeille eikä abstrakteille standardin lainauksille.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.3-3 **Henkilöt tietävät, mitä seuraa ISMS:n vaatimusten noudattamatta jättämisestä.**

Mistä sen tunnistaa: Seuraukset kerrotaan koulutusaineistossa ja työohjeissa ja liitetään kohdan A.6.4 menettelyyn. Myös yritys ilman työntekijöitä kattaa tämän alihankkijoiden ja freelancereiden osalta sopimuksin.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.4-1 **ISMS:n kannalta merkityksellinen sisäinen ja ulkoinen viestintä on määritetty: mistä viestitään, milloin, kenen kanssa ja millä keinoin.**

Mistä sen tunnistaa: Viestintämatriisi, jossa on rivejä kuten tietoturvahäiriö asiakkaille, ilmoitus valvontaviranomaiselle 72 tunnin kuluessa ja kuukausittainen tilanneraportti johdolle. Se on kriisiviestinnän perusta, ja se katselmoidaan jokaisen häiriön jälkeen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.5.1-1 **ISMS sisältää standardin edellyttämän dokumentoidun tiedon sekä sen dokumentoidun tiedon, jonka organisaatio on määrittänyt tarpeelliseksi ISMS:n vaikuttavuuden kannalta.** Asiakirja

Mistä sen tunnistaa: Asiakirjaluettelo, jossa on jokainen ISMS:n asiakirja tarkoituksineen, omistajineen, versioineen ja säilytyspaikkoineen. Se osoittaa, ettei pakollisista asiakirjoista puutu mitään, ja se on auditoijalle nopein sisäänkäynti.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.5.2-1 **Asiakirjoja luotaessa ja päivitettäessä varmistetaan asianmukainen tunnistetieto, muoto ja tallennusväline, ja asiakirjat katselmoidaan ja hyväksytään soveltuvuuden osalta.**

Mistä sen tunnistaa: Yhtenäinen asiakirjaotsake, jossa on otsikko, versio, päiväys, laatija ja hyväksyjä. Gitiin perustuvissa ympäristöissä muutospyyntöjen katselmoinnit hyväksyntöineen täyttävät katselmointi- ja hyväksyntävaatimuksen, kunhan historia on muuttumaton.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.5.3-1 **Tarvittava dokumentoitu tieto on saatavilla ja käyttökelpoista siellä ja silloin, kun sitä tarvitaan.**

Mistä sen tunnistaa: Keskitetty tallennuspaikka, johon jokainen siihen oikeutettu pääsee, hakutoimintoineen. Tämä on testattavissa otannalla: mikä tahansa työohje löytyy alle minuutissa.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.5.3-2 **Dokumentoitu tieto on riittävästi suojattu erityisesti luottamuksellisuuden menetystä, asiatonta käyttöä ja eheyden menetystä vastaan.**

Mistä sen tunnistaa: Roolipohjaiset käyttöoikeudet ISMS:n asiakirjoihin, versiointi historioineen, kirjoitussuojaus hyväksytyille versioille ja asiakirjavaraston varmuuskopio. Varmuuskopion näyttö unohtuu useimmin.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.5.3-3 **Jakelu, pääsy, haku, tallennus, muutostenhallinta sekä dokumentoidun tiedon säilytysajat ja hävittäminen on ohjeistettu.**

Mistä sen tunnistaa: Lyhyt asiakirjahallinnan sääntö säilytysaikoineen ja poistosääntöineen. Se sovitetaan yhteen lakisääteisten velvoitteiden kanssa (kauppaoikeus, verolainsäädäntö, GDPR), ja se on perusta kohdille A.5.33 ja A.8.10.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7.5.3-4 **Ulkoista alkuperää oleva dokumentoitu tieto, joka on tarpeen ISMS:n suunnittelussa ja käytössä, on tunnistettu ja hallinnassa.**

Mistä sen tunnistaa: Luettelo ulkoisista asiakirjoista versioineen ja lähteineen: standardit, säädöstekstit, toimittajien kovennusohjeet, pilvipalveluiden tietoturvadokumentaatio ja käsittelysopimukset. Ilman versiotietoa hallintaa ei voi osoittaa.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

8 Toiminta 8

8.1-1 **Prosessit, joita tarvitaan tietoturvavaatimusten täyttämiseen ja kohdan 6 toimenpiteiden toteuttamiseen, on suunniteltu ja otettu käyttöön, niitä ohjataan, ja näille prosesseille on laadittu kriteerit.**

Mistä sen tunnistaa: Toimintakäsikirja tai ajo-ohjeet selkeine kriteereineen, esimerkiksi kriittisten korjauspäivitysten enimmäisasennusaika, julkaisukriteerit käyttöönotoille ja hälytysrajat. Kriteerit ilman lukuja ovat auditoinnissa arvottomia.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

8.1-2 **Prosessien suunnitelmanmukaisesta toteutumisesta on dokumentoitua tietoa siinä laajuudessa, että toteutumaan voi luottaa.** Asiakirja

Mistä sen tunnistaa: Näyttönä on toiminnan tallenteet: tikettihistoria, CI-putken ajot, korjauspäivitysraportit, varmuuskopiolokit ja käyttöoikeuksien katselmoinnit. Nämä tallenteet ovat vaiheen 2 auditoinnissa varsinainen näyttö vaikuttavuudesta.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

8.1-3 **Suunniteltuja muutoksia ohjataan ja tahattomien muutosten seuraukset katselmoidaan, ja tarvittaessa haitallisia vaikutuksia lievennetään.**

Mistä sen tunnistaa: Muutosprosessi hyväksyntöineen ja peruutuspolkuineen, liitettynä kohtaan A.8.32. Tahattomista muutoksista (virheellinen konfiguraatio, vahingossa laajentuneet oikeudet) dokumentoidaan häiriö ja osoitetaan korjaus.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

8.1-4 **Ulkoisesti tuotetut prosessit, tuotteet ja palvelut, jotka ovat ISMS:n kannalta merkityksellisiä, on määritetty ja ne ovat hallinnassa.**

Mistä sen tunnistaa: Toimittajaluettelo, jossa on kriittisyys, sopimusviite ja näytön tila (toimittajan ISO 27001 -sertifikaatti, SOC 2 -raportti, käsittelysopimus). Pienelle yritykselle tämä on suurin vipu, koska suurin osa tietotekniikasta pyörii joka tapauksessa ulkopuolella.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

8.2-1 **Riskin arvioinnit tehdään suunnitelluin väliajoin sekä aina merkittävien muutosten tai häiriöiden yhteydessä, laaditut kriteerit huomioon ottaen.**

Mistä sen tunnistaa: Rytmi (tyypillisesti vuosittain) sekä määritellyt käynnistävät syyt ylimääräisille arvioinneille. Näyttönä on riskirekisterin päivätyt versiot ja merkinnät kalenterissa tai tikettijärjestelmässä.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

8.2-2 **Riskin arviointien tulokset säilytetään dokumentoituna tietona.** Asiakirja

Mistä sen tunnistaa: Riskirekisterin aiemmat versiot päiväyksineen, ei ainoastaan nykytilaa. Tiedoston ylikirjoittaminen tekee kehityksen osoittamisen mahdottomaksi, ja versiointi tiedostojärjestelmässä tai Gitissä ratkaisee tämän.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

8.3-1 **Riskin käsittelysuunnitelma on toteutettu.**

Mistä sen tunnistaa: Suunnitelmaa verrataan todellisuuteen: valmiit toimenpiteet toteutuspäivineen ja konkreettisine tuotoksineen (konfiguraatio, politiikka, sopimus). Avoimet toimenpiteet tarvitsevat dokumentoidun perustelun ja uuden tavoitepäivän.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

8.3-2 **Riskin käsittelyn tulokset säilytetään dokumentoituna tietona.** Asiakirja

Mistä sen tunnistaa: Tilanneraportit tai suljetut toimenpiteet viittauksineen näyttöön. Pelkkä rekisteri riittää, jos jokaisella rivillä on valmistumispäivä ja linkki näyttöön.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

9 Suorituskyvyn arviointi 21

9.1-1 **On määritetty, mitä seurataan ja mitataan, mukaan lukien tietoturvaprosessit ja hallintakeinot.**

Mistä sen tunnistaa: Mittaritaulukko, jossa on hallittava määrä kestäviä mittareita: korjauspäivitysten jono, MFA:n kattavuus, häiriöiden ratkaisuaika, viimeisimmän palautustestin tulos ja avoimet havainnot. Muutama mittari, joita todella kerätään, voittaa pitkän toivelistan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

9.1-2 **Seurannan, mittauksen, analysoinnin ja arvioinnin menetelmät on määritelty, ja ne tuottavat päteviä tuloksia.**

Mistä sen tunnistaa: Jokaisesta mittarista kirjataan tietolähde ja laskentatapa, esimerkiksi vienti haavoittuvuusskannerista tai identiteetinhallinnan raportista. Lähteen jäljitettävyys on tulosten paikkansapitävyyden ydin.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.1-3 **On määritelty, milloin seuranta ja mittaus tehdään ja kuka ne tekee, sekä milloin tulokset analysoidaan ja arvioidaan.**

Mistä sen tunnistaa: Mittaritaulukkoon lisätään sarakkeet aikavälille ja vastuuhenkilölle. Toistuva kalenterivaraus arviointia varten osoittaa säännöllisyyden paremmin kuin mikään kuvaus.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.1-4 **Seurannan ja mittauksen tulokset säilytetään dokumentoituna tietona.** Asiakirja

Mistä sen tunnistaa: Arkistoidut arvioinnit, viedyt koontinäytöt tai mittaritaulukko, jota ylläpidetään aikasarjana. Reaaliaikainen näkymä ilman historiaa ei täytä vaatimusta.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.1-5 **Tietoturvallisuuden suorituskyky ja ISMS:n vaikuttavuus arvioidaan mittaustulosten perusteella.**

Mistä sen tunnistaa: Kirjallinen arviointi eikä pelkkiä lukuja: suuntaus, syyt ja toimenpidetarve. Tämä arviointiteksti on samalla johdon katselmuksen lähtötieto.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.2.1-1 **Sisäiset auditoinnit tehdään suunnitelluin väliajoin, ja ne antavat tietoa siitä, täyttääkö ISMS organisaation omat vaatimukset ja standardin vaatimukset ja onko se toteutettu vaikuttavasti.**

Mistä sen tunnistaa: Ennen sertifiointiauditointia on saatettu päätökseen vähintään yksi täysi sisäisen auditoinnin kierros, joka kattaa koko soveltamisalan. Ilman sitä sertifiointi jää saavuttamatta, ja tämä on yksi yleisimmistä kompastuskivistä ensimmäisissä sertifioinneissa.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.2.2-1 **Auditointiohjelma on suunniteltu ja laadittu ja sitä ylläpidetään, se määrittelee aikavälit, menetelmät, vastuut, suunnitteluvaatimukset ja raportoinnin, ja siinä otetaan huomioon kyseessä olevien prosessien merkitys ja aiempien auditointien tulokset.**

Mistä sen tunnistaa: Monivuotinen auditointiohjelma, joka kattaa kaikki standardin kohdat ja kaikki soveltuvat hallintakeinot sertifiointijakson aikana ja jossa kriittiset alueet auditoidaan useammin. Yksinkertainen kolmen vuoden taulukko riittää täysin.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.2.2-2 **Auditointikriteerit ja auditoinnin laajuus on määritelty jokaiselle auditoinnille.**

Mistä sen tunnistaa: Auditointisuunnitelma kutakin ajankohtaa kohti, kriteereineen (standardi, sisäiset politiikat, sopimukset) ja selkeine laajuuksineen. Yhden sivun auditointisuunnitelma auditointia kohti riittää ja toimii samalla raportin pohjana.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.2.2-3 **Auditoijat valitaan ja auditoinnit tehdään tavalla, joka varmistaa objektiivisuuden ja puolueettomuuden. Kukaan ei auditoi omaa työtään.**

Mistä sen tunnistaa: Riippumattomuus on tässä kova este: se, joka on kirjoittanut politiikat ja konfiguroinut järjestelmät, ei auditoi niitä. Hyvin pienessä yrityksessä tämä tarkoittaa lähes aina ulkopuolista sisäistä auditoijaa, esimerkiksi sopimuskonsulttia tai kollegaa kumppaniyrityksestä, ja näyttönä on auditointisopimus sekä auditoijan riippumattomuusvakuutus. Vasta riittävän suurissa tiimeissä rooli voidaan kierrättää sisäisesti henkilölle, jolla ei ole vastuuta auditoitavasta alueesta, ja se osoitetaan silloin roolimatriisissa.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

9.2.2-4 **Auditoinnin tulokset raportoidaan asianomaiselle johdolle.**

Mistä sen tunnistaa: Auditointiraportti havaintoineen, poikkeamineen, suosituksineen ja jakelulistoineen sekä näyttö luovutuksesta johdolle, esimerkiksi pöytäkirjaan merkitty kohta tai päivätty luovutus sähköpostitse.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

9.2.2-5 **Auditointiohjelmasta ja auditoinnin tuloksista säilytetään dokumentoitu tieto.** Asiakirja

Mistä sen tunnistaa: Auditointiohjelma, auditointisuunnitelmat, auditointiraportit ja niistä syntyneet toimenpiteet säilytetään yhdessä paikassa. Yhteys havainnosta korjaavaan toimenpiteeseen (kohta 10.2) näkyy päästä päähän.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

9.3.1-1 **Ylin johto katselmoi ISMS:n suunnitelluin väliajoin varmistaakseen sen jatkuvan soveltuvuuden, riittävyyden ja vaikuttavuuden.**

Mistä sen tunnistaa: Vähintään kerran vuodessa ja ajoitettuna ennen ulkoista auditointia. Myös hyvin pienessä yrityksessä laaditaan päivätty ja allekirjoitettu pöytäkirja, silloinkin kun johto ja ISMS:n omistaja ovat sama henkilö.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

9.3.2-1 **Johdon katselmuksessa käsitellään aiempien johdon katselmusten toimenpiteiden tilanne.**

Mistä sen tunnistaa: Pöytäkirja alkaa seurantataulukolla, jossa on viime vuoden päätökset ja niiden nykytila. Ilman tätä takaisinviittausta katselmus katsotaan puutteelliseksi.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

9.3.2-2 **Johdon katselmuksessa käsitellään ISMS:n kannalta merkityksellisten ulkoisten ja sisäisten asioiden muutokset, mukaan lukien ilmastonmuutoksen merkitykselliset näkökohdat.**

Mistä sen tunnistaa: Oma asialistan kohta, joka viittaa päivitettyyn toimintaympäristön analyysiin. Ilmastonmuutosta ei mainita nimeltä tämän kohdan tekstissä (Amd 1:2024 muuttaa vain kohtia 4.1 ja 4.2), mutta se kulkeutuu tänne kohdan 4.1 asioiden muutosten kautta, ja auditoijat odottavat sitä. Myös tulos ei merkityksellinen, ei muutoksia kuuluu pöytäkirjaan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

9.3.2-3 **Johdon katselmuksessa käsitellään ISMS:n kannalta merkityksellisten sidosryhmien tarpeiden ja odotusten muutokset.**

Mistä sen tunnistaa: Uudet asiakasvaatimukset sopimuksista ja tietoturvakyselyistä, uudet lakisääteiset velvoitteet ja sertifiointielimen vaatimukset. Ne kirjataan pöytäkirjaan luettelona lähteineen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

9.3.2-4 **Johdon katselmuksessa käsitellään palaute tietoturvallisuuden suorituskyvystä, mukaan lukien poikkeamat ja korjaavat toimenpiteet, seurannan ja mittauksen tulokset, auditointien tulokset sekä tietoturvatavoitteiden toteutuminen.**

Mistä sen tunnistaa: Nämä neljä lohkoa käsitellään erillisinä asialistan kohtina, muuten yksi niistä puuttuu myöhemmin pöytäkirjasta. Mittaritaulukko, auditointiraportti ja tavoitetaulukko liitetään pöytäkirjaan liitteiksi.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.3.2-5 **Johdon katselmuksessa käsitellään sidosryhmiltä saatu palaute.**

Mistä sen tunnistaa: Tietoturvaan liittyvät asiakkaiden reklamaatiot, asiakasauditointien tulokset, ilmoituskanavan ilmoitukset ja palveluntuottajien palaute. Tämä kirjataan pöytäkirjaan myös silloin, kun havainto on, ettei niitä ole tullut.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.3.2-6 **Johdon katselmuksessa käsitellään riskin arvioinnin tulokset ja riskin käsittelysuunnitelman tilanne.**

Mistä sen tunnistaa: Liitteinä ovat ajantasainen riskirekisteri ja käsittelysuunnitelman toteutustilanne sekä riskien omistajien nimenomainen vahvistus jäännösriskien hyväksymisestä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.3.2-7 **Johdon katselmuksessa käsitellään jatkuvan parantamisen mahdollisuudet.**

Mistä sen tunnistaa: Asialistan kohta, jossa on konkreettisia parantamisideoita ja päätös kustakin. Hyväksytyt ideat siirtyvät parantamisrekisteriin merkinnöiksi määräaikoineen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.3.3-1 **Johdon katselmuksen tuloksiin sisältyvät päätökset jatkuvan parantamisen mahdollisuuksista ja mahdollisesta tarpeesta muuttaa ISMS:ää.**

Mistä sen tunnistaa: Pöytäkirja päättyy päätösosioon: päätös, vastuuhenkilö ja määräaika. Pöytäkirja ilman päätöksiä on auditoinnissa havainto, koska johtamisvaikutus jää silloin puuttumaan.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9.3.3-2 **Johdon katselmuksen tuloksista säilytetään näyttönä dokumentoitu tieto.** Asiakirja

Mistä sen tunnistaa: Allekirjoitettu pöytäkirja, jossa on päiväys, osallistujat, lähtötiedot, arviointi ja päätökset. Se on yksi ensimmäisistä asiakirjoista, joita sertifiointielin pyytää vaiheessa 1.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

10 Parantaminen 7

10.1-1 **ISMS:n soveltuvuutta, riittävyyttä ja vaikuttavuutta parannetaan jatkuvasti.**

Mistä sen tunnistaa: Parantamisrekisteri, joka saa syötteensä useasta lähteestä (auditoinnit, häiriöt, ideat, mittarien poikkeamat) ja jossa edistyminen näkyy ajan myötä. Näyttönä on jatkuvuus usean kuukauden yli, ei merkintöjen lukumäärä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

10.2-1 **Kun poikkeama ilmenee, organisaatio reagoi siihen: se ottaa poikkeaman haltuun, korjaa sen ja hoitaa seuraukset.**

Mistä sen tunnistaa: Poikkeamaraportti välittömine toimenpiteineen ja päiväyksineen. Lähteitä ovat sisäiset auditoinnit, ulkoiset auditoinnit, häiriöt ja arjen havainnot, ja ne kaikki syöttävät samaa rekisteriä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

10.2-2 **On arvioitu, tarvitaanko toimenpiteitä syiden poistamiseksi, jotta poikkeama ei toistu eikä ilmene muualla, ja tähän sisältyy sen selvittäminen, onko vastaavia poikkeamia olemassa tai voisiko niitä ilmetä.**

Mistä sen tunnistaa: Juurisyyanalyysi dokumentoidaan, esimerkiksi 5 Why tai Ishikawa, ja lisäksi kirjataan nimenomainen kannanotto siirrettävyydestä muihin järjestelmiin tai prosesseihin. Siirrettävyyden vaihe jää useimmin väliin.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

10.2-3 **Tarvittavat korjaavat toimenpiteet on toteutettu ja niiden vaikuttavuus katselmoidaan.**

Mistä sen tunnistaa: Jokaisesta toimenpiteestä kirjataan toteutuspäivä, näyttötuotos ja myöhempi vaikuttavuuden katselmointi omine päiväyksineen. Kaksi päivämääräkenttää riviä kohti on yksinkertaisin tapa olla kadottamatta vaikuttavuuden katselmointia.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

10.2-4 **Tarvittaessa ISMS:ään tehdään muutoksia poikkeaman seurauksena.**

Mistä sen tunnistaa: Jos poikkeama juontuu aukosta politiikassa, riskirekisterissä tai soveltuvuuslausunnossa, muutos näkyy siellä. Viittaus poikkeamasta päivitettyyn asiakirjaversioon sulkee ketjun.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

10.2-5 **Korjaavat toimenpiteet ovat oikeassa suhteessa havaittujen poikkeamien vaikutuksiin.**

Mistä sen tunnistaa: Rekisterissä on vakavuusluokitus, josta toimenpiteen oikeasuhtaisuus käy ilmi. Vähäpätöistä asiaa ei hoideta projektina eikä vakavaan poikkeamaan vastata pelkällä muistutussähköpostilla.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

10.2-6 **Poikkeamien luonteesta, niiden johdosta tehdyistä toimenpiteistä ja korjaavien toimenpiteiden tuloksista säilytetään dokumentoitu tieto.** Asiakirja

Mistä sen tunnistaa: Poikkeamien ja korjaavien toimenpiteiden rekisteri, jossa on sarakkeet luonteelle, syylle, toimenpiteelle, vastuuhenkilölle, määräajalle ja vaikuttavuuden katselmoinnin tulokselle. Se on pakollinen näyttö, ja se otetaan esiin jokaisessa seuranta-auditoinnissa.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5 Liite A: Organisatoriset hallintakeinot 37

A.5.1 **Tietoturvapolitiikat: Kattava tietoturvapolitiikka ja aihekohtaiset politiikat on määritelty, johto on hyväksynyt ne, niistä on viestitty, ja ne katselmoidaan suunnitelluin väliajoin ja aina merkittävien muutosten yhteydessä.** Asiakirja

Mistä sen tunnistaa: Politiikkakokonaisuus, jossa on versio, hyväksymispäivä ja seuraava katselmointipäivä, sekä näyttö kuittauksista. Pienelle yritykselle riittää kehyspolitiikka ja kourallinen aihekohtaisia politiikkoja (pääsy, salaus, etätyö, häiriöt).

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.2 **Tietoturvaroolit ja vastuut: Tietoturvaroolit ja vastuut on määritelty ja jaettu organisaation tarpeiden mukaan.**

Mistä sen tunnistaa: Roolimatriisi nimineen, sijaisineen ja tehtävineen. Hyvin pienessä yrityksessä kerrotaan avoimesti, missä useita rooleja kasautuu yhdelle henkilölle, ja tämä liitetään kohdan A.5.3 korvaaviin hallintakeinoihin.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.3 **Tehtävien eriyttäminen: Tehtävät ja vastuualueet, joiden on tarkoitus valvoa toisiaan, eivät ole yhden henkilön hallussa. Tavoitteena on, ettei kukaan voi yksin käynnistää, hyväksyä ja peittää muutosta.**

Mistä sen tunnistaa: Pienessä yrityksessä täysi eriyttäminen on rakenteellisesti mahdotonta, ja kattava väite vaatimustenmukaisuudesta romahtaa heti auditointihaastattelussa. Kestävää on rehellinen analyysi: mitkä tehtäväyhdistelmät ovat kriittisiä (kehittäminen ja julkaisu, oikeuksien myöntäminen ja niiden käyttö, maksujen käynnistäminen ja hyväksyminen), mitkä niistä ovat yhdellä henkilöllä ja mitkä korvaavat hallintakeinot ovat käytössä. Toimiviksi osoittautuneita ovat muuttumattomat auditointilokit, joihin kolmas osapuoli pääsee, MFA korotetun oikeuden tileillä, automaattiset CI-portit ja haarasuojaus nelisilmäperiaatteen sijaan, ulkopuolisen henkilön säännöllinen lokien katselmointi sekä erillinen hyväksyntä maksuille. Analyysi ja korvaavat hallintakeinot säilytetään omana päivättynä asiakirjanaan, ja siihen linkitetään soveltuvuuslausunnosta.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.4 **Johdon vastuut: Johto edellyttää koko henkilöstöltä tietoturvallisuuden soveltamista laadittujen politiikkojen ja menettelyjen mukaisesti.**

Mistä sen tunnistaa: Sitoumus työ- ja toimeksiantosopimuksissa, politiikkojen kuittaus perehdytyksessä ja johdon säännölliset muistutukset. Näyttönä on allekirjoitetut sitoumukset ja palaverien muistiot.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.5 **Yhteydenpito viranomaisiin: Asianmukaisia yhteyksiä merkityksellisiin viranomaisiin ylläpidetään, ja ne tavoitetaan tarvittaessa.**

Mistä sen tunnistaa: Yhteystietoluettelo, jossa on toimivaltainen tietosuojaviranomainen, poliisi tai kyberrikosyksikkö, kansallinen kyberturvallisuuden ilmoituspiste ja soveltamisalan niin vaatiessa NIS2-ilmoituskanavat. Määräajat (kuten GDPR:n 72 tuntia) merkitään suoraan luetteloon.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.6 **Yhteydenpito erityisryhmiin: Yhteyksiä erityisryhmiin, tietoturvafoorumeihin ja ammatillisiin yhdistyksiin ylläpidetään.**

Mistä sen tunnistaa: Jäsenyydet, tilatut tiedotteet (kansallinen CERT, toimittajien syötteet) ja osallistuminen erityisryhmiin. Yksinkertainen näyttö on luettelo tilauksista sekä yksi esimerkki siitä, miten tiedote johti toimenpiteeseen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.7 **Uhkatiedustelu: Tietoa tietoturvauhkista kerätään ja analysoidaan, jotta siitä johdetaan asianmukaisia toimenpiteitä.**

Mistä sen tunnistaa: Uutta vuoden 2022 laitoksessa. Pienelle yritykselle toimiva tapa on tilata kansallisen CERTin ja toimittajien tiedotteet ja tehdä sen jälkeen lyhyt kuukausittainen katselmointi, jossa päätetään merkityksellisyydestä ja josta johdetaan tiketit. Näyttönä on analyysi eikä tilaus.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.8 **Tietoturvallisuus projektinhallinnassa: Tietoturvallisuus on liitetty osaksi projektinhallintaa projektin tyypistä riippumatta.**

Mistä sen tunnistaa: Tietoturvakohdat projektin tarkistuslistassa: suojaustarpeet, riskin katselmointi, tietosuojatarkistus ja tietoturvahyväksyntä ennen tuotantoon siirtoa. Ketterissä tiimeissä ne ankkuroidaan kiinteiksi kohdiksi aloitusvalmiuden ja valmiin määritelmään.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.9 **Tiedon ja muiden suojattavien kohteiden luettelo: Luettelo tiedosta ja muista siihen liittyvistä suojattavista kohteista nimettyine omistajineen on laadittu ja sitä ylläpidetään.**

Mistä sen tunnistaa: Suojattavien kohteiden luettelo, joka kattaa laitteet, ohjelmistot, pilvipalvelut, tietovarastot, verkkotunnukset ja tilit, kunkin omistajineen ja suojaustarpeineen. Pienessä yrityksessä sen voi koota automaattisesti MDM-viennistä, lisenssiluettelosta ja pilvipalvelun hallintanäkymästä, ja ajantasainen päiväys on pakollinen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.5.10 **Tiedon ja muiden suojattavien kohteiden hyväksyttävä käyttö: Säännöt tiedon ja muiden siihen liittyvien suojattavien kohteiden hyväksyttävästä käytöstä ja käsittelystä on tunnistettu, dokumentoitu ja otettu käyttöön.** Asiakirja

Mistä sen tunnistaa: Hyväksyttävän käytön politiikka laitteille, verkoille, pilvitileille ja tekoälytyökaluille, kuittauksineen. Henkilökohtaiset laitteet ja ulkoiset tekoälypalvelut katetaan nimenomaisesti, koska juuri siellä vuotaa eniten.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.5.11 **Suojattavien kohteiden palautus: Kun työsuhde päättyy tai muuttuu, on ohjeistettu ja kirjallisesti vahvistettu, että kaikki luovutetut laitteet, avaimet, tilit ja asiakirjat palautetaan.**

Mistä sen tunnistaa: Lähtöprosessin tarkistuslista, jossa on palautuskuittaus kannettavalle, tunnistautumisvälineille, avaimille, varmenteille ja tallennusvälineille, sekä tilien sulkeminen samana päivänä. Tämä koskee yhtä lailla freelancereita ja harjoittelijoita.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.5.12 **Tiedon luokittelu: Tieto luokitellaan sen suojaustarpeiden mukaan luottamuksellisuuden, eheyden, saatavuuden ja lakisääteisten vaatimusten osalta.**

Mistä sen tunnistaa: Yksinkertainen malli, jossa on kolme tai neljä tasoa (julkinen, sisäinen, luottamuksellinen, erittäin luottamuksellinen) ja konkreettiset käsittelysäännöt kullekin tasolle. Luokittelu kirjataan suojattavien kohteiden luetteloon tai käsittelytoimien selosteeseen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.5.13 **Tiedon merkitseminen: Luokitustaso on tunnistettavissa itse asiakirjasta, tiedostosta tai viestistä, jotta vastaanottaja tietää käsittelytavan kysymättä.**

Mistä sen tunnistaa: Merkintä asiakirjan otsakkeessa, tiedostonimessä, sähköpostin aiheessa tai pilvitoimisto-ohjelmiston luottamuksellisuusmerkintöinä. Näyttönä on otokset todella merkityistä asiakirjoista eikä pelkkä sääntö.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.5.14 **Tiedon siirto: Säännöt, menettelyt ja sopimukset tiedon siirtämisestä organisaation sisällä ja ulkoisten osapuolten kanssa ovat olemassa.**

Mistä sen tunnistaa: Sääntö siitä, mikä kanava on sallittu millekin luokitustasolle: salattu sähköposti tai tietohuone luottamukselliselle sisällölle, ei lähetystä yksityisten pikaviestimien kautta. Luottamukselliset siirrot varmistetaan salassapitosopimuksin.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.5.15 **Pääsynhallinta: Säännöt fyysisen ja loogisen pääsyn hallitsemiseksi tietoon ja muihin siihen liittyviin suojattaviin kohteisiin on laadittu ja otettu käyttöön liiketoiminnan ja tietoturvan vaatimusten pohjalta.**

Mistä sen tunnistaa: Pääsynhallintapolitiikka, joka noudattaa tarveperusteisuutta ja vähimmän oikeuden periaatetta, sekä roolien ja oikeuksien kohdistus. Näyttönä on todellinen oikeuksien konfiguraatio identiteetinhallinnassa eikä pelkkä politiikka.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.5.16 **Identiteetin hallinta: Identiteettien koko elinkaari on hallinnassa.**

Mistä sen tunnistaa: Prosessi luonnista muutoksen kautta käytöstä poistoon, mieluiten keskitettynä identiteetinhallintaan ja kertakirjautumiseen. Jaettuja ryhmätilejä ei käytetä, ja jos se on teknisesti väistämätöntä, tili nimetään, perustellaan ja sen käyttö lokitetaan.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.17 **Todentamistiedot: Todentamistietojen jakamista ja hallintaa ohjaa hallintaprosessi, joka edellyttää henkilöiltä niiden asianmukaista käsittelyä.**

Mistä sen tunnistaa: Salasanojen hallintaohjelma pakollisena työkaluna, politiikka salasanojen laadusta ja MFA:sta, turvallinen ensimmäinen kirjautuminen sekä nollausmenettely henkilöllisyyden todentamisineen. Näyttönä on konfiguraation näyttökuvat ja salasanojen hallintaohjelman raportti.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.18 **Käyttöoikeudet: Käyttöoikeudet myönnetään, katselmoidaan, muutetaan ja poistetaan pääsynhallintapolitiikan mukaisesti.**

Mistä sen tunnistaa: Säännöllinen käyttöoikeuksien katselmointi vähintään kerran vuodessa, dokumentoituine tuloksineen tiliä kohti ja näyttöineen poistetuista oikeuksista. Oikeuksien poisto lähtöpäivänä on kohta, jonka auditoijat jäljittävät mielellään konkreettisen tapauksen kautta.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.19 **Tietoturvallisuus toimittajasuhteissa: Prosessit ja menettelyt kolmansien osapuolten tuotteiden ja palvelujen käytöstä syntyvien tietoturvariskien hallitsemiseksi on määritelty ja otettu käyttöön.**

Mistä sen tunnistaa: Toimittajaluettelo, jossa on kriittisyystaso ja arvioinnin syvyys. Kriittisiltä toimittajilta hankitaan näyttö (ISO 27001 -sertifikaatti, SOC 2 -raportti) omien auditointien sijaan, mikä on pienelle yritykselle ainoa realistinen reitti.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.20 **Tietoturvallisuuden käsittely toimittajasopimuksissa: Merkitykselliset tietoturvavaatimukset on sovittu jokaisen toimittajan kanssa ja kirjattu sopimuksiin.**

Mistä sen tunnistaa: Tietoturvallisuuden sopimusliite, jossa on häiriöiden ilmoitusvelvollisuudet, alikäsittelijöitä koskevat säännöt, poistovelvoitteet ja auditointioikeudet. Vakiopalveluissa toimittajan ehdot ja käsittelysopimus riittävät, kunhan niiden sisältö on katselmoitu ja dokumentoitu.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.21 **Tietoturvallisuuden hallinta ICT-toimitusketjussa: Prosessit tieto- ja viestintätekniikan toimitusketjun tietoturvariskien hallitsemiseksi on määritelty ja otettu käyttöön.**

Mistä sen tunnistaa: Tämä kattaa ohjelmistoriippuvuudet ja toimittajien omat alihankkijat. Käytännössä tämä tarkoittaa ohjelmiston osaluetteloa (SBOM) tai riippuvuusluetteloa, automaattisia tarkistuksia haavoittuvista paketeista CI-putkessa ja ohjelmistojen hankintaa vain allekirjoitetuista tai virallisista kanavista.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.22 **Toimittajapalvelujen seuranta, katselmointi ja muutostenhallinta: Toimittajapalvelujen muutoksia seurataan, katselmoidaan ja hallitaan säännöllisesti.**

Mistä sen tunnistaa: Vuosittainen toimittaja-arviointi, jossa käydään läpi häiriöt, saatavuusraportit ja sertifikaattien voimassaolo, sekä kanava toimittajan muutosilmoituksille. Tulos kirjataan lyhyeksi muistiinpanoksi toimittajaa kohti.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.23 **Tietoturvallisuus pilvipalvelujen käytössä: Prosessit pilvipalvelujen hankkimiseen, käyttöön, hallintaan ja käytöstä luopumiseen on laadittu tietoturvavaatimusten mukaisesti.**

Mistä sen tunnistaa: Uutta vuoden 2022 laitoksessa ja keskeinen hallintakeino pienelle pilveen nojaavalle yritykselle. Näyttönä on pilvipolitiikka, jossa on hyväksymisprosessi uusille palveluille, dokumentoitu jaetun vastuun malli palvelua kohti, kovennusasetukset sekä irtautumissuunnitelma, johon kuuluu tietojen palautus ja vahvistus poistosta.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.24 **Tietoturvahäiriöiden hallinnan suunnittelu ja valmistautuminen: Häiriöiden käsittelyn prosessit, roolit ja vastuut on suunniteltu ja laadittu.** Asiakirja

Mistä sen tunnistaa: Häiriöiden hallinnan suunnitelma, jossa on ilmoitusreitti, roolit, eskalointitasot, yhteystiedot työajan ulkopuolelle ja viestintäpohjat. Pienelle tiimille realistinen tapa on yksi sivu, mutta harjoiteltuna.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.25 **Tietoturvatapahtumien arviointi ja niitä koskeva päätös: Tietoturvatapahtumat arvioidaan ja niistä päätetään, luokitellaanko ne tietoturvahäiriöiksi.**

Mistä sen tunnistaa: Luokittelukriteerit vakavuusmatriiseineen ja tapahtumarekisteri, jossa myös hylätyt tapahtumat näkyvät perusteluineen. Ero tapahtuman ja häiriön välillä näkyy rekisterissä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.26 **Vastaaminen tietoturvahäiriöihin: Häiriöt käsitellään dokumentoitujen menettelyjen mukaisesti.**

Mistä sen tunnistaa: Häiriöasiakirjat aikajanoineen, tehtyine toimenpiteineen, osallistuneine henkilöineen ja sulkemispäätöksineen. Jos todellista häiriötä ei ole vielä ollut, dokumentoitu pöytäharjoitus on paras saatavilla oleva näyttö.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.27 **Tietoturvahäiriöistä oppiminen: Häiriöistä saatua tietoa käytetään tietoturvan hallintakeinojen vahvistamiseen.**

Mistä sen tunnistaa: Syyttelemätön jälkikatselmointi juurisyyanalyyseineen ja siitä johdettuine toimenpiteineen, liitettynä parantamisrekisteriin ja tarvittaessa riskirekisteriin.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.28 **Näytön kerääminen: On ohjeistettu, miten tietoturvatapahtumaan liittyvät jäljet tunnistetaan, turvataan ja säilytetään niin, että ne pysyvät käyttökelpoisina myöhemmin.**

Mistä sen tunnistaa: Lyhyt näytön turvaamisen menettely: järjestelmiä ei rakenneta uudelleen ennenaikaisesti, levykuvat ja lokit turvataan ja säilytysketju dokumentoidaan. Pienelle yritykselle riittää, että määritellään vakavuustaso, jolta alkaen ulkopuolinen forensiikkatoimittaja kutsutaan paikalle, sekä sen yhteystiedot.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.29 **Tietoturvallisuus häiriötilanteessa: Organisaatio suunnittelee, miten tietoturvallisuus säilyy asianmukaisella tasolla häiriön aikana.**

Mistä sen tunnistaa: Hätäjärjestelyt eivät kytke tietoturvaa pois päältä. Dokumentoidaan, että MFA, lokitus ja pääsyrajoitukset ovat voimassa myös varakäytössä ja että hätätilanteen tilit (break-glass-tilit) ovat sinetöityjä ja dokumentoituja ja että ne katselmoidaan jälkikäteen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.30 **ICT-valmius liiketoiminnan jatkuvuudelle: ICT-valmius on suunniteltu ja toteutettu, sitä ylläpidetään ja se testataan liiketoiminnan jatkuvuustavoitteiden ja ICT-jatkuvuusvaatimusten pohjalta.**

Mistä sen tunnistaa: Uutta vuoden 2022 laitoksessa. Näyttönä on määritellyt palautumisaikatavoitteet (RTO) ja palautumispistetavoitteet (RPO) kriittistä järjestelmää kohti, palautusmenettely ja vähintään yksi dokumentoitu testi vuodessa. Onnistunut palautustesti päiväyksineen ja kestoineen on vahvin yksittäinen näyttö.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.31 **Lakisääteiset, säädösperusteiset, viranomais- ja sopimusvaatimukset: Merkitykselliset vaatimukset ja tapa täyttää ne on tunnistettu ja dokumentoitu, ja ne ovat ajan tasalla.** Asiakirja

Mistä sen tunnistaa: Lakirekisteri, joka kattaa GDPR:n, sähköisen viestinnän lainsäädännön, kauppa- ja verolainsäädännön sekä soveltuvin osin NIS2:n tai toimialakohtaiset säännöt, kunkin toteuttavine sääntöineen ja katselmointipäivineen. Vuosittainen katselmointi riittää, mutta se on päivätty.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.32 **Immateriaalioikeudet: Asianmukaiset menettelyt immateriaalioikeuksien suojaamiseksi on otettu käyttöön.**

Mistä sen tunnistaa: Lisenssiluettelo käytössä olevista ohjelmistoista, avoimen lähdekoodin lisenssien tarkistus tuotteessa (lisenssiskanneri CI-putkessa) ja sääntö kolmannen osapuolen koodin ja generoidun koodin käsittelystä. Näyttönä on käännöksen lisenssiraportti.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.33 **Tallenteiden suojaus: Liiketoiminnan ja näytön tallenteet säilytetään niin, etteivät ne voi kadota, muuttua huomaamatta tai joutua vääriin käsiin, ja tämä pätee koko säilytysajan.**

Mistä sen tunnistaa: Säilytyssuunnitelma lakisääteisine aikoineen, peukalointia kestävä tallennus, rajoitettu pääsy ja varmuuskopio. Verotuksen kannalta merkityksellisistä tallenteista nimetään lakisääteiset säilytysajat nimenomaisesti, koska auditoijat tarkistavat mielellään juuri sen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.34 **Yksityisyys ja henkilötietojen suoja: Yksityisyyttä ja henkilötietojen (PII) suojaa koskevat vaatimukset on tunnistettu ja ne täytetään sovellettavan lain mukaisesti.**

Mistä sen tunnistaa: Seloste käsittelytoimista, käsittelysopimukset, poistosuunnitelma, prosessi rekisteröidyn oikeuksille ja tarvittaessa tietosuojaa koskeva vaikutustenarviointi. Yhteys ISMS:ään yhteisen suojattavien kohteiden luettelon kautta estää sen, että kaikkea ylläpidetään kahteen kertaan.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.35 **Tietoturvallisuuden riippumaton katselmointi: Organisaation tapa hallita tietoturvallisuutta katselmoidaan riippumattomasti suunnitelluin väliajoin ja aina merkittävien muutosten yhteydessä.**

Mistä sen tunnistaa: Näyttönä on riippumattoman auditoijan tekemä sisäinen auditointi, ulkoiset tunkeutumistestit tai itse sertifiointiauditointi. Riippumaton tarkoittaa, ettei sitä tee henkilö, joka vastaa katselmoitavasta alueesta.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.36 **Tietoturvapolitiikkojen, sääntöjen ja standardien noudattaminen: Organisaation omien tietoturvapolitiikkojen ja sovellettavien sääntöjen noudattaminen katselmoidaan säännöllisesti.**

Mistä sen tunnistaa: Noudattamisen tarkistukset päiväyksineen ja tuloksineen, esimerkiksi konfiguraation vertaaminen omaan kovennusperustasoon, asiakirjamerkintöjen otanta ja automaattiset politiikkatarkistukset pilvessä. Poikkeamat siirtyvät korjaavien toimenpiteiden rekisteriin.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.5.37 **Toimintamenettelyjen dokumentointi: Tietojenkäsittelyn välineitä koskevat toimintamenettelyt on dokumentoitu ja saatettu niitä tarvitsevien henkilöiden saataville.** Asiakirja

Mistä sen tunnistaa: Ajo-ohjeet varmuuskopiointiin ja palautukseen, käyttöönottoon, käyttäjähallintaan, korjauspäivityksiin ja häiriöiden käsittelyyn. Lyhyt ja ajantasainen voittaa laajan ja vanhentuneen, ja viimeisen muutoksen päiväys ajo-ohjetta kohti on pakollinen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.6 Liite A: Henkilöstöä koskevat hallintakeinot 8

A.6.1 **Taustaselvitys: Henkilöt, jotka tulevat työskentelemään organisaatiolle, selvitetään etukäteen lain rajoissa ja suojaustarpeisiin suhteutetusti, ja arkaluonteisissa rooleissa selvitys toistetaan työsuhteen aikana.**

Mistä sen tunnistaa: Ilman työntekijöitä tämä hallintakeino voidaan perustella tällä hetkellä ei sovellu, mutta menettely palkkaamisen varalle määritellään silti ja merkitään soveltuvuuslausuntoon suunniteltuna. Toimiva laajuus on henkilöllisyyden, ansioluettelon ja suositusten todentaminen sekä todistukset, ja rikosrekisteriote vain silloin, kun suojaustarpeet sen oikeuttavat ja laki sen sallii. Sama taso vaaditaan freelancereilta ja alihankkijoilta sopimuksin, muuten aukko avautuu juuri siihen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.6.2 **Työsuhteen ehdot: Sopimuksissa todetaan henkilöstön ja organisaation tietoturvavastuut.**

Mistä sen tunnistaa: Tietoturvaehto työ- tai palvelusopimuksessa, viitaten sovellettaviin politiikkoihin. Freelancereilla sama ehto palvelusopimuksessa sekä salassapitosopimus.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.6.3 **Tietoturvatietoisuus, koulutus ja harjoittelu: Henkilöstö ja merkitykselliset ulkoiset osapuolet saavat asianmukaisen tietoisuuden ja koulutuksen sekä säännölliset päivitykset organisaation politiikoista.**

Mistä sen tunnistaa: Vuosittainen koulutus osallistumisnäyttöineen ja päiväyksineen, täydennettynä tietojenkalastelusimulaatioilla, joiden klikkausosuus arvioidaan. Myös yksinyrittäjä tarvitsee näytön omasta täydennyskoulutuksestaan, esimerkiksi kurssivahvistukset.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.6.4 **Kurinpitomenettely: Muodollinen ja viestitty menettely on olemassa toimenpiteisiin ryhtymiseksi niitä henkilöitä kohtaan, jotka ovat rikkoneet tietoturvapolitiikkoja.**

Mistä sen tunnistaa: Ilman työntekijöitä tämä voidaan perustella tällä hetkellä ei sovellu, mutta menettely määritellään silti palkkaamisen varalle, sillä vain sen soveltaminen jää pois, ei sääntö. Vaadittavaa on porrastettu ja viestitty seuraamusasteikko (keskustelu, huomautus, varoitus, työsuhteen päättäminen) työlainsäädännön ja henkilöstön edustusta koskevien sääntöjen mukaisesti. Alihankkijoiden osalta seuraamustaso kirjataan sopimukseen, esimerkiksi sopimussakkona tai irtisanomisoikeutena.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.6.5 **Vastuut työsuhteen päättymisen tai muutoksen jälkeen: Tietoturvavastuut ja velvollisuudet, jotka pysyvät voimassa työsuhteen päättymisen tai roolin vaihdon jälkeen, on määritelty, ne pannaan täytäntöön ja niistä viestitään asianomaisille henkilöille.**

Mistä sen tunnistaa: Lähtöprosessin tarkistuslista, jossa on oikeuksien poisto, suojattavien kohteiden palautus, luovutus ja nimenomainen muistutus jatkuvista salassapitovelvoitteista. Allekirjoitettu lähtökeskustelun tallenne on yksinkertaisin näyttö.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.6.6 **Salassapitosopimukset: On määritetty, kenen on allekirjoitettava salassapitosopimus. Sisältö vastaa tiedon suojaustarpeita, ja sopimukset allekirjoitetaan, arkistoidaan ja katselmoidaan säännöllisesti niiden pitämiseksi ajan tasalla.**

Mistä sen tunnistaa: Allekirjoitetut salassapitosopimukset työntekijöille, freelancereille, palveluntuottajille ja harjoittelijoille, jälkivaikutusaikoineen. Yhteenvetotaulukko, jossa on sopimuskumppani, päiväys ja voimassaolo, tekee kokonaisuudesta auditoitavan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.6.7 **Etätyö: Tietoturvatoimenpiteet on otettu käyttöön silloin, kun henkilöt työskentelevät organisaation tilojen ulkopuolella ja käsittelevät samalla organisaation tietoa.**

Mistä sen tunnistaa: Kotitoimistoa ja etätyötä koskeva politiikka, jossa on vaatimukset levyn salauksesta, näytön lukituksesta, turvallisesta langattomasta verkosta, VPN:n tai zero trust -yhteyden käytöstä, näkösuojista ja kiellosta käyttää henkilökohtaisia laitteita ilman hyväksyntää. Näyttönä on päätelaitteiden MDM-vaatimustenmukaisuusraportti.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.6.8 **Tietoturvatapahtumista ilmoittaminen: Käytössä on keino, jolla henkilöt voivat ilmoittaa havaituista tai epäillyistä tietoturvatapahtumista ajoissa.**

Mistä sen tunnistaa: Selkeästi viestitty ilmoituskanava (postilaatikko, keskustelukanava, puhelinnumero) ja vakuutus siitä, ettei vilpittömässä mielessä tehdystä ilmoituksesta seuraa sanktioita. Näyttönä on ilmoitusten määrä tapahtumarekisterissä, ja pysyvästi tyhjä rekisteri on auditoinnissa varoitusmerkki.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7 Liite A: Fyysiset hallintakeinot 14

A.7.1 **Fyysiset turvarajat: Turvarajat on määritelty ja niitä käytetään suojaamaan alueita, joilla on tietoa ja tietojenkäsittelyn välineitä.**

Mistä sen tunnistaa: Kuvaus rajoista luonnoksineen tai valokuvineen: rakennus, toimisto ja palvelinkaappi. Kotitoimistossa raja on lukittava työhuone tai sen puuttuessa lukittava kaappi, ja se kuvataan sen sijaan että jätettäisiin pois.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.2 **Fyysinen kulku: Turva-alueita suojaavat asianmukainen kulunvalvonta ja kulkupisteet.**

Mistä sen tunnistaa: Avain- tai kulkukorttirekisteri luovutuksineen ja palautuksineen sekä vierailijasääntö saattamisineen ja kirjauksineen. Jos käytössä on yhteisötoimisto tai konesali, näyttönä otetaan operaattorin kulunvalvonta ja se varmistetaan sopimuksella.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.3 **Toimistojen, huoneiden ja tilojen turvaaminen: Toimistojen, huoneiden ja tilojen fyysinen turvallisuus on suunniteltu ja toteutettu.**

Mistä sen tunnistaa: Lukittavat ovet, ikkunasuojaus katutasossa, ei ulos näkyviä luottamuksellisia näyttöjä eikä yrityksen kylttiä arkaluonteisissa tiloissa. Lyhyt kuvaus ja valokuva riittävät näytöksi.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.4 **Fyysisen turvallisuuden valvonta: Tiloja valvotaan jatkuvasti luvattoman fyysisen pääsyn varalta.**

Mistä sen tunnistaa: Uutta vuoden 2022 laitoksessa. Vaihtoehtoja ovat hälytysjärjestelmä, liiketunnistimet, kameravalvonta tai kulkulokit. Kameravalvonnan tietosuojanmukaisuus tarkistetaan, ja kotitoimistossa perusteltu vaihtoehto on hälytysjärjestelmän, lukitun huoneen ja sen havainnon yhdistelmä, ettei siellä säilytetä arkaluonteisia palvelimia.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.5 **Suojautuminen fyysisiltä ja ympäristön uhkilta: Suojaus fyysisiä ja ympäristön uhkia vastaan on olemassa, esimerkiksi luonnonkatastrofeja sekä tahallisia ja tahattomia vahinkoja vastaan.**

Mistä sen tunnistaa: Katselmointi tulipalon, veden, kuumuuden, sähkökatkon ja murron osalta yhdessä käytössä olevien toimenpiteiden kanssa (palovaroittimet, sammuttimet, ei laitteita vesiputkien alla, varmuuskopio eri sijainnissa). Tähän kytkeytyy kohdan 4.1 ilmastonmuutosta koskeva määritys.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.6 **Työskentely turva-alueilla: Toimenpiteet turva-alueilla työskentelyyn on suunniteltu ja toteutettu.**

Mistä sen tunnistaa: Säännöt palvelinhuoneeseen tai korkean luottamuksellisuuden alueille: ei valvomatonta kolmannen osapuolen pääsyä, ei tallentamista kameroilla tai mobiililaitteilla ja tehdyn työn kirjaaminen. Jos turva-alueita ei ole, se voidaan perustella viittaamalla pelkkään pilvipohjaiseen toimintaan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.7 **Siisti työpöytä ja tyhjä näyttö: Säännöt siististä työpöydästä paperien ja siirrettävien tallennusvälineiden osalta sekä lukituista näytöistä on määritelty ja niitä noudatetaan.**

Mistä sen tunnistaa: Tämä pätee täysin myös kotitoimistossa, joten sitä ei merkitä ei sovellu. Näyttönä on lyhyt sääntö (asiakirjat lukkojen taakse, näytön lukitus viiden minuutin jälkeen, ei tunnuksia sisältäviä muistilappuja) sekä laitepolitiikan teknisesti pakottama lukitus, jonka konfiguraation voi viedä ulos.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.8 **Laitteiden sijoittaminen ja suojaus: Laitteet on sijoitettu turvallisesti ja suojattu.**

Mistä sen tunnistaa: Sijoitus pois kulkuväyliltä ja yleisiltä alueilta, ei näkymää ulkoa, suojaus kuumuudelta ja kosteudelta sekä vaijerilukot mobiililaitteille. Lyhyt kuvaus kotitoimisto- tai toimistopolitiikassa riittää.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.9 **Toimitilojen ulkopuolisten suojattavien kohteiden turvallisuus: Toimitilojen ulkopuolella olevat suojattavat kohteet on suojattu.**

Mistä sen tunnistaa: Pienessä yrityksessä kyse on lähinnä kannettavasta, älypuhelimesta ja ulkoisista tallennusvälineistä, eikä tätä voi selittää pois. Näyttönä on pakotettu levyn salaus, MDM:n kautta käytössä oleva etätyhjennys, sääntö joka kieltää laitteiden jättämisen ajoneuvoihin ja julkisten verkkojen käytön ilman VPN:ää, sekä ilmoitusreitti katoamisesta. MDM-vaatimustenmukaisuusraportti, joka näyttää salaustilan laitetta kohti, on vahvin yksittäinen näyttö.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.10 **Tallennusvälineet: Tallennusvälineitä hallitaan koko elinkaarensa ajan luokittelumallin ja käsittelyvaatimusten mukaisesti hankinnasta käytön ja kuljetuksen kautta hävittämiseen.**

Mistä sen tunnistaa: Tämä pätee myös puhtaasti liikkuvassa työssä, koska USB-tikkuja, ulkoisia levyjä ja varmuuskopiovälineitä on olemassa. Näyttönä on välinerekisteri, salatut välineet, teknisesti pakotettu kielto hyväksymättömille siirrettäville välineille, turvallinen säilytys lukittavassa paikassa ja siirto kohtaan A.7.14 elinkaaren lopussa.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.11 **Tukevat käyttöhyödykkeet: Tietojenkäsittelyn välineet on suojattu tukevien käyttöhyödykkeiden ja erityisesti sähkönsyötön häiriöiltä.**

Mistä sen tunnistaa: Kun palvelimia ajetaan omissa tiloissa, käytössä on katkeamaton virransyöttö dokumentoituine testeineen. Pelkästään pilveen nojaavassa ratkaisussa näyttönä on viittaus toimittajan sitoumuksiin sekä sääntö siitä, miten työtä jatketaan paikallisen sähkö- tai verkkokatkon aikana (puhelimen jakama yhteys, varasijainti).

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.12 **Kaapeloinnin turvallisuus: Sähkö-, data- ja viestintäkaapelointi on suojattu kuuntelulta, häiriöiltä ja vaurioilta.**

Mistä sen tunnistaa: Kun kaapelointi on omassa hallinnassa, suojaus vaurioilta ja luvattomalta pääsyltä ristikytkentäpaneeleihin. Pienissä toimistoissa ja kotitoimistoissa perustelu on kevyt, mutta se annetaan: reititin ja verkkopistorasiat eivät ole julkisesti saavutettavissa ja käyttämättömät portit on kytketty pois.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.13 **Laitteiden kunnossapito: Laitteita huolletaan oikein tiedon saatavuuden, eheyden ja luottamuksellisuuden varmistamiseksi.**

Mistä sen tunnistaa: Huoltosuunnitelma tai toimittajatuen tila laitetta kohti sekä sääntö kolmannen osapuolen tekemistä korjauksista (tallennusväline irrotetaan ensin tai tiedot tyhjennetään, ja toimittajan kanssa tehdään salassapitosopimus). Tuen päättymispäiviä seurataan suojattavien kohteiden luettelossa.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.7.14 **Laitteiden turvallinen hävittäminen tai uudelleenkäyttö: Ennen kuin tallennustilaa sisältävä laite luovutetaan, myydään tai romutetaan, on todennettu ja kirjattu, ettei siltä voi enää palauttaa suojattavia tietoja eikä lisensoitua ohjelmistoa.**

Mistä sen tunnistaa: Tämä pätee myös kotitoimistossa ja käytöstä poistetuissa henkilökohtaisissa laitteissa, joita on käytetty työhön. Näyttönä on tyhjennystallenne laitetta kohti sarjanumeroineen, päiväyksineen ja menetelmineen (salausavaimen tuhoaminen salatuilla SSD-levyillä, ylikirjoitus, fyysinen tuhoaminen) tai toimittajan antama tuhoamistodistus. Salatuissa laitteissa riittää dokumentoitu avaimen tuhoaminen, kunhan menettely on kuvattu.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8 Liite A: Teknologiset hallintakeinot 34

A.8.1 **Käyttäjien päätelaitteet: Päätelaitteille tallennettu, niillä käsiteltävä tai niiden kautta saavutettava tieto on suojattu.**

Mistä sen tunnistaa: Kovennusperustaso käyttöjärjestelmää kohti, keskitetty hallinta MDM:n kautta, levyn salaus, automaattiset päivitykset ja näytön lukitus. MDM-vaatimustenmukaisuusraportti, jossa on tila laitetta kohti, osoittaa nämä kaikki kerralla.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.2 **Korotetut käyttöoikeudet: Korotettujen käyttöoikeuksien myöntämistä ja käyttöä on rajoitettu ja se on hallinnassa.**

Mistä sen tunnistaa: Luettelo kaikista pääkäyttäjätileistä perusteluineen, erilliset pääkäyttäjätilit joita ei käytetä päivittäiseen työhön, pakotettu MFA, määräaikainen oikeuksien korotus silloin kun se on mahdollista, sekä säännöllinen katselmointi. Pienessä yrityksessä tämä on tärkein korvaava hallintakeino kohdalle A.5.3.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.3 **Tiedon käytön rajoittaminen: Pääsyä tietoon ja muihin siihen liittyviin suojattaviin kohteisiin on rajoitettu laaditun pääsynhallintapolitiikan mukaisesti.**

Mistä sen tunnistaa: Oikeuksien malli, joka perustuu rooleihin ja ryhmiin yksittäisten myöntöjen sijaan, ja näyttönä on vienti ryhmäjäsenyyksistä. Pilvitallennuksen julkiset jakolinkit katselmoidaan säännöllisesti ja niiden annetaan vanhentua.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.4 **Pääsy lähdekoodiin: Luku- ja kirjoitusoikeus lähdekoodiin, kehitystyökaluihin ja ohjelmistokirjastoihin on asianmukaisesti hallinnassa.**

Mistä sen tunnistaa: Koodivaraston oikeudet rooleittain, suojatut päähaarat, pakotetut katselmoinnit tai pakotetut tilatarkistukset ja suoran päähaaraan kirjoittamisen esto. Näyttönä on haarasuojauksen konfiguraatio ja organisaation jäsenluettelo.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.5 **Turvallinen todentaminen: Turvalliset todentamistekniikat ja menettelyt on otettu käyttöön pääsyrajoitusten ja aihekohtaisen politiikan pohjalta.**

Mistä sen tunnistaa: MFA kaikkeen ulkoiseen pääsyyn ja kaikille pääkäyttäjätileille, kalastelua kestävät menetelmät (pääsyavaimet, FIDO2) silloin kun se on mahdollista, sekä lukitus epäonnistuneiden yritysten jälkeen. Näyttönä on identiteetinhallinnan raportti MFA:n kattavuudesta.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.6 **Kapasiteetin hallinta: Tallennustilaa, laskentaa, kaistaa ja lisenssejä seurataan, ja tarvetta säädetään riittävän ajoissa, jotta pullonkaulat eivät koskaan uhkaa saatavuutta.**

Mistä sen tunnistaa: Tallennustilan, laskentakuorman, lisenssikiintiöiden ja pilvibudjettien seuranta raja-arvohälytyksineen. Pienessä yrityksessä riittää hälytys levynkäytöstä ja kustannusrajoista sekä vuosittainen kapasiteetin tarkastelu.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.7 **Suojautuminen haittaohjelmilta: Tekniset suojaukset haittaohjelmia vastaan ovat käytössä ja ajan tasalla, ja laitteita käyttävät henkilöt on koulutettu riittävän hyvin, jotta he eivät heikennä näitä suojauksia.**

Mistä sen tunnistaa: Aktiivinen päätelaitesuojaus keskitettyine tilanäkymineen, sähköpostisuodatin joka tarkastaa liitteet ja linkit, sekä sääntö, joka kieltää hyväksymättömien ohjelmistojen suorittamisen. Suojausratkaisun päivätty tilaraportti on suora näyttö.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.8 **Teknisten haavoittuvuuksien hallinta: Organisaatio hankkii aktiivisesti tietoa käyttämänsä teknologian haavoittuvuuksista, päättää jokaisesta havainnosta, kuinka altis organisaatio sille on, ja sulkee aukon määriteltyjen määräaikojen kuluessa tai perustelee toisenlaisen vastauksen.**

Mistä sen tunnistaa: Haavoittuvuuksien hallinta, jossa on lähde (skanneri, riippuvuustarkistus CI-putkessa, toimittajien tiedotteet), vakavuusluokitus ja määritellyt määräajat tasoa kohti, esimerkiksi kriittinen 7 päivän kuluessa. Näyttönä on skannausraportit useasta ajankohdasta, joista näkyy avointen havaintojen väheneminen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.9 **Konfiguraationhallinta: Laitteiden, ohjelmistojen, palvelujen ja verkkojen konfiguraatiot, mukaan lukien tietoturvakonfiguraatiot, on laadittu, dokumentoitu ja otettu käyttöön, niitä seurataan ja ne katselmoidaan.**

Mistä sen tunnistaa: Uutta vuoden 2022 laitoksessa. Näyttönä on dokumentoidut perustason konfiguraatiot (kovennusperustasot) ja niiden pakottaminen, mieluiten infrastruktuurina koodina versionhallinnassa tai MDM-profiileina. Konfiguraatiopoikkeamien havaitseminen ja säännöllinen konfiguraatioiden vertailu täydentävät kokonaisuuden.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.10 **Tiedon poistaminen: Tietojärjestelmiin, laitteille ja tallennusvälineille tallennettu tieto poistetaan, kun sitä ei enää tarvita.**

Mistä sen tunnistaa: Uutta vuoden 2022 laitoksessa ja tiiviisti sidoksissa GDPR:ään. Näyttönä on poistosuunnitelma säilytysaikoineen tietoluokkaa kohti, teknisesti toteutetut säilytyskäytännöt pilvipalveluissa ja tietokannoissa sekä poistolokit. Myös varmuuskopiot ja lokiarkistot tarvitsevat säilytysajan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.11 **Tietojen peittäminen: Tietojen peittämistä sovelletaan pääsynhallintaa koskevan aihekohtaisen politiikan sekä liiketoiminnan ja lain vaatimusten mukaisesti.**

Mistä sen tunnistaa: Uutta vuoden 2022 laitoksessa. Käytännössä tämä tarkoittaa, ettei tuotantotietoa ole testi- ja kehitysympäristöissä vaan niissä käytetään anonymisoitua tai synteettistä tietoa, että analytiikassa käytetään pseudonymisointia ja että tilinumerot ja tunnukset peitetään lokeissa ja tukiliittymissä. Näyttönä on skripti tai menettely, joka tuottaa testitiedot.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.12 **Tietovuotojen esto: Tietovuotojen estoon tähtääviä toimenpiteitä sovelletaan järjestelmiin, verkkoihin ja laitteisiin, jotka käsittelevät, tallentavat tai välittävät arkaluonteista tietoa.**

Mistä sen tunnistaa: Uutta vuoden 2022 laitoksessa. Pienessä yrityksessä realistisia keinoja ovat pilvitallennuksen jakolinkkien hallinta, hyväksymättömien siirrettävien välineiden esto, säännöt jotka kieltävät edelleenlähetyksen yksityisiin postilaatikoihin, tarkistukset luottamuksellisen tiedon syöttämisestä ulkoisiin tekoälypalveluihin sekä salaisuuksien skannaus lähdekoodista. Näyttönä on konfiguraatio ja osumien katselmoinnit.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.13 **Tiedon varmuuskopiointi: Tiedosta, ohjelmistoista ja järjestelmistä on varmuuskopiot määritellyn säännön mukaisesti (laajuus, aikaväli, säilytys, sijainti), ja niistä palauttamista todella testataan säännöllisin väliajoin.**

Mistä sen tunnistaa: Varmuuskopiointipolitiikka, jossa on aikaväli, säilytys ja toisessa sijainnissa oleva kopio 3-2-1-periaatteen mukaisesti, varmuuskopioiden salaus sekä suojaus kiristysohjelman aiheuttamaa ylikirjoitusta vastaan (muuttumattomat varmuuskopiot). Ratkaisevaa on dokumentoitu palautustesti päiväyksineen ja tuloksineen, koska testaamaton varmuuskopio on auditoinnissa olematon.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.14 **Tietojenkäsittelyn välineiden redundanssi: Tietojenkäsittelyn välineet on toteutettu riittävällä redundanssilla saatavuusvaatimusten täyttämiseksi.**

Mistä sen tunnistaa: Redundanssi mitoitetaan saatavuustavoitteiden mukaan eikä suurimman mahdollisen mukaan. Näyttönä on arkkitehtuurikuvaus, jossa on rinnakkaiset instanssit tai vyöhykkeet, varalaitteet ja perusteltu päätös siitä, missä redundanssia tarkoituksella ei ole.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.15 **Lokitus: Tietoturvan kannalta merkitykselliset toimet jättävät jäljen. Lokeja tuotetaan, säilytetään, suojataan muuttamiselta ja niitä myös analysoidaan eikä ainoastaan kerätä.**

Mistä sen tunnistaa: Vähintään lokitetaan kirjautumiset ja epäonnistuneet yritykset, oikeuksien muutokset, hallinnolliset toimet ja pääsy luottamukselliseen tietoon. Lokit on suojattu muuttamiselta ja niillä on määritelty säilytysaika, ja pienessä yrityksessä muuttumattomat lokit ovat samalla korvaus puuttuvalle tehtävien eriyttämiselle kohdassa A.5.3.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.16 **Valvontatoimet: Verkkoja, järjestelmiä ja sovelluksia valvotaan poikkeavan käyttäytymisen varalta, ja mahdollisten tietoturvahäiriöiden arvioimiseksi ryhdytään asianmukaisiin toimiin.**

Mistä sen tunnistaa: Uutta vuoden 2022 laitoksessa. Tämä toimii ilman omaa tietoturvatiimiä: identiteetinhallinnan hälytykset mahdottomista matkoista ja epäonnistuneiden yritysten sarjoista sekä pilvialustan hälytykset poikkeavista kuluista tai oikeuksien muutoksista, ohjattuna valvottuun postilaatikkoon määritellyllä vasteajalla. Näyttönä on hälytyssäännöt sekä esimerkit käsitellyistä hälytyksistä.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.17 **Kellojen synkronointi: Kaikki lokia kirjoittavat järjestelmät ottavat aikansa määritellystä ja luotetusta lähteestä, jotta tapahtumat voidaan asettaa oikeaan järjestykseen järjestelmien välillä.**

Mistä sen tunnistaa: NTP-konfiguraatio palvelimilla ja päätelaitteilla sekä yhtenäinen aikavyöhyke lokeissa (mieluiten UTC). Ilman synkronoitua aikaa kohdan A.5.28 mukainen häiriön kulun selvittäminen ei kestä tarkastelua, ja näytöksi riittää ote konfiguraatiosta.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.18 **Etuoikeutettujen apuohjelmien käyttö: Sellaisten apuohjelmien käyttöä, jotka voivat ohittaa järjestelmän suojaukset, on rajoitettu ja se on tiukasti hallinnassa.**

Mistä sen tunnistaa: Luettelo hyväksytyistä hallintatyökaluista, paikallisten pääkäyttäjäoikeuksien rajoittaminen, sovellusten hallinta (sallittujen luettelo) silloin kun se on mahdollista, sekä käytön lokitus. Näyttönä on politiikka sekä oikeuksien hallinnan konfiguraatio.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.19 **Ohjelmistojen asentaminen tuotantojärjestelmiin: Menettelyt ja toimenpiteet ohjelmistoasennusten turvalliseen hallintaan tuotantojärjestelmissä on otettu käyttöön.**

Mistä sen tunnistaa: Vain hyväksyttyä ohjelmistoa luotetuista lähteistä, asennus keskitetyn jakelun tai pakettienhallinnan kautta, peruutuspolku ja edellisen version säilyttäminen. Näyttönä on hyväksymisluettelo ja käyttöönottolokit.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.20 **Verkkojen turvallisuus: Verkoilla ja aktiivisilla verkkolaitteilla on nimetty omistaja, kovennettu konfiguraatio ja jäljitettävä sääntöjoukko, joka määrittelee, mikä liikenne ylipäätään on sallittua.**

Mistä sen tunnistaa: Palomuurin sääntöjoukko, joka noudattaa oletusarvoista estoa, dokumentoidut avoimet portit perusteluineen, turvallinen langattoman verkon konfiguraatio ja vaihdetut oletustunnukset verkkolaitteissa. Näyttönä on sääntöjoukon vienti ja ulkoinen porttiskannaus.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.21 **Verkkopalvelujen turvallisuus: Verkkopalvelujen turvamekanismit, palvelutasot ja hallintavaatimukset on tunnistettu ja otettu käyttöön ja niitä seurataan.**

Mistä sen tunnistaa: Jokaisesta käytössä olevasta verkkopalvelusta (VPN, DNS, sähköposti, CDN) kirjataan turvasitoumukset ja oma konfiguraatio, mukaan lukien siirron aikainen salaus ja toimittajan palvelutasositoumukset. Näyttönä on konfiguraation yhteenveto sekä sopimus tai palvelukuvaus.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.22 **Verkkojen erottelu: Verkko on jaettu vyöhykkeisiin niin, että palvelut, käyttäjäryhmät ja järjestelmät, joilla on eri suojaustarpeet, eivät tavoita toisiaan suodattamatta.**

Mistä sen tunnistaa: Erilliset verkkosegmentit tai VLANit vieraille, hallinnolle ja tuotannolle, ja pilvessä erilliset tilit tai virtuaaliverkot turvaryhmineen. Kotitoimistossa toimiva toteutus on erillinen verkko tai VLAN työlaitteille, erillään henkilökohtaisista laitteista ja kodin älytekniikasta.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.23 **Verkkosuodatus: Pääsyä ulkoisille verkkosivustoille hallitaan haitalliselle sisällölle altistumisen vähentämiseksi.**

Mistä sen tunnistaa: Uutta vuoden 2022 laitoksessa. Tämä saavutetaan vähällä vaivalla suodattavalla DNS-palvelulla tai päätelaitesuojaukseen sisältyvällä verkkosuodatuksella, estettyine luokkineen ja estettyjen pyyntöjen lokituksineen. Näyttönä on suodattimen konfiguraatio ja ote raportoinnista.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

A.8.24 **Salauksen käyttö: On sitovasti määritelty, missä salausta sovelletaan, millä algoritmeilla ja miten avaimet luodaan, säilytetään, vaihdetaan ja tuhotaan koko elinkaarensa ajan.** Asiakirja

Mistä sen tunnistaa: Salauspolitiikka hyväksyttyine algoritmeineen ja vähimmäisavainpituuksineen, salaus siirrossa (TLS) ja levossa sekä avaintenhallinnan menettely, joka kattaa luonnin, säilytyksen, vaihdon ja tuhoamisen. Näyttönä on politiikka sekä avainpalvelun tai avainholvin konfiguraatio.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.8.25 **Turvallisen kehittämisen elinkaari: Säännöt ohjelmistojen ja järjestelmien turvalliseen kehittämiseen on laadittu ja niitä sovelletaan.**

Mistä sen tunnistaa: Kehitysprosessin kuvaus, jossa on tietoturvan kosketuspisteet vaihetta kohti: vaatimukset, suunnittelu, toteutus, testaus, julkaisu ja käyttö. Pienelle tiimille riittää yksi sivu, joka viittaa konkreettisiin CI-portteihin ja katselmointivelvoitteeseen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.8.26 **Sovellusten tietoturvavaatimukset: Sovellusten tietoturvavaatimukset on tunnistettu, määritelty ja hyväksytty kehittämisen ja hankinnan aikana.**

Mistä sen tunnistaa: Tietoturvavaatimukset nimenomaisina kohtina vaatimusluettelossa tai uudelleenkäytettävänä tarkistuslistana, joka nojaa esimerkiksi yleisiin sovellusten tietoturvan todentamisen standardeihin. Näyttönä on tiketit tai vaatimusasiakirjat, joissa on tietoturvanäkökulma.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.8.27 **Turvallisen järjestelmäarkkitehtuurin ja suunnittelun periaatteet: Turvallisen järjestelmäsuunnittelun periaatteet on laadittu ja dokumentoitu, ja niitä sovelletaan kehitystoimintaan.**

Mistä sen tunnistaa: Dokumentoidut periaatteet, kuten vähimmän oikeuden periaate, syvyyssuuntainen puolustus, turvalliset oletusasetukset, tietojen minimointi ja zero trust -ajattelu, sekä niiden näkyvä soveltaminen arkkitehtuuriluonnoksissa tai päätöstallenteissa.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.8.28 **Turvallinen ohjelmointi: Turvallisen ohjelmoinnin periaatteita sovelletaan ohjelmistokehityksessä.**

Mistä sen tunnistaa: Uutta vuoden 2022 laitoksessa. Näyttönä on sitovat ohjelmointisäännöt, staattinen koodianalyysi ja salaisuuksien skannaus pakollisina CI-portteina, tarkastettujen kirjastojen käyttö ja dokumentoidut koodikatselmoinnit. Kun tehtävien eriyttäminen on mahdotonta, pakotetut automaattiset portit korvaavat nelisilmäperiaatteen, ja tämä perustellaan ja osoitetaan putken konfiguraatiolla.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.8.29 **Tietoturvatestaus kehityksessä ja hyväksynnässä: Tietoturvatestauksen prosessit on määritelty ja otettu käyttöön kehityksen elinkaaren sisällä.**

Mistä sen tunnistaa: Automaattiset tietoturvatestit putkessa (riippuvuustarkistukset, staattinen ja dynaaminen analyysi) sekä säännöllinen tunkeutumistesti silloin kun suojaustarpeet ovat korkeat. Näyttönä on päivätyt testiraportit ja havaintojen seuranta.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.8.30 **Ulkoistettu kehittäminen: Ulkoistettua kehitystoimintaa ohjataan, seurataan ja katselmoidaan.**

Mistä sen tunnistaa: Kun kehittäminen on ulkoistettu, tietoturvavaatimukset asetetaan sopimuksessa, koodin omistus ja katselmointioikeus varmistetaan, ja koodikatselmoinnit ja tietoturvatestit tehdään ennen hyväksyntää. Ilman ulkoistettua kehittämistä soveltumattomuus perustellaan johdonmukaisesti soveltuvuuslausunnossa.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.8.31 **Kehitys-, testi- ja tuotantoympäristöjen erottaminen: Kehitys-, testi- ja tuotantoympäristöt on erotettu toisistaan ja suojattu.**

Mistä sen tunnistaa: Erilliset tilit, projektit tai nimiavaruudet, erilliset tunnukset ja erilliset tietojoukot. Yhdessä kohdan A.8.11 kanssa varmistetaan, ettei tuotantotietoa päädy tuotannon ulkopuolisiin ympäristöihin. Näyttönä on ympäristöjen yhteenveto ja oikeuksien jako.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.8.32 **Muutostenhallinta: Tietojenkäsittelyn välineiden ja tietojärjestelmien muutoksiin sovelletaan muutostenhallinnan menettelyjä.**

Mistä sen tunnistaa: Muutosprosessi, jossa on pyyntö, vaikutusten arviointi, testaus, hyväksyntä, toteutus ja peruutuspolku. Kehitystiimeissä muutospyyntöputki pakotettuine tarkistuksineen ja lokitettuine käyttöönottoineen täyttää tämän kohdan, kunhan historia on muuttumaton.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.8.33 **Testitiedot: Testitiedot valitaan, suojataan ja hallitaan asianmukaisesti.**

Mistä sen tunnistaa: Periaate on, ettei testijärjestelmissä ole todellisia henkilötietoja. Kun se on väistämätöntä, dokumentoidaan hyväksyntä, peittäminen, pääsyn rajoitus ja poisto testin jälkeen. Näyttönä on testitietojen suunnitelma ja poistolokit.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

A.8.34 **Tietojärjestelmien suojaus auditointitestauksen aikana: Auditointitestit, joihin liittyy pääsy tuotantojärjestelmiin, suunnitellaan ja sovitaan johdon kanssa toiminnan häiriöiden välttämiseksi.**

Mistä sen tunnistaa: Auditointisopimus, jossa on aikaikkuna, laajuus, vain luku -oikeus silloin kun se on mahdollista, auditointipääsyn lokitus ja johdon hyväksyntä. Tämä koskee myös tunkeutumistestejä, ja näyttönä on kirjallinen testivaltuutus aikaikkunoineen ja hätäyhteyshenkilöineen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu