ISO/IEC 27001:2022 + Amd 1:2024 Informacijos saugumo vadybos sistemos (ISMS)

Informacijos saugumas, ISMS, sertifikuojama visame pasaulyje

181 reikalavimai. Pagal šį standartą galima sertifikuotis akredituotoje sertifikavimo įstaigoje. Redakcija 07/2026.

> ISO/IEC 27001 nustato informacijos saugumo vadybos sistemos reikalavimus: ji yra pagrįsta rizika, dokumentuota ir įrodomai rezultatyvi. Vertinimas pagal šį standartą yra akredituotas sertifikavimo auditas dviem etapais (dokumentų peržiūra, po to rezultatyvumo vertinimas vietoje), po kurio kasmet vyksta priežiūros auditai, o po trejų metų pakartotinis sertifikavimas.

Įmonė	Data	Pildė

4 Organizacijos aplinka 8

4.1-1 Išorės ir vidaus klausimai, veikiantys organizacijos gebėjimą pasiekti numatytus ISMS rezultatus, yra nustatyti ir nuolat atnaujinami.

Iš ko tai galima atpažinti: Įrodymas yra aplinkos analizė, parengta kaip atskiras dokumentas arba kaip ISMS vadovo skyrius: rinkos aplinka, klientų ir sutarčių padėtis, teisinis pagrindas (GDPR, NIS2), technologijų rinkinys, darbuotojų skaičius, priklausomybė nuo debesijos paslaugų teikėjų. Mažoms organizacijoms pakanka vieno puslapio lentelės su data ir peržiūros ciklu, jeigu vadovybinė vertinamoji analizė rodo, kad ji tikrai atnaujinama.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

4.1-2 Organizacija yra nustačiusi, ar klimato kaita jai yra svarbus klausimas. Sprendimas yra pagrįstas nepriklausomai nuo to, ar atsakymas teigiamas, ar neigiamas.

Iš ko tai galima atpažinti: Šis reikalavimas įvestas Amd 1:2024 pakeitimu, ir auditoriai jo klausia atskirai. Aplinkos analizėje palikite atskirą eilutę: karščio laikotarpiai, veikiantys serverių patalpas ir prieinamumą, ekstremalūs orai, veikiantys debesijos paslaugų teikėjų duomenų centrus, elektros tinklo stabilumas. Pagrįsta išvada, kad tai nesvarbu, yra priimtina, o trūkstamas įrašas nėra.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

4.2-1 Suinteresuotosios šalys, svarbios ISMS, yra nustatytos.

Iš ko tai galima atpažinti: Suinteresuotųjų šalių sąrašas, apimantis klientus, darbuotojus, duomenų tvarkytojus ir pasitelktus duomenų tvarkytojus, priežiūros institucijas, draudikus, sertifikavimo įstaigą ir akcininkus. Mažose organizacijose pakanka lentelės su šalimi, jos lūkesčiu ir lūkesčio šaltiniu.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

4.2-2 Šių suinteresuotųjų šalių svarbūs reikalavimai yra nustatyti, įskaitant reikalavimus, susijusius su klimato kaita.

Iš ko tai galima atpažinti: Prie kiekvienos šalies nurodykite konkretų šaltinį: sutarties punktą, duomenų tvarkymo sutartį, kliento klausimyną, teisinę prievolę. Amd 1:2024 prideda pastabą, kad suinteresuotosios šalys gali kelti su klimato kaita susijusius reikalavimus. Tai nėra atskiras privalomas reikalavimas, tačiau auditoriai jį įprastai kelia, pavyzdžiui, darnumo klausimai stambaus kliento atliekamame tiekėjo audite. Pakanka vienos eilutės suinteresuotųjų šalių lentelėje su rezultatu, įskaitant išvadą, kad tokių reikalavimų nėra.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

4.2-3 Nuspręsta ir atsekama, kurie iš šių reikalavimų įgyvendinami ISMS priemonėmis.

Iš ko tai galima atpažinti: Į suinteresuotųjų šalių lentelę įtraukite stulpelį, nurodantį taisyklę, kuri įgyvendina reikalavimą (politika, valdymo priemonė, sutarties priedas). Tai parodo, kad reikalavimai buvo ne tik surinkti, bet ir tikrai apdoroti.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

4.3-1 **ISMS taikymo sritis yra nustatyta ir atsižvelgia į 4.1 klausimus, 4.2 reikalavimus, taip pat į sąsajas ir priklausomybes nuo trečiųjų šalių vykdomos veiklos.**

Iš ko tai galima atpažinti: Taikymo srityje įvardytos vietos, organizaciniai padaliniai, produktai, sistemos ir tinklo ribos. Perduotos vykdyti dalys (prieglobos paslaugos, mokėjimų teikėjai, palaikymas) aprašomos kaip sąsajos su aiškia atsakomybės riba. Dirbtinai susiaurintą taikymo sritį, iš kurios išimti pagrindiniai procesai, sertifikavimo įstaigos atmeta.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

4.3-2 **Taikymo sritis yra prieinama kaip dokumentuota informacija ir vienareikšmiškai nurodo ISMS ribas.** Dokumentas

Iš ko tai galima atpažinti: Patvirtintas taikymo srities dokumentas su versija, data ir aukščiausiosios vadovybės patvirtinimu. Tiksli jo formuluotė vėliau atsiranda sertifikate, todėl formuluokite ją tiksliai ir taip, kad ją būtų galima viešai cituoti.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

4.4-1 **ISMS, įskaitant reikalingus procesus ir jų sąveiką, yra sukurta, įdiegta, palaikoma ir nuolat gerinama.**

Iš ko tai galima atpažinti: Procesų žemėlapis arba procesų sąrašas, siejantis rizikos valdymą, incidentų tvarkymą, pakeitimų valdymą, auditą ir vadovybinę vertinamąją analizę su savininkais ir dažnumu. Už schemą svarbesni yra gyvi įrodymai: užduočių įrašai, protokolai, kalendoriaus įrašai.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

5 Lyderystė 8

5.1-1 **Aukščiausioji vadovybė prisiima atsakomybę už ISMS rezultatyvumą ir užtikrina, kad politika ir tikslai yra nustatyti ir suderinami su strategine kryptimi.**

Iš ko tai galima atpažinti: Įrodymas yra pasirašyti politikos, taikymo srities ir pritaikomumo pareiškimo patvirtinimai, vadovybinės vertinamosios analizės protokolai ir dokumentuoti biudžeto sprendimai. Labai mažose organizacijose aukščiausioji vadovybė dažnai yra tas pats asmuo kaip ir ISMS savininkas; tai priimtina, tačiau vaidmenų apraše nurodoma atvirai.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

5.1-2 **ISMS reikalavimai yra integruoti į verslo procesus, o rezultatyvaus informacijos saugumo svarba yra komunikuojama.**

Iš ko tai galima atpažinti: Geriausiai matoma ten, kur saugumas nėra atskiras segtuvas: saugumo kriterijus baigtumo apibrėžtyje, saugumo patikra pardavimo arba pirkimo procese, pasikartojantis saugumo klausimas komandos susirinkimų protokoluose.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

5.1-3 **Vadovybė skiria reikalingus išteklius, remia žmones, prisidedančius prie ISMS rezultatyvumo, ir skatina nuolatinį gerinimą.**

Iš ko tai galima atpažinti: Patvirtintas saugumo biudžetas, mokymams skirtas laikas, išorės auditorių arba įsilaužimo testuotojų pasitelkimas. Gerinimo arba veiksmų registras su įrašais per kelis ketvirčius rodo tęstinumą, o ne vienkartines pastangas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

5.2-1 **Informacijos saugumo politika yra sukurta, atitinka organizacijos paskirtį ir sudaro pagrindą informacijos saugumo tikslams.** Dokumentas

Iš ko tai galima atpažinti: Trumpas patvirtintas politikos dokumentas, pakanka dviejų ar trijų puslapių. Jame įvardijami apsaugos tikslai, taikymo sritis, atsakomybės ir rizika pagrįsto požiūrio principas. Bendrinis šablono tekstas be ryšio su tikra veikla audite iškart krinta į akis.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

5.2-2 **Politikoje yra įsipareigojimas tenkinti taikomus reikalavimus ir įsipareigojimas nuolat gerinti ISMS.** Dokumentas

Iš ko tai galima atpažinti: Abu įsipareigojimai politikoje pateikiami kaip aiškūs sakiniai ir 1 etapo audite skaitomi pažodžiui. Papildomai nurodykite pagrindžiančius procesus (teisės aktų registras, gerinimo registras).

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

5.2-3 **Politika yra komunikuojama organizacijoje ir tinkamai prieinama suinteresuotosioms šalims.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra intraneto arba wiki įrašas su privalomu susipažinimu, įvedimo į darbą kontrolinis sąrašas su patvirtinimu arba paskelbta santrauka svetainėje. Paprasčiausias patikimas įrodymas yra platinimo sąrašas su susipažinimo patvirtinimais.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

5.3-1 **Su saugumu susijusių vaidmenų atsakomybės ir įgaliojimai yra paskirti ir komunikuoti organizacijoje.**

Iš ko tai galima atpažinti: Vaidmenų matrica (RACI), apimanti ISMS savininką, rizikų savininkus, turto savininkus, incidentų koordinatorių ir duomenų apsaugos kontaktinį asmenį. Vieno asmens arba labai mažose komandose kiekvieną vaidmenį priskirkite konkrečiam asmeniui, o susidariusią vaidmenų sankaupą dokumentuokite atvirai, o ne slėpkite.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

5.3-2 **Įgaliojimas užtikrinti ISMS atitiktį standartui ir teikti aukščiausiajai vadovybei ataskaitas apie ISMS veiklos rezultatus yra priskirtas konkrečiam vaidmeniui.**

Iš ko tai galima atpažinti: Paskyrimo raštas arba ISMS savininko vaidmens aprašas su aiškiai nurodytu atskaitomybės ryšiu vadovybei. Šis atskaitomybės ryšys realiai įrodomas vadovybinės vertinamosios analizės protokolais.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

6 Planavimas 21

6.1.1-1 **Remiantis 4.1 klausimais ir 4.2 reikalavimais, yra nustatytos rizikos ir galimybės, į kurias reikia atsižvelgti, kad ISMS pasiektų numatytus rezultatus, o nepageidaujamų padarinių būtų išvengta.**

Iš ko tai galima atpažinti: Registras, siejantis aplinkos klausimus su rizikomis ir galimybėmis, tvarkomas atskirai arba rizikų registre. Svarbiausia yra atsekamumas: kiekvienas aplinkos analizės klausimas matomai veda į vertinimą arba į pagrįstą sprendimą jo nenagrinėti.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

6.1.1-2 **Veiksmai šioms rizikoms ir galimybėms valdyti yra suplanuoti, integruoti į ISMS procesus, o jų rezultatyvumas yra vertinamas.**

Iš ko tai galima atpažinti: Veiksmų planas su atsakingu asmeniu, terminu ir rezultatyvumo kriterijumi. Rezultatyvumo vertinimą laikykite atskirame stulpelyje, kitaip auditui trūks įrodymo, kad veiksmas buvo ne tik įgyvendintas, bet ir patikrintas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

6.1.2-1 **Informacijos saugumo rizikos vertinimo procesas yra nustatytas ir taikomas; jis apima rizikos priimtinumo kriterijus ir rizikos vertinimų atlikimo kriterijus.** Dokumentas

Iš ko tai galima atpažinti: Rizikos valdymo politika su tikimybės ir poveikio skalėmis, nustatyta rizikų matrica ir aiškia priimtinumo riba. Riba yra skaičius arba zona, o ne formuluotė, tokia kaip savo nuožiūra.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

6.1.2-2 **Procesas užtikrina, kad pakartotiniai rizikos vertinimai duotų nuoseklius, pagrįstus ir palyginamus rezultatus.**

Iš ko tai galima atpažinti: Įrodymas yra nustatyta metodika su apibrėžtomis skalėmis ir dviejų vertinimo versijų palyginimas: tos pačios rizikos, ta pati vertinimo logika, paaiškinami skirtumai. Stipriausias įrodymas čia yra praėjusių metų rizikų registro versija su data.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.1.2-3 **Informacijos saugumo rizikos yra nustatytos taip, kad taikymo srityje būtų aptiktas konfidencialumo, vientisumo ir prieinamumo praradimas, ir kiekvienai rizikai yra priskirtas rizikos savininkas.**

Iš ko tai galima atpažinti: Rizikų registras su nuorodomis į turtą arba procesus, į tris apsaugos tikslus ir į įvardytą rizikos savininką. Rizikos savininkas turi įgaliojimus priimti riziką; mažose organizacijose tai paprastai yra vadovas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.1.2-4 **Nustatytos rizikos yra išanalizuotos: apibrėžti galimi padariniai, realistiška tikimybė ir iš jų išplaukiantis rizikos lygis.**

Iš ko tai galima atpažinti: Stulpeliai poveikiui, tikimybei ir gautam rizikos lygiui, kiekvienas su trumpu pagrindimu. Vienas pagrindimo sakinys kiekvienai rizikai užkerta kelią dažniausiam audito radiniui, kai skaičiai pateikiami be išvedimo.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.1.2-5 **Rizikos yra palygintos su priimtinumo kriterijais ir surikiuotos pagal apdorojimo pirmumą.**

Iš ko tai galima atpažinti: Rizikų registre matoma, kurios rizikos yra virš priimtinumo ribos ir kokia eile jos bus apdorojamos. Pakanka surikiuoto rodinio arba pirmumo stulpelio.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.1.2-6 **Rizikos vertinimo procesas yra prieinamas kaip dokumentuota informacija.** Dokumentas

Iš ko tai galima atpažinti: Pati metodika yra privalomas dokumentas, ne tik jos rezultatas. Patvirtinta politika su versija ir patvirtinimo data, susieta iš ISMS dokumentų rodyklės.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.1.3-1 **Kiekvienai rizikai, viršijančiai priimtinumo ribą, yra parinktas tinkamas apdorojimo būdas (mažinti, vengti, perduoti arba priimti).**

Iš ko tai galima atpažinti: Apdorojimo būdo stulpelis rizikų registre. Kai rizika priimama, užrašykite pagrindimą ir oficialų rizikos savininko pritarimą; kai ji perduodama, įvardykite sutartį arba draudimo liudijimą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.1.3-2 **Visos valdymo priemonės, reikalingos pasirinktiems rizikos apdorojimo būdams įgyvendinti, yra nustatytos.**

Iš ko tai galima atpažinti: Valdymo priemones formuluokite konkrečiai ir patikrinamai, su atsakingu asmeniu ir terminu. Nuoroda į jau vykdomus techninius darbus (MFA diegimas, atsarginės kopijos patikra) tinka, jeigu ji veda į užduoties įrašą arba konfigūracijos artefaktą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.1.3-3 **Nustatytos valdymo priemonės yra palygintos su A priedo valdymo priemonėmis, kad būtų patikrinta, ar nepraleista kuri nors reikalinga valdymo priemonė.**

Iš ko tai galima atpažinti: Palyginimas yra atskiras, atsekamas žingsnis, o ne šalutinis rezultatas. Įrodymas yra susiejimo stulpelis rizikų registre su nuorodomis į A priedo numerius ir palyginimo protokolas su data.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.1.3-4 **Pritaikomumo pareiškimas (SoA) yra parengtas. Jame atskirai įvertintos visos 93 A priedo valdymo priemonės, kiekvienai nurodytas pritaikomumas su pagrindimu, įgyvendinimo būsena ir kiekvieno neįtraukimo pagrindimas.** Dokumentas

Iš ko tai galima atpažinti: SoA yra pagrindinis privalomas dokumentas ir viso audito žemėlapis. Jis yra išsamus: netaikomos valdymo priemonės taip pat įrašomos su pagrindimu, niekada ne kaip tuščia eilutė. Rekomenduojami stulpeliai: valdymo priemonės numeris, pavadinimas, taikoma taip arba ne, pagrindimas, įgyvendinimo būsena, nuoroda į politiką arba įrodymą, sąsaja su rizika. Versija ir vadovybės patvirtinimas yra privalomi, nes SoA per kiekvieną priežiūros auditą lyginamas su tikrove.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.1.3-5 **Parengtas rizikos apdorojimo planas, kuriame sujungtos valdymo priemonės, atsakomybės, terminai ir reikalingi ištekliai.** Dokumentas

Iš ko tai galima atpažinti: Tai gali būti rizikų skaičiuoklės lapas arba projektų lenta. Svarbu, kad terminai būtų realistiški ir kad praleisti terminai būtų matomai perplanuoti, nes būtent tai auditorius ir tikrina.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.1.3-6 **Rizikos apdorojimo planą yra patvirtinę rizikų savininkai, o likutines rizikas jie yra oficialiai priėmę.** Dokumentas

Iš ko tai galima atpažinti: Parašas, elektroninis patvirtinimas arba sprendimas protokole su data. Pakanka vienos eilutės vadovybinės vertinamosios analizės protokole su nuoroda į registro versiją, jeigu versija yra vienareikšmė.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.1.3-7 **Rizikos apdorojimo procesas yra prieinamas kaip dokumentuota informacija.** Dokumentas

Iš ko tai galima atpažinti: Paprastai aprašomas tame pačiame politikos dokumente kaip ir rizikos vertinimas. Aprašoma visa eiga nuo vertinimo per būdo parinkimą iki likutinės rizikos priėmimo.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.2-1 **Informacijos saugumo tikslai yra nustatyti svarbioms funkcijoms ir lygiams, dera su politika ir yra išmatuojami, kai tai praktiškai įmanoma.**

Iš ko tai galima atpažinti: Tikslų lentelė, kurioje yra nuo trijų iki šešių tikslų, kiekvienas su rodikliu, pradine verte, siektina verte ir terminu. Pavyzdys: sistemų, kuriose įjungtas MFA, dalis iki ketvirčio pabaigos padidinama nuo 80 iki 100 procentų. Tikslai be skaičiaus laikomi neišmatuojamais.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.2-2 **Tikslai atsižvelgia į taikomus informacijos saugumo reikalavimus, taip pat į rizikos vertinimo ir rizikos apdorojimo rezultatus.**

Iš ko tai galima atpažinti: Į tikslų lentelę įtraukite kilmės stulpelį: iš kurios rizikos, kurio kliento reikalavimo arba kurios teisinės prievolės tikslas kyla. Tai apsaugo nuo tikslų, kurie atrodo atsitiktiniai.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.2-3 **Tikslai yra stebimi, komunikuojami ir prireikus atnaujinami.**

Iš ko tai galima atpažinti: Ketvirtinis pažangos sekimas tikslų lentelėje ir informavimas komandai, pavyzdžiui, trumpas įrašas wiki arba klausimas komandos susirinkimo darbotvarkėje. Ankstesnės versijos parodo, kad atnaujinimai tikrai vyksta.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6.2-4 **Informacijos saugumo tikslai yra prieinami kaip dokumentuota informacija.** Dokumentas

Iš ko tai galima atpažinti: Pakanka patvirtinto tikslų dokumento su data. Jis gali būti vadovybinės vertinamosios analizės dalis, tačiau ten egzistuoja kaip atskiras, lengvai randamas skyrius.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

6.2-5 **Kiekvienam tikslui yra suplanuota, kas bus daroma, kokių išteklių reikia, kas yra atsakingas, kada tai bus baigta ir kaip bus vertinami rezultatai.**

Iš ko tai galima atpažinti: Šie penki punktai tikrinami atskirai ir audite klausiami atskirai. Įrenkite juos kaip penkis stulpelius tikslų lentelėje, tada atitiktis matoma iš karto.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

6.3-1 **Kai organizacija nustato, kad ISMS reikia pakeitimų, tie pakeitimai atliekami planingai.**

Iš ko tai galima atpažinti: Įrodymas yra pakeitimų paraiškos, protokolai arba užduočių įrašai, rodantys pakeitimo priežastį, poveikio vertinimą, pritarimą ir įgyvendinimą. Įprastos priežastys mažose organizacijose: debesijos paslaugų teikėjo keitimas, naujos vietos, pirmas darbuotojo priėmimas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7 Parama 15

7.1-1 **Ištekliai, reikalingi ISMS sukurti, įdiegti, palaikyti ir nuolat gerinti, yra nustatyti ir skirti.**

Iš ko tai galima atpažinti: Saugumo biudžeto eilutė, įrankių licencijos (slaptažodžių tvarkyklė, MDM, įvykių registravimo platforma), suplanuotos žmogaus dienos ISMS priežiūrai ir išorės audito paslaugos. Sąskaita arba biudžeto patvirtinimas tai įrodo greičiau nei bet koks aprašymas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.2-1 **Reikalinga žmonių, kurių darbas veikia informacijos saugumo veiklos rezultatus, kompetencija yra nustatyta.**

Iš ko tai galima atpažinti: Kompetencijų matrica arba vaidmenų aprašai, kuriuose išvardytos kiekvienam vaidmeniui reikalingos žinios, pavyzdžiui, saugus kūrimas programuotojams, incidentų tvarkymas koordinatoriui. Labai mažose komandose pakanka vienos eilutės kiekvienam asmeniui.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.2-2 **Kompetencija yra užtikrinta tinkamu išsilavinimu, mokymu arba patirtimi.**

Iš ko tai galima atpažinti: Pažymėjimai, kursų patvirtinimai, gyvenimo aprašymai arba dokumentuota praktinė patirtis. Savarankiškas mokymasis priimtinas, jeigu jis įrodytas, pavyzdžiui, internetinių kursų baigimo įrašais arba išlaikytais vidaus žinių patikrinimais.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.2-3 **Kur yra kompetencijos spragų, imtasi veiksmų joms pašalinti, o šių veiksmų rezultatyvumas yra įvertintas.**

Iš ko tai galima atpažinti: Mokymo planas su siektinos ir faktinės būklės palyginimu ir rezultatyvumo patikra, pavyzdžiui, patikrinimo rezultatas, apgaulingų laiškų imitacijos paspaudimų dalis arba stebėjimas darbo vietoje. Rezultatyvumo patikra dažnai pamirštama ir yra klasikinis mažareikšmis radinys.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.2-4 **Tinkama dokumentuota informacija yra prieinama kaip kompetencijos įrodymas.** Dokumentas

Iš ko tai galima atpažinti: Kiekvieno asmens kompetencijos arba mokymo aplankas su įrodymais ir datomis. Mažose organizacijose pakanka katalogo su saugomais PDF įrašais ir apžvalginės lentelės.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.3-1 **Taikymo srityje dirbantys žmonės yra susipažinę su informacijos saugumo politika.**

Iš ko tai galima atpažinti: Susipažinimo patvirtinimas įvedant į darbą ir po kiekvieno politikos pakeitimo, su data ir versija. Pakanka wiki susipažinimo žymos arba pasirašyto sąrašo.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.3-2 **Žmonės žino savo indėlį į ISMS rezultatyvumą ir geresnių informacijos saugumo veiklos rezultatų naudą.**

Iš ko tai galima atpažinti: Mokymo medžiaga ir dalyvių sąrašai, kuriuose matomas ryšys su paties darbuotojo darbu. Auditoriai kalbina darbuotojus tiesiogiai, todėl mokykite konkrečiais kasdieniais pavyzdžiais, o ne abstrakčiomis standarto ištraukomis.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.3-3 **Žmonės žino ISMS reikalavimų nesilaikymo padarinius.**

Iš ko tai galima atpažinti: Padarinius nurodykite mokymo skaidrėse ir darbo instrukcijose ir susiekite juos su A.6.4 procesu. Net organizacijos be darbuotojų tai nustato rangovams ir laisvai samdomiems specialistams jų sutartyse.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.4-1 **ISMS svarbi vidaus ir išorės komunikacija yra nustatyta: kas komunikuojama, kada, su kuo ir kokiomis priemonėmis.**

Iš ko tai galima atpažinti: Komunikacijos matrica su tokiomis eilutėmis kaip pranešimas klientams apie saugumo incidentą, pranešimas priežiūros institucijai per 72 valandas, mėnesinė būklės ataskaita vadovybei. Ji yra krizių komunikacijos pagrindas ir peržiūrima po kiekvieno incidento.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.5.1-1 **ISMS apima standarto reikalaujamą dokumentuotą informaciją ir dokumentuotą informaciją, kurią organizacija yra pripažinusi reikalinga ISMS rezultatyvumui.** Dokumentas

Iš ko tai galima atpažinti: Dokumentų rodyklė, kurioje išvardytas kiekvienas ISMS dokumentas su paskirtimi, savininku, versija ir saugojimo vieta. Ji parodo, kad privalomi dokumentai yra visi, ir yra greičiausias auditoriaus įėjimo taškas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.5.2-1 **Kuriant ir atnaujinant dokumentus yra užtikrintas tinkamas identifikavimas, formatas ir laikmena, o dokumentai yra peržiūrimi ir patvirtinami dėl tinkamumo.**

Iš ko tai galima atpažinti: Vienoda dokumento antraštė su pavadinimu, versija, data, autoriumi ir tvirtinančiu asmeniu. Git pagrindu veikiančiose aplinkose sujungimo prašymų peržiūros su pritarimu tenkina peržiūros ir patvirtinimo reikalavimą, jeigu istorija yra nekeičiama.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.5.3-1 **Dokumentuota informacija yra prieinama ir tinkama naudoti ten ir tada, kai jos reikia.**

Iš ko tai galima atpažinti: Centrinė saugojimo vieta, pasiekiama visiems turintiems teisę, su paieškos funkcija. Tikrinama atrankiniu būdu: bet kurią darbo instrukciją galima rasti greičiau nei per minutę.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

7.5.3-2 **Dokumentuota informacija yra tinkamai apsaugota, ypač nuo konfidencialumo praradimo, netinkamo naudojimo ir vientisumo praradimo.**

Iš ko tai galima atpažinti: Vaidmenimis pagrįstos prieigos teisės prie ISMS dokumentų, versijų tvarkymas su istorija, patvirtintų versijų apsauga nuo rašymo ir dokumentų saugyklos atsarginė kopija. Dažniausiai pamirštamas būtent atsarginės kopijos įrodymas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

7.5.3-3 **Dokumentuotos informacijos platinimas, prieiga, paieška, saugojimas, pakeitimų valdymas, taip pat saugojimo trukmė ir tvarkymas pasibaigus terminui yra reglamentuoti.**

Iš ko tai galima atpažinti: Trumpa dokumentų valdymo taisyklė su saugojimo terminais ir naikinimo nuostatomis. Ji suderinama su teisinėmis prievolėmis (komercinė teisė, mokesčių teisė, GDPR) ir yra pagrindas A.5.33 ir A.8.10 punktams.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

7.5.3-4 **Išorės kilmės dokumentuota informacija, reikalinga ISMS planuoti ir eksploatuoti, yra nustatyta ir valdoma.**

Iš ko tai galima atpažinti: Išorės dokumentų sąrašas su versija ir šaltiniu: standartai, teisės aktai, gamintojų apsaugos sugriežtinimo vadovai, debesijos saugumo dokumentacija, duomenų tvarkymo sutartys. Be nuorodos į versiją valdymo įrodyti neįmanoma.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

8 Veikla 8

8.1-1 **Procesai, reikalingi informacijos saugumo reikalavimams tenkinti ir 6 skyriaus veiksmams įgyvendinti, yra suplanuoti, įdiegti ir valdomi, o šiems procesams yra nustatyti kriterijai.**

Iš ko tai galima atpažinti: Eksploatavimo vadovas arba veiksmų aprašai su aiškiais kriterijais, pavyzdžiui, ilgiausias laikas kritinėms pataisoms įdiegti, laidos išleidimo kriterijai, įspėjimų ribos. Kriterijai be skaičių audite yra bevertiai.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

8.1-2 **Dokumentuota informacija yra prieinama tiek, kiek reikia pasitikėti, kad procesai buvo vykdomi taip, kaip suplanuota.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra veiklos įrašai: užduočių istorija, CI konvejerio vykdymai, pataisų ataskaitos, atsarginių kopijų žurnalai, prieigos peržiūros. Šie įrašai yra tikrasis rezultatyvumo įrodymas 2 etapo audite.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

8.1-3 **Suplanuoti pakeitimai yra valdomi, o neplanuotų pakeitimų padariniai yra peržiūrimi; prireikus neigiamas poveikis yra sumažinamas.**

Iš ko tai galima atpažinti: Pakeitimų procesas su pritarimu ir grįžimo į ankstesnę būseną keliu, susietas su A.8.32. Neplanuotus pakeitimus (netinkama konfigūracija, atsitiktinis teisių išplėtimas) dokumentuokite kaip incidentą ir įrodykite pataisymą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

8.1-4 **Iš išorės teikiami procesai, produktai ir paslaugos, svarbūs ISMS, yra nustatyti ir valdomi.**

Iš ko tai galima atpažinti: Tiekėjų sąrašas su svarbos lygiu, sutarties nuoroda ir įrodymų būkle (teikėjo ISO 27001 sertifikatas, SOC 2 ataskaita, duomenų tvarkymo sutartis). Mažoms organizacijoms tai yra didžiausias svertas, nes didžioji dalis informacinių technologijų vis tiek veikia išorėje.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

8.2-1 **Rizikos vertinimai yra atliekami suplanuotais intervalais ir įvykus reikšmingiems pakeitimams arba incidentams, atsižvelgiant į nustatytus kriterijus.**

Iš ko tai galima atpažinti: Nustatytas ritmas (paprastai kartą per metus) ir apibrėžtos priežastys neplanuotiems vertinimams. Įrodymas yra rizikų registro versijos su datomis ir įrašai kalendoriuje arba užduočių sistemoje.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

8.2-2 **Rizikos vertinimų rezultatai yra saugomi kaip dokumentuota informacija.** Dokumentas

Iš ko tai galima atpažinti: Ankstesnės rizikų registro versijos su datomis, o ne tik dabartinė būklė. Perrašius failą raidos įrodyti nebeįmanoma; versijų tvarkymas failų sistemoje arba Git tai išsprendžia.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

8.3-1 **Rizikos apdorojimo planas yra įgyvendinamas.**

Iš ko tai galima atpažinti: Palyginkite planą su tikrove: įvykdyti veiksmai su įgyvendinimo data ir konkrečiu artefaktu (konfigūracija, politika, sutartis). Neįvykdytiems veiksmams reikia dokumentuoto pagrindimo ir naujo termino.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

8.3-2 **Rizikos apdorojimo rezultatai yra saugomi kaip dokumentuota informacija.** Dokumentas

Iš ko tai galima atpažinti: Būklės ataskaitos arba užbaigti veiksmų punktai su nuoroda į įrodymą. Pakanka vien registro, jeigu kiekvienoje eilutėje yra užbaigimo data ir nuoroda į įrodymą.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9 Veiklos rezultatų vertinimas 21

9.1-1 **Yra nustatyta, ką reikia stebėti ir matuoti, įskaitant informacijos saugumo procesus ir valdymo priemones.**

Iš ko tai galima atpažinti: Rodiklių lentelė su valdomu kiekiu patikimų matų: neįdiegtų pataisų kiekis, MFA aprėptis, incidentų sprendimo trukmė, paskutinės atkūrimo patikros rezultatas, neuždaryti radiniai. Keli tikrai renkami rodikliai vertingesni už ilgą pageidavimų sąrašą.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.1-2 **Stebėsenos, matavimo, analizės ir vertinimo metodai yra nustatyti ir duoda pagrįstus rezultatus.**

Iš ko tai galima atpažinti: Kiekvienam rodikliui dokumentuokite duomenų šaltinį ir skaičiavimą, pavyzdžiui, išrašą iš pažeidžiamumų skaitytuvo arba iš tapatybės teikėjo ataskaitos. Šaltinio atsekamumas yra pagrįstumo esmė.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.1-3 **Yra nustatyta, kada ir kas atlieka stebėseną ir matavimą ir kada rezultatai yra analizuojami ir vertinami.**

Iš ko tai galima atpažinti: Į rodiklių lentelę įtraukite dažnumo ir atsakingo asmens stulpelius. Pasikartojantis kalendoriaus įrašas vertinimui reguliarumą įrodo geriau nei bet koks aprašymas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.1-4 **Stebėsenos ir matavimo rezultatai yra saugomi kaip dokumentuota informacija.** Dokumentas

Iš ko tai galima atpažinti: Suarchyvuoti vertinimai, išsaugotos ataskaitų skydelių kopijos arba rodiklių lentelė, tvarkoma kaip laiko eilutė. Tiesioginis rodinys be istorijos reikalavimo netenkina.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.1-5 **Informacijos saugumo veiklos rezultatai ir ISMS rezultatyvumas yra vertinami remiantis matavimo rezultatais.**

Iš ko tai galima atpažinti: Rašytinis vertinimas, o ne vien skaičiai: tendencija, priežastys, veiksmų poreikis. Šis vertinimo tekstas kartu yra ir vadovybinės vertinamosios analizės įvestis.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

9.2.1-1 **Vidaus auditai yra atliekami suplanuotais intervalais ir suteikia informacijos, ar ISMS atitinka pačios organizacijos reikalavimus ir standarto reikalavimus ir ar yra rezultatyviai įdiegta.**

Iš ko tai galima atpažinti: Prieš sertifikavimo auditą baigiamas bent vienas visas vidaus audito ciklas, apimantis visą taikymo sritį. Be jo sertifikavimas nepasiekiamas; tai viena dažniausių kliūčių pirmojo sertifikavimo metu.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

9.2.2-1 **Audito programa yra suplanuota, sukurta ir palaikoma; joje nustatytas dažnumas, metodai, atsakomybės, planavimo reikalavimai ir ataskaitų teikimas, taip pat atsižvelgta į susijusių procesų svarbą ir ankstesnių auditų rezultatus.**

Iš ko tai galima atpažinti: Kelerių metų audito programa, per sertifikavimo ciklą apimanti visus skyrius ir visas taikomas valdymo priemones, su didesniu dažnumu kritinėse srityse. Visiškai pakanka paprastos trejų metų lentelės.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

9.2.2-2 **Kiekvienam auditui yra nustatyti audito kriterijai ir audito apimtis.**

Iš ko tai galima atpažinti: Audito planas kiekvienai datai su kriterijais (standartas, vidaus politikos, sutartys) ir aiškia apimtimi. Pakanka vieno puslapio audito plano kiekvienam auditui, jis kartu tinka ir kaip ataskaitos pagrindas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

9.2.2-3 **Auditoriai yra parinkti, o auditai atliekami taip, kad būtų užtikrintas objektyvumas ir nešališkumas. Niekas neaudituoja savo paties darbo.**

Iš ko tai galima atpažinti: Nepriklausomumas čia yra sunkiausia kliūtis: kas parašė politikas ir sukonfigūravo sistemas, tas jų neaudituoja. Labai mažose organizacijose tai beveik visada reiškia išorinį vidaus auditorių, pavyzdžiui, pagal sutartį dirbantį konsultantą arba kolegą iš partnerės įmonės; įrodymas yra audito sutartis ir auditoriaus nepriklausomumo deklaracija. Tik pakankamai didelėse komandose vaidmuo viduje perduodamas asmeniui, neatsakingam už audituojamą sritį, ir tai tuomet parodoma vaidmenų matricoje.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

9.2.2-4 **Audito rezultatai yra pateikiami atitinkamai vadovybei.**

Iš ko tai galima atpažinti: Audito ataskaita su radiniais, neatitiktimis, rekomendacijomis ir platinimo sąrašu bei perdavimo vadovybei įrodymas, pavyzdžiui, protokolo punktas arba elektroninio laiško perdavimas su data.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

9.2.2-5 **Dokumentuota informacija apie audito programą ir audito rezultatus yra saugoma.** Dokumentas

Iš ko tai galima atpažinti: Audito programą, audito planus, audito ataskaitas ir iš jų kylančius veiksmus laikykite vienoje vietoje. Ryšys nuo radinio iki koregavimo veiksmo (10.2 skyrius) matomas nuo pradžios iki pabaigos.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

9.3.1-1 **Aukščiausioji vadovybė suplanuotais intervalais analizuoja ISMS, kad užtikrintų nuolatinį jos tinkamumą, pakankamumą ir rezultatyvumą.**

Iš ko tai galima atpažinti: Bent kartą per metus ir suplanuotai prieš išorės auditą. Net labai mažose organizacijose parengiami pasirašyti protokolai su data, net ir tada, kai vadovybė ir ISMS savininkas yra tas pats asmuo.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.3.2-1 **Vadovybinė vertinamoji analizė apima ankstesnių vadovybinių vertinamųjų analizių veiksmų būklę.**

Iš ko tai galima atpažinti: Protokolas pradedamas praėjusių metų sprendimų ir jų dabartinės būklės sekimo lentele. Be šios nuorodos atgal analizė laikoma neišsamia.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.3.2-2 **Vadovybinė vertinamoji analizė apima ISMS svarbių išorės ir vidaus klausimų pokyčius, įskaitant svarbius klimato kaitos aspektus.**

Iš ko tai galima atpažinti: Atskiras darbotvarkės punktas su nuoroda į atnaujintą aplinkos analizę. Klimato kaita šio skyriaus tekste tiesiogiai neįvardyta (Amd 1:2024 keičia tik 4.1 ir 4.2), tačiau ji patenka čia per 4.1 klausimų pokyčius, ir auditoriai to tikisi. Net išvada, kad tai nesvarbu ir nepasikeitė, įrašoma į protokolą.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.3.2-3 **Vadovybinė vertinamoji analizė apima ISMS svarbių suinteresuotųjų šalių poreikių ir lūkesčių pokyčius.**

Iš ko tai galima atpažinti: Nauji klientų reikalavimai iš sutarčių ir saugumo klausimynų, naujos teisinės prievolės, sertifikavimo įstaigos reikalavimai. Užrašykite juos protokole kaip sąrašą su šaltiniais.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.3.2-4 **Vadovybinė vertinamoji analizė apima grįžtamąjį ryšį apie informacijos saugumo veiklos rezultatus, įskaitant neatitiktis ir koregavimo veiksmus, stebėsenos ir matavimo rezultatus, auditų rezultatus ir informacijos saugumo tikslų įgyvendinimą.**

Iš ko tai galima atpažinti: Šiuos keturis blokus tvarkykite kaip atskirus darbotvarkės punktus, kitaip vieno iš jų protokole vėliau trūks. Rodiklių lentelę, audito ataskaitą ir tikslų lentelę pridėkite kaip priedus.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.3.2-5 **Vadovybinė vertinamoji analizė apima suinteresuotųjų šalių grįžtamąjį ryšį.**

Iš ko tai galima atpažinti: Su saugumu susiję klientų skundai, klientų auditų rezultatai, pranešimai iš pranešėjų kanalo, paslaugų teikėjų grįžtamasis ryšys. Įrašykite tai į protokolą net ir tada, kai išvada yra, kad tokių nebuvo gauta.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.3.2-6 **Vadovybinė vertinamoji analizė apima rizikos vertinimo rezultatus ir rizikos apdorojimo plano būklę.**

Iš ko tai galima atpažinti: Pridėkite dabartinį rizikų registrą ir apdorojimo plano įgyvendinimo būklę su aiškiu rizikų savininkų patvirtinimu, kad likutinės rizikos priimtos.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.3.2-7 **Vadovybinė vertinamoji analizė apima nuolatinio gerinimo galimybes.**

Iš ko tai galima atpažinti: Darbotvarkės punktas su konkrečiomis gerinimo idėjomis ir sprendimu dėl kiekvienos. Priimtos idėjos perkeliamos į gerinimo registrą kaip įrašai su terminais.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.3.3-1 **Vadovybinės vertinamosios analizės rezultatai apima sprendimus dėl nuolatinio gerinimo galimybių ir dėl ISMS pakeitimų poreikio.**

Iš ko tai galima atpažinti: Protokolas baigiamas sprendimų skyriumi: sprendimas, atsakingas asmuo, terminas. Protokolas be sprendimų audite tampa radiniu, nes tada trūksta lyderystės poveikio.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

9.3.3-2 **Dokumentuota informacija yra saugoma kaip vadovybinės vertinamosios analizės rezultatų įrodymas.** Dokumentas

Iš ko tai galima atpažinti: Pasirašytas protokolas su data, dalyviais, įvestimis, vertinimu ir sprendimais. Tai vienas pirmųjų dokumentų, kurių sertifikavimo įstaiga prašo 1 etape.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

10 Gerinimas 7

10.1-1 **ISMS tinkamumas, pakankamumas ir rezultatyvumas yra nuolat gerinami.**

Iš ko tai galima atpažinti: Gerinimo registras, papildomas iš kelių šaltinių (auditai, incidentai, idėjos, rodiklių nuokrypiai), su matoma pažanga laikui bėgant. Įrodymas yra tęstinumas per kelis mėnesius, o ne įrašų gausa.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

10.2-1 **Atsiradus neatitikčiai organizacija į ją reaguoja: ją suvaldo, pataiso ir tvarko jos padarinius.**

Iš ko tai galima atpažinti: Neatitikties pranešimas su neatidėliotinu veiksmu ir data. Šaltiniai yra vidaus auditai, išorės auditai, incidentai ir kasdienės veiklos pastebėjimai; jie visi papildo tą patį registrą.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

10.2-2 **Yra įvertinta, ar reikia veiksmų priežastims pašalinti, kad neatitiktis nepasikartotų ir neatsirastų kitur; tai apima patikrinimą, ar panašių neatitikčių yra arba galėtų atsirasti.**

Iš ko tai galima atpažinti: Dokumentuokite pagrindinės priežasties analizę, pavyzdžiui, 5 Why arba Ishikawa metodu, ir aiškiai užrašykite išvadą dėl perkeliamumo į kitas sistemas arba procesus. Perkeliamumo žingsnis praleidžiamas dažniausiai.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

10.2-3 **Visi reikalingi koregavimo veiksmai yra įgyvendinti, o jų rezultatyvumas yra peržiūrėtas.**

Iš ko tai galima atpažinti: Prie kiekvieno veiksmo užrašykite įgyvendinimo datą, įrodymo artefaktą ir vėlesnę rezultatyvumo peržiūrą su jos data. Du datos laukai kiekvienoje eilutėje yra paprasčiausias būdas nepamesti rezultatyvumo peržiūros.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

10.2-4 **Prireikus dėl neatitikties ISMS yra pakeičiama.**

Iš ko tai galima atpažinti: Jei neatitiktis kyla iš spragos politikoje, rizikų registre arba SoA, pakeitimas tampa matomas būtent ten. Nuoroda nuo neatitikties į atnaujintą dokumento versiją uždaro grandinę.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

10.2-5 **Koregavimo veiksmai atitinka nustatytų neatitikčių poveikį.**

Iš ko tai galima atpažinti: Registre nurodytas sunkumo lygis, iš kurio matomas veiksmo proporcingumas. Nei smulkmenos tvarkomos kaip projektas, nei į rimtus nuokrypius atsakoma vien priminimo laišku.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

10.2-6 **Dokumentuota informacija apie neatitikčių pobūdį, dėl jų atliktus veiksmus ir koregavimo veiksmų rezultatus yra saugoma.** Dokumentas

Iš ko tai galima atpažinti: Neatitikčių ir koregavimo veiksmų registras su stulpeliais pobūdžiui, priežasčiai, veiksmui, atsakingam asmeniui, terminui ir rezultatyvumo peržiūros rezultatui. Tai privalomas įrodymas, prašomas per kiekvieną priežiūros auditą.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5 A priedas: organizacinės valdymo priemonės 37

A.5.1 **Informacijos saugumo politikos: bendroji informacijos saugumo politika ir teminės politikos yra nustatytos, vadovybės patvirtintos, komunikuotos ir peržiūrimos suplanuotais intervalais bei įvykus reikšmingiems pokyčiams.** Dokumentas

Iš ko tai galima atpažinti: Politikų rinkinys su versija, patvirtinimo data ir kitos peržiūros data bei susipažinimo įrodymai. Mažoms organizacijoms pakanka bendrosios politikos ir kelių teminių politikų (prieiga, kriptografija, nuotolinis darbas, incidentai).

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5.2 **Informacijos saugumo vaidmenys ir atsakomybės: informacijos saugumo vaidmenys ir atsakomybės yra nustatyti ir paskirstyti pagal organizacijos poreikius.**

Iš ko tai galima atpažinti: Vaidmenų matrica su įvardytais asmenimis, juos pavaduojančiais asmenimis ir užduotimis. Labai mažose organizacijose atvirai nurodykite, kur keli vaidmenys susikaupia viename asmenyje, ir susiekite tai su kompensuojamosiomis valdymo priemonėmis pagal A.5.3.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5.3 **Pareigų atskyrimas: pareigos ir atsakomybės sritys, kurios viena kitą kontroliuoja, nėra sutelktos viename asmenyje. Tikslas yra toks, kad niekas negalėtų vienas inicijuoti, patvirtinti ir nuslėpti pakeitimo.**

Iš ko tai galima atpažinti: Mažose organizacijose visiškas atskyrimas struktūriškai neįmanomas; bendras teiginys apie atitiktį audito pokalbyje subyra iš karto. Atlaiko sąžininga analizė: kurie pareigų deriniai yra kritiniai (kurti ir išleisti laidą, suteikti teises ir jomis naudotis, inicijuoti ir tvirtinti mokėjimus), kurie iš jų sutelkti viename asmenyje ir kurios kompensuojamosios valdymo priemonės taikomos. Pasiteisinę sprendimai yra nekeičiami audito žurnalai, prieinami trečiajai šaliai, MFA privilegijuotoms paskyroms, automatiniai CI vartai ir šakų apsauga vietoj keturių akių peržiūros, periodinė žurnalų peržiūra, kurią atlieka išorės asmuo, ir atskiras mokėjimų tvirtinimas. Analizę ir kompensuojamąsias valdymo priemones laikykite kaip atskirą dokumentą su data ir susiekite jį iš SoA.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5.4 **Vadovybės atsakomybės: vadovybė reikalauja, kad visi darbuotojai taikytų informacijos saugumą pagal nustatytas politikas ir procedūras.**

Iš ko tai galima atpažinti: Įsipareigojimas darbo ir rangos sutartyse, susipažinimas su politikomis įvedant į darbą ir reguliarūs vadovybės priminimai. Įrodymas yra pasirašyti įsipareigojimai ir susirinkimų protokolai.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5.5 **Ryšiai su institucijomis: tinkami ryšiai su svarbiomis institucijomis yra palaikomi ir prireikus pasiekiami.**

Iš ko tai galima atpažinti: Kontaktų sąrašas su kompetentinga duomenų apsaugos institucija, policija arba elektroninių nusikaltimų padaliniu, nacionaliniu kibernetinio saugumo pranešimų punktu ir, kai tai patenka į taikymo sritį, NIS2 pranešimų kanalais. Terminus (pavyzdžiui, 72 valandas pagal GDPR) užrašykite tiesiai sąraše.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.6 **Ryšiai su specialiomis interesų grupėmis: ryšiai su specialiomis interesų grupėmis, saugumo forumais ir profesinėmis asociacijomis yra palaikomi.**

Iš ko tai galima atpažinti: Narystės, prenumeruojami įspėjimai (nacionalinis CERT, gamintojų srautai), dalyvavimas specialiose interesų grupėse. Paprastas įrodymas yra prenumeratų sąrašas ir vienas pavyzdys, kaip įspėjimas virto veiksmu.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.7 **Grėsmių žvalgyba: informacija apie informacijos saugumo grėsmes yra renkama ir analizuojama, kad iš jos būtų išvesti tinkami veiksmai.**

Iš ko tai galima atpažinti: Nauja 2022 metų leidime. Mažoms organizacijoms tinka toks kelias: prenumeruoti nacionalinio CERT ir gamintojų įspėjimus, o paskui kas mėnesį atlikti trumpą peržiūrą su sprendimu dėl svarbos ir iš jo kylančiomis užduotimis. Įrodymas yra analizė, o ne prenumerata.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.8 **Informacijos saugumas projektų valdyme: informacijos saugumas yra integruotas į projektų valdymą, nepriklausomai nuo projekto rūšies.**

Iš ko tai galima atpažinti: Saugumo punktai projekto kontroliniame sąraše: apsaugos poreikiai, rizikos peržiūra, duomenų apsaugos patikra, saugumo pritarimas prieš paleidimą. Judriose komandose įtvirtinkite juos kaip nuolatinius punktus pasirengimo apibrėžtyje ir baigtumo apibrėžtyje.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.9 **Informacijos ir kito susijusio turto sąrašas: informacijos ir kito susijusio turto sąrašas su įvardytais savininkais yra sudarytas ir palaikomas.**

Iš ko tai galima atpažinti: Turto sąrašas, apimantis aparatinę įrangą, programinę įrangą, debesijos paslaugas, duomenų saugyklas, interneto sritis (domenus) ir paskyras, kiekvieną su savininku ir apsaugos poreikiais. Mažose organizacijose jį galima surinkti automatiškai iš MDM išrašo, licencijų sąrašo ir debesijos valdymo pulto; dabartinė data yra privaloma.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.10 **Priimtinas informacijos ir kito susijusio turto naudojimas: informacijos ir kito susijusio turto priimtino naudojimo ir tvarkymo taisyklės yra nustatytos, dokumentuotos ir įdiegtos.** Dokumentas

Iš ko tai galima atpažinti: Priimtino naudojimo politika įrenginiams, tinklams, debesijos paskyroms ir dirbtinio intelekto įrankiams su susipažinimo patvirtinimu. Asmeninius įrenginius ir išorės dirbtinio intelekto paslaugas aprėpkite aiškiai, nes būtent ten nuteka daugiausia duomenų.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.11 **Turto grąžinimas: pasibaigus arba pasikeitus darbo santykiams yra reglamentuota ir raštu patvirtinama, kad visi išduoti įrenginiai, raktai, paskyros ir dokumentai yra grąžinti.**

Iš ko tai galima atpažinti: Išėjimo iš darbo kontrolinis sąrašas su grąžinimo patvirtinimu nešiojamajam kompiuteriui, atpažinimo raktams, raktams, sertifikatams ir laikmenoms bei paskyrų išjungimas tą pačią dieną. Tai lygiai taip pat taikoma laisvai samdomiems specialistams ir praktikantams.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.12 **Informacijos klasifikavimas: informacija yra klasifikuojama pagal jos apsaugos poreikius konfidencialumo, vientisumo, prieinamumo ir teisinių reikalavimų atžvilgiu.**

Iš ko tai galima atpažinti: Paprasta schema su trimis arba keturiais lygiais (vieša, vidaus, konfidenciali, griežtai konfidenciali) ir konkrečiomis tvarkymo taisyklėmis kiekvienam lygiui. Priskyrimą užrašykite turto sąraše arba duomenų tvarkymo veiklos įrašuose.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.13 **Informacijos ženklinimas: klasifikavimo lygis atpažįstamas pačiame dokumente, faile arba pranešime, todėl gavėjai žino, kaip su juo elgtis, ir jiems nereikia klausti.**

Iš ko tai galima atpažinti: Ženklinimas dokumento antraštėje, failo pavadinime, elektroninio laiško temoje arba jautrumo žymomis debesijos biuro programose. Įrodymas yra tikrai paženklintų dokumentų pavyzdžiai, o ne vien taisyklė.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.14 **Informacijos perdavimas: informacijos perdavimo organizacijos viduje ir su išorės šalimis taisyklės, procedūros ir susitarimai yra sukurti.**

Iš ko tai galima atpažinti: Taisyklė, nurodanti, kuris kanalas leidžiamas kuriam klasifikavimo lygiui: šifruotas elektroninis laiškas arba duomenų kambarys konfidencialiam turiniui, jokio siuntimo per asmenines žinučių programas. Konfidencialius perdavimus paremkite konfidencialumo susitarimais.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.15 **Prieigos valdymas: taisyklės, valdančios fizinę ir loginę prieigą prie informacijos ir kito susijusio turto, yra sukurtos ir įdiegtos remiantis veiklos ir saugumo reikalavimais.**

Iš ko tai galima atpažinti: Prieigos valdymo politika, paremta būtinumo žinoti ir mažiausios privilegijos principais, su vaidmenų ir teisių susiejimu. Įrodymas yra tikroji teisių konfigūracija tapatybės teikėjo sistemoje, o ne vien politika.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.16 **Tapatybių valdymas: visas tapatybių būvio ciklas yra valdomas.**

Iš ko tai galima atpažinti: Procesas nuo sukūrimo per pakeitimą iki išjungimo, geriausia sutelktas tapatybės teikėjo sistemoje su vieningu prisijungimu (SSO). Jokių bendrai naudojamų grupinių paskyrų; kai techniškai neišvengiama, paskyrą įvardykite, pagrįskite ir registruokite jos naudojimą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.17 **Autentifikavimo informacija: autentifikavimo informacijos suteikimas ir tvarkymas yra valdomas per valdymo procesą, kuris reikalauja iš žmonių tinkamo elgesio su ja.**

Iš ko tai galima atpažinti: Slaptažodžių tvarkyklė kaip privalomas įrankis, politika dėl slaptažodžių kokybės ir MFA, saugi pirminė prieiga ir slaptažodžio nustatymo iš naujo procedūra su tapatybės patikra. Įrodymas yra konfigūracijos ekrano nuotraukos ir slaptažodžių tvarkyklės ataskaita.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.18 **Prieigos teisės: prieigos teisės yra suteikiamos, peržiūrimos, keičiamos ir panaikinamos pagal prieigos valdymo politiką.**

Iš ko tai galima atpažinti: Periodinė prieigos peržiūra bent kartą per metus su dokumentuotu rezultatu kiekvienai paskyrai ir panaikintų teisių įrodymu. Teisių panaikinimą išėjimo dieną auditoriai mėgsta atsekti per konkretų atvejį.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.19 **Informacijos saugumas santykiuose su tiekėjais: procesai ir procedūros saugumo rizikoms, kylančioms naudojant trečiųjų šalių produktus ir paslaugas, valdyti yra nustatyti ir įdiegti.**

Iš ko tai galima atpažinti: Tiekėjų sąrašas su svarbos lygiu ir vertinimo gyliu. Kritiniams teikėjams surinkite įrodymus (ISO 27001 sertifikatas, SOC 2 ataskaita), o ne atlikinėkite savo auditus; mažoms organizacijoms tai vienintelis realus kelias.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.20 **Informacijos saugumas tiekėjų sutartyse: su kiekvienu tiekėju yra suderinti svarbūs saugumo reikalavimai ir jie įrašyti į sutartis.**

Iš ko tai galima atpažinti: Informacijos saugumo sutarties priedas su pareiga pranešti apie incidentus, nuostatomis dėl pasitelktų duomenų tvarkytojų, naikinimo prievolėmis ir audito teisėmis. Standartinėms paslaugoms pakanka teikėjo sąlygų ir duomenų tvarkymo sutarties, jeigu jų turinys yra peržiūrėtas ir dokumentuotas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.21 **Informacijos saugumo valdymas informacinių ir ryšių technologijų tiekimo grandinėje: procesai saugumo rizikoms šioje tiekimo grandinėje valdyti yra nustatyti ir įdiegti.**

Iš ko tai galima atpažinti: Tai apima programinės įrangos priklausomybes ir pačių teikėjų subtiekėjus. Praktiškai: programinės įrangos sudėties sąrašas (SBOM) arba priklausomybių sąrašas, automatiniai pažeidžiamų paketų patikrinimai CI ir programinės įrangos gavimas tik iš pasirašytų arba oficialių kanalų.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.22 **Tiekėjų paslaugų stebėsena, peržiūra ir pakeitimų valdymas: tiekėjų paslaugų pakeitimai yra reguliariai stebimi, peržiūrimi ir valdomi.**

Iš ko tai galima atpažinti: Metinė tiekėjų peržiūra, kurioje vertinami incidentai, prieinamumo ataskaitos ir sertifikatų galiojimas, bei kanalas teikėjo skelbiamiems pakeitimams. Rezultatą užrašykite kaip trumpą pastabą kiekvienam tiekėjui.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.23 **Informacijos saugumas naudojant debesijos paslaugas: debesijos paslaugų įsigijimo, naudojimo, valdymo ir atsisakymo procesai yra sukurti pagal saugumo reikalavimus.**

Iš ko tai galima atpažinti: Nauja 2022 metų leidime ir pagrindinė valdymo priemonė mažoms debesija paremtoms organizacijoms. Įrodymas yra debesijos politika su naujų paslaugų tvirtinimo procesu, dokumentuotas kiekvienos paslaugos bendros atsakomybės modelis, apsaugos sugriežtinimo nuostatos ir pasitraukimo strategija su duomenų grąžinimu ir naikinimo patvirtinimu.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.24 **Informacijos saugumo incidentų valdymo planavimas ir pasirengimas: incidentų tvarkymo procesai, vaidmenys ir atsakomybės yra suplanuoti ir nustatyti.** Dokumentas

Iš ko tai galima atpažinti: Reagavimo į incidentus planas su pranešimo keliu, vaidmenimis, eskalavimo lygiais, kontaktais ne darbo metu ir komunikacijos šablonais. Mažoms komandoms realistiška: vienas puslapis, bet išbandytas praktikoje.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.25 **Informacijos saugumo įvykių vertinimas ir sprendimas dėl jų: saugumo įvykiai yra vertinami ir priimamas sprendimas, ar juos priskirti informacijos saugumo incidentams.**

Iš ko tai galima atpažinti: Atrankos kriterijai su sunkumo matrica ir įvykių registras, kuriame su pagrindimu įrašomi ir atmesti įvykiai. Registre matomas skirtumas tarp įvykio ir incidento.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.26 **Reagavimas į informacijos saugumo incidentus: incidentai yra tvarkomi pagal dokumentuotas procedūras.**

Iš ko tai galima atpažinti: Incidentų bylos su laiko juosta, atliktais veiksmais, dalyvavusiais asmenimis ir uždarymo sprendimu. Jeigu tikro incidento dar nebuvo, geriausias įmanomas įrodymas yra dokumentuotos stalo pratybos.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5.27 **Mokymasis iš informacijos saugumo incidentų: iš incidentų įgytos žinios naudojamos saugumo valdymo priemonėms stiprinti.**

Iš ko tai galima atpažinti: Kaltės neieškanti peržiūra po incidento su pagrindinės priežasties analize ir iš jos kylančiais veiksmais, susieta su gerinimo registru ir prireikus su rizikų registru.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5.28 **Įrodymų rinkimas: yra reglamentuota, kaip su saugumo įvykiu susiję pėdsakai nustatomi, apsaugomi ir saugomi, kad vėliau liktų tinkami naudoti.**

Iš ko tai galima atpažinti: Trumpa įrodymų išsaugojimo procedūra: neatkurkite sistemų per anksti, apsaugokite atvaizdus ir žurnalus, dokumentuokite įrodymų perdavimo grandinę. Mažoms organizacijoms pakanka nustatyti sunkumo lygį, nuo kurio pasitelkiamas išorės ekspertizės teikėjas, ir jo kontaktinius duomenis.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5.29 **Informacijos saugumas veiklos sutrikimo metu: organizacija planuoja, kaip informacijos saugumas sutrikimo metu palaikomas tinkamu lygiu.**

Iš ko tai galima atpažinti: Ekstremaliųjų situacijų tvarka saugumo neišjungia. Dokumentuokite, kad MFA, įvykių registravimas ir prieigos apribojimai galioja ir atsarginio veikimo metu ir kad ekstremaliųjų situacijų paskyros (break-glass accounts) yra užantspauduotos, dokumentuotos ir vėliau peržiūrimos.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5.30 **Informacinių ir ryšių technologijų (IRT) parengtis veiklos tęstinumui: IRT parengtis yra suplanuota, įdiegta, palaikoma ir išbandyta remiantis veiklos tęstinumo tikslais ir IRT tęstinumo reikalavimais.**

Iš ko tai galima atpažinti: Nauja 2022 metų leidime. Įrodymas yra nustatyti atkūrimo trukmės tikslai (RTO) ir atkūrimo taško tikslai (RPO) kiekvienai kritinei sistemai, atkūrimo procedūra ir bent vienas dokumentuotas bandymas per metus. Stipriausias atskiras įrodymas yra sėkminga atkūrimo patikra su data ir trukme.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5.31 **Teisės aktų, reglamentavimo ir sutartiniai reikalavimai: svarbūs reikalavimai ir jų tenkinimo būdas yra nustatyti, dokumentuoti ir nuolat atnaujinami.** Dokumentas

Iš ko tai galima atpažinti: Teisės aktų registras, apimantis GDPR, elektroninių ryšių teisę, komercinę ir mokesčių teisę, o kai taikoma, NIS2 arba sektorines taisykles, kiekvienam su jį įgyvendinančia vidaus taisykle ir peržiūros data. Pakanka metinės peržiūros, tačiau ji pažymima data.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5.32 **Intelektinės nuosavybės teisės: tinkamos procedūros intelektinės nuosavybės teisėms apsaugoti yra įdiegtos.**

Iš ko tai galima atpažinti: Naudojamos programinės įrangos licencijų sąrašas, atvirojo kodo licencijų patikra produkte (licencijų skaitytuvas CI) ir taisyklė, kaip elgtis su trečiųjų šalių kodu ir sugeneruotu kodu. Įrodymas yra licencijų ataskaita iš kūrimo proceso.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.5.33 **Įrašų apsauga: veiklos ir įrodomieji įrašai saugomi taip, kad jų nebūtų galima prarasti ar nepastebimai pakeisti ir kad jie nepatektų į netinkamas rankas, ir tai galioja visą saugojimo laikotarpį.**

Iš ko tai galima atpažinti: Saugojimo terminų sąrašas su teisės aktų nustatytais terminais, klastojimui atspari saugykla, ribota prieiga ir atsarginė kopija. Mokesčiams svarbiems įrašams aiškiai nurodykite teisės aktų nustatytus saugojimo terminus, nes auditoriai mėgsta tikrinti būtent tai.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.34 **Privatumas ir asmens duomenų apsauga: privatumo ir asmens duomenų (PII) apsaugos reikalavimai yra nustatyti ir tenkinami pagal taikomus teisės aktus.**

Iš ko tai galima atpažinti: Duomenų tvarkymo veiklos įrašai, duomenų tvarkymo sutartys, naikinimo tvarka, duomenų subjektų teisių įgyvendinimo procesas ir, kai reikia, poveikio duomenų apsaugai vertinimas. Susiejus tai bendru turto sąrašu su ISMS, nereikia visko tvarkyti du kartus.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.35 **Nepriklausoma informacijos saugumo peržiūra: organizacijos informacijos saugumo valdymo būdas yra nepriklausomai peržiūrimas suplanuotais intervalais ir įvykus reikšmingiems pokyčiams.**

Iš ko tai galima atpažinti: Įrodymas yra vidaus auditas, atliktas nepriklausomo auditoriaus, išorės įsilaužimo testai arba pats sertifikavimo auditas. Nepriklausomai reiškia, kad peržiūros neatlieka asmuo, atsakingas už peržiūrimą sritį.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.36 **Informacijos saugumo politikų, taisyklių ir standartų laikymasis: pačios organizacijos saugumo politikų ir taikomų taisyklių laikymasis yra reguliariai peržiūrimas.**

Iš ko tai galima atpažinti: Atitikties patikros su data ir rezultatu, pavyzdžiui, konfigūracijos palyginimas su savo apsaugos sugriežtinimo baze, atrankinė dokumentų ženklinimo patikra, automatiniai politikos patikrinimai debesijoje. Nuokrypiai patenka į koregavimo veiksmų registrą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5.37 **Dokumentuotos eksploatavimo procedūros: informacijos apdorojimo priemonių eksploatavimo procedūros yra dokumentuotos ir prieinamos tiems, kuriems jų reikia.** Dokumentas

Iš ko tai galima atpažinti: Veiksmų aprašai atsarginėms kopijoms ir atkūrimui, diegimui, naudotojų administravimui, pataisų diegimui ir incidentų tvarkymui. Trumpa ir aktualu yra geriau nei išsamu ir pasenę; paskutinio pakeitimo data kiekviename apraše yra privaloma.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.6 A priedas: su žmonėmis susijusios valdymo priemonės 8

A.6.1 **Patikra: kandidatai, kurie dirbs organizacijai, yra iš anksto patikrinami neperžengiant teisės aktų ribų ir proporcingai apsaugos poreikiams; jautriems vaidmenims patikra kartojama darbo laikotarpiu.**

Iš ko tai galima atpažinti: Neturint darbuotojų šią valdymo priemonę galima pagrįstai laikyti šiuo metu netaikoma, tačiau procedūra darbuotojų priėmimo atvejui vis tiek nustatoma ir pritaikomumo pareiškime pažymima kaip suplanuota. Įgyvendinama apimtis: tapatybės, gyvenimo aprašymo ir rekomendacijų patikrinimas bei pažymėjimai; teistumo patikra tik ten, kur tai pateisina apsaugos poreikiai ir leidžia teisės aktai. To paties lygio reikalaukite iš laisvai samdomų specialistų ir rangovų per jų sutartis, kitaip spraga atsiveria būtent ten.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.6.2 **Darbo sutarties sąlygos: sutartiniuose susitarimuose nurodytos darbuotojų ir organizacijos informacijos saugumo atsakomybės.**

Iš ko tai galima atpažinti: Saugumo sąlyga darbo arba paslaugų sutartyje su nuoroda į taikomas politikas. Laisvai samdomiems specialistams ta pati sąlyga paslaugų sutartyje ir konfidencialumo susitarimas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.6.3 **Informacijos saugumo sąmoningumas, švietimas ir mokymas: darbuotojai ir svarbios išorės šalys gauna tinkamą sąmoningumo ugdymą ir mokymą bei reguliarią informaciją apie organizacijos politikų pakeitimus.**

Iš ko tai galima atpažinti: Metinis mokymas su dalyvavimo įrodymu ir data, papildytas apgaulingų laiškų imitacijomis su įvertinta paspaudimų dalimi. Net vieniems savarankiškai dirbantiems asmenims reikia savo kvalifikacijos kėlimo įrodymų, pavyzdžiui, kursų patvirtinimų.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.6.4 **Drausminimo procesas: yra oficialus ir komunikuotas procesas, pagal kurį imamasi priemonių prieš saugumo politikas pažeidusius asmenis.**

Iš ko tai galima atpažinti: Neturint darbuotojų tai galima pagrįstai laikyti šiuo metu netaikoma, tačiau procesas darbuotojų priėmimo atvejui vis tiek nustatomas; nustoja galioti tik jo taikymas, o ne pati taisyklė. Reikalinga laipsniška ir komunikuota atsako eilė (pokalbis, pastaba, oficialus įspėjimas, atleidimas), atitinkanti darbo teisę ir darbuotojų atstovavimo taisykles. Rangovams sankcijų lygį įtvirtinkite sutartyje, pavyzdžiui, netesybas arba teisę nutraukti sutartį.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.6.5 **Atsakomybės pasibaigus darbo santykiams arba juos pakeitus: saugumo atsakomybės ir pareigos, liekančios galioti pasibaigus darbo santykiams arba pakeitus vaidmenį, yra nustatytos, įgyvendinamos ir pateiktos susijusiems asmenims.**

Iš ko tai galima atpažinti: Išėjimo iš darbo kontrolinis sąrašas su teisių panaikinimu, turto grąžinimu, perdavimu ir aiškiu priminimu apie toliau galiojančias konfidencialumo prievoles. Paprasčiausias įrodymas yra pasirašytas išėjimo pokalbio įrašas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.6.6 **Konfidencialumo arba neatskleidimo susitarimai: yra nustatyta, kas pasirašo konfidencialumo susitarimą. Turinys atitinka informacijos apsaugos poreikius, susitarimai yra pasirašyti, saugomi byloje ir reguliariai peržiūrimi, kad liktų aktualūs.**

Iš ko tai galima atpažinti: Pasirašyti konfidencialumo susitarimai darbuotojams, laisvai samdomiems specialistams, paslaugų teikėjams ir praktikantams su galiojimo po sutarties pabaigos terminu. Apžvalginė lentelė su kita šalimi, data ir galiojimu leidžia visą rinkinį audituoti.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.6.7 **Nuotolinis darbas: saugumo priemonės yra įdiegtos ten, kur žmonės dirba už organizacijos patalpų ribų ir tuo metu naudojasi organizacijos informacija.**

Iš ko tai galima atpažinti: Darbo namuose ir nuotolinio darbo politika su reikalavimais dėl disko šifravimo, ekrano užrakto, saugaus belaidžio tinklo, VPN arba nulinio pasitikėjimo prieigos naudojimo, privatumo ekranų ir draudimo be leidimo naudoti asmeninius įrenginius. Įrodymas yra galinių įrenginių MDM atitikties ataskaita.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.6.8 **Pranešimas apie informacijos saugumo įvykius: yra mechanizmas, per kurį žmonės gali laiku pranešti apie pastebėtus arba įtariamus saugumo įvykius.**

Iš ko tai galima atpažinti: Aiškiai paskelbtas pranešimų kanalas (pašto dėžutė, pokalbių kanalas, telefono numeris) su patikinimu, kad už sąžiningus pranešimus sankcijų nebus. Įrodymas yra pranešimų kiekis įvykių registre; nuolat tuščias registras audite yra įspėjamasis ženklas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.7 A priedas: fizinės valdymo priemonės 14

A.7.1 Fizinio saugumo perimetrai: saugumo perimetrai yra nustatyti ir naudojami sritims, kuriose yra informacija ir informacijos apdorojimo priemonės, apsaugoti.

Iš ko tai galima atpažinti: Perimetrų aprašymas su schema arba nuotraukomis: pastatas, biuras, serverių spinta. Dirbant namuose perimetras yra užrakinamas darbo kambarys arba, jo nesant, užrakinama spinta; geriau tai aprašyti nei praleisti.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.7.2 Fizinis patekimas: saugios sritys yra apsaugotos tinkamomis patekimo kontrolės priemonėmis ir patekimo taškais.

Iš ko tai galima atpažinti: Raktų arba kortelių registras su išdavimu ir grąžinimu ir lankytojų taisyklė su palydėjimu bei žurnalu. Naudojantis bendradarbystės erdve arba duomenų centru, kaip įrodymą imkite operatoriaus patekimo kontrolės priemones ir įtvirtinkite jas sutartimi.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.7.3 Biurų, patalpų ir įrenginių apsauga: biurų, patalpų ir įrenginių fizinė apsauga yra suprojektuota ir įdiegta.

Iš ko tai galima atpažinti: Užrakinamos durys, langų apsauga pirmame aukšte, jokių iš išorės matomų konfidencialių ekranų, jokios įmonės iškabos ant jautrių patalpų. Kaip įrodymo pakanka trumpo aprašymo ir nuotraukos.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.7.4 Fizinio saugumo stebėsena: patalpos yra nuolat stebimos dėl neteisėto fizinio patekimo.

Iš ko tai galima atpažinti: Nauja 2022 metų leidime. Galimybės yra signalizacija, judesio jutikliai, vaizdo stebėjimas arba patekimo žurnalai. Vaizdo stebėjimas tikrinamas dėl atitikties duomenų apsaugos reikalavimams; dirbant namuose pagrįsta alternatyva yra signalizacijos, rakinamo kambario ir išvados, kad jautrių serverių ten nelaikoma, derinys.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.7.5 Apsauga nuo fizinių ir aplinkos grėsmių: yra įdiegta apsauga nuo fizinių ir aplinkos grėsmių, tokių kaip stichinės nelaimės ir tyčinė arba netyčinė žala.

Iš ko tai galima atpažinti: Gaisro, vandens, karščio, elektros dingimo ir įsilaužimo peržiūra kartu su įdiegtomis priemonėmis (dūmų jutikliai, gesintuvai, jokios įrangos po vandentiekio vamzdžiais, atsarginė kopija saugoma kitoje vietoje). Būtent čia prisijungia klimato kaitos sprendimas iš 4.1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.7.6 Darbas saugiose srityse: priemonės darbui saugiose srityse yra suprojektuotos ir įdiegtos.

Iš ko tai galima atpažinti: Taisyklės serverių patalpai arba didelio konfidencialumo sritims: jokio neprižiūrimo trečiųjų šalių patekimo, jokio filmavimo kameromis arba mobiliaisiais įrenginiais, atliktų darbų registravimas. Jeigu saugių sričių nėra, tai pagrindžiama nuoroda į veiklą vien debesijoje.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.7.7 Tvarkingas darbo stalas ir užrakintas ekranas: taisyklės dėl tvarkingo darbo stalo, susijusios su popieriais ir keičiamosiomis laikmenomis, bei dėl užrakintų ekranų yra nustatytos ir jų laikomasi.

Iš ko tai galima atpažinti: Tai visa apimtimi galioja ir dirbant namuose, todėl netaikoma priemone paskelbti negalima. Įrodymas yra trumpa taisyklė (dokumentus rakinti, ekrano užraktas po penkių minučių, jokių lipnių lapelių su prisijungimo duomenimis) ir techniškai priverstinis užraktas įrenginių politika, kurios konfigūraciją galima eksportuoti.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.7.8 **Įrangos išdėstymas ir apsauga: įranga yra saugiai išdėstyta ir apsaugota.**

Iš ko tai galima atpažinti: Išdėstymas atokiau nuo praėjimų ir viešų zonų, jokio matomumo iš išorės, apsauga nuo karščio ir drėgmės, lyno spynos mobiliesiems įrenginiams. Pakanka trumpo aprašymo darbo namuose arba biuro politikoje.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.7.9 **Turto apsauga už patalpų ribų: už patalpų ribų esantis turtas yra apsaugotas.**

Iš ko tai galima atpažinti: Mažose organizacijose tai daugiausia nešiojamasis kompiuteris, išmanusis telefonas ir išorinės laikmenos, ir nuo šios priemonės išsisukti neįmanoma. Įrodymas yra priverstinis disko šifravimas, per MDM įjungtas nuotolinis duomenų ištrynimas, taisyklė nepalikti įrenginių transporto priemonėse ir nesijungti prie viešų tinklų be VPN bei pranešimo apie praradimą kelias. Patikimiausias atskiras įrodymas yra MDM atitikties ataskaita su šifravimo būsena kiekvienam įrenginiui.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.7.10 **Laikmenos: laikmenos yra valdomos visą jų būvio ciklą pagal klasifikavimo schemą ir tvarkymo reikalavimus, nuo įsigijimo per naudojimą ir gabenimą iki sunaikinimo.**

Iš ko tai galima atpažinti: Tai galioja net dirbant vien mobiliai, nes USB atmintinės, išoriniai diskai ir atsarginių kopijų laikmenos egzistuoja. Įrodymas yra laikmenų registras, šifruotos laikmenos, techniškai priverstinis nepatvirtintų keičiamųjų laikmenų draudimas, saugus laikymas rakinamoje vietoje ir perdavimas į A.7.14 pasibaigus naudojimo laikui.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.7.11 **Pagalbinės komunalinės paslaugos: informacijos apdorojimo priemonės yra apsaugotos nuo pagalbinių komunalinių paslaugų, ypač elektros tiekimo, sutrikimo.**

Iš ko tai galima atpažinti: Kai serveriai laikomi savo patalpose, nepertraukiamo maitinimo šaltinis su dokumentuotu bandymu. Veikiant vien debesijoje įrodymas yra nuoroda į teikėjo įsipareigojimus ir taisyklė, kaip toliau dirbti nutrūkus vietiniam elektros arba interneto tiekimui (mobilusis ryšys per telefoną, atsarginė vieta).

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.7.12 **Kabelių saugumas: elektros, duomenų ir ryšių kabeliai yra apsaugoti nuo pasiklausymo, trikdžių ir pažeidimų.**

Iš ko tai galima atpažinti: Kai kabeliai priklauso pačiai organizacijai, apsauga nuo pažeidimų ir nuo neteisėtos prieigos prie komutavimo skydų. Mažuose biuruose ir dirbant namuose pagrindimas yra trumpas, bet jis pateikiamas: maršruto parinktuvas ir tinklo lizdai nėra viešai pasiekiami, nenaudojami prievadai išjungti.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.7.13 **Įrangos priežiūra: įranga yra tinkamai prižiūrima, kad būtų užtikrintas informacijos prieinamumas, vientisumas ir konfidencialumas.**

Iš ko tai galima atpažinti: Priežiūros planas arba gamintojo palaikymo būsena kiekvienam įrenginiui ir taisyklė dėl trečiųjų šalių atliekamo remonto (pirma išimti laikmeną arba ištrinti duomenis ir sudaryti konfidencialumo susitarimą su teikėju). Palaikymo pabaigos datas sekite turto sąraše.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.7.14 **Saugus įrangos pašalinimas arba pakartotinis naudojimas: prieš perduodant, parduodant arba nurašant įrenginį su laikmena yra patikrinama ir užrašoma, kad jame nebeįmanoma atkurti nei saugomų duomenų, nei licencijuotos programinės įrangos.**

Iš ko tai galima atpažinti: Tai galioja ir dirbant namuose, ir nurašomiems asmeniniams įrenginiams, kurie buvo naudojami darbui. Įrodymas yra ištrynimo įrašas kiekvienam įrenginiui su serijos numeriu, data ir metodu (kriptografinis ištrynimas šifruotuose SSD diskuose, perrašymas, fizinis sunaikinimas) arba teikėjo išduotas sunaikinimo pažymėjimas. Šifruotiems įrenginiams pakanka dokumentuoto rakto sunaikinimo, jeigu procedūra yra aprašyta.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8 A priedas: technologinės valdymo priemonės 34

A.8.1 Naudotojų galiniai įrenginiai: informacija, laikoma naudotojų galiniuose įrenginiuose, juose apdorojama arba per juos pasiekiama, yra apsaugota.

Iš ko tai galima atpažinti: Apsaugos sugriežtinimo bazė kiekvienai operacinei sistemai, centrinis valdymas per MDM, disko šifravimas, automatiniai atnaujinimai ir ekrano užraktas. MDM atitikties ataskaita su būsena kiekvienam įrenginiui visa tai įrodo iš karto.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.2 Privilegijuotos prieigos teisės: privilegijuotų prieigos teisių suteikimas ir naudojimas yra ribojamas ir valdomas.

Iš ko tai galima atpažinti: Visų administratorių paskyrų sąrašas su pagrindimu, atskiros administratorių paskyros, nenaudojamos kasdieniam darbui, priverstinis MFA, ribotos trukmės teisių išplėtimas, kur tai įmanoma, ir periodinė peržiūra. Mažose organizacijose tai yra svarbiausia A.5.3 kompensuojamoji valdymo priemonė.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.3 Prieigos prie informacijos ribojimas: prieiga prie informacijos ir kito susijusio turto yra ribojama pagal nustatytą prieigos valdymo politiką.

Iš ko tai galima atpažinti: Teisių suteikimo tvarka, paremta vaidmenimis ir grupėmis, o ne pavieniais suteikimais, įrodoma narystės grupėse išrašu. Viešas bendrinimo nuorodas debesijos saugykloje reguliariai peržiūrėkite ir leiskite joms nustoti galioti.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.4 Prieiga prie pirminio kodo: skaitymo ir rašymo prieiga prie pirminio kodo, kūrimo įrankių ir programinės įrangos bibliotekų yra tinkamai valdoma.

Iš ko tai galima atpažinti: Saugyklos teisės pagal vaidmenis, apsaugotos pagrindinės šakos, privalomos peržiūros arba privalomi būsenos patikrinimai, jokio tiesioginio siuntimo į pagrindinę šaką. Įrodymas yra šakų apsaugos konfigūracija ir organizacijos narių sąrašas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.5 Saugus autentifikavimas: saugaus autentifikavimo technologijos ir procedūros yra įdiegtos remiantis prieigos apribojimais ir temine politika.

Iš ko tai galima atpažinti: MFA visai išorinei prieigai ir visoms administratorių paskyroms, apgaulei atsparūs metodai (slaptaraktai, FIDO2), kur tai įmanoma, ir užblokavimas po nesėkmingų bandymų. Įrodymas yra tapatybės teikėjo MFA aprėpties ataskaita.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.6 Pajėgumo valdymas: saugykla, skaičiavimo galia, pralaidumas ir licencijos yra stebimi, o poreikis derinamas pakankamai anksti, kad siauros vietos niekada negrėstų prieinamumui.

Iš ko tai galima atpažinti: Saugyklos, skaičiavimo apkrovos, licencijų kvotų ir debesijos biudžetų stebėsena su ribiniais įspėjimais. Mažose organizacijose pakanka įspėjimo dėl disko užimtumo ir dėl išlaidų ribų bei metinės pajėgumo apžvalgos.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.7 Apsauga nuo kenkėjiškos programinės įrangos: techninės apsaugos nuo kenkėjiškos programinės įrangos priemonės yra įjungtos ir atnaujintos, o įrenginius naudojantys žmonės apmokyti pakankamai, kad šių priemonių nesusilpnintų.

Iš ko tai galima atpažinti: Veikianti galinių įrenginių apsauga su centrine būsenos apžvalga, pašto filtras, tikrinantis priedus ir nuorodas, ir taisyklė, draudžianti paleisti nepatvirtintą programinę įrangą. Tiesioginis įrodymas yra apsaugos sprendimo būsenos ataskaita su data.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.8 **Techninių pažeidžiamumų valdymas: organizacija aktyviai sužino apie naudojamų technologijų pažeidžiamumus, dėl kiekvieno radinio nusprendžia, kiek yra paveikta, ir spragą uždaro per nustatytus terminus arba pagrindžia kitokį atsaką.**

Iš ko tai galima atpažinti: Pažeidžiamumų valdymas su šaltiniu (skaitytuvas, priklausomybių patikra CI, gamintojų įspėjimai), sunkumo įvertinimu ir nustatytais terminais kiekvienam lygiui, pavyzdžiui, kritiniams per 7 dienas. Įrodymas yra kelių skirtingų laiko momentų nuskaitymo ataskaitos, rodančios neuždarytų radinių mažėjimą.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.9 **Konfigūracijos valdymas: aparatinės įrangos, programinės įrangos, paslaugų ir tinklų konfigūracijos, įskaitant saugumo konfigūracijas, yra sukurtos, dokumentuotos, įdiegtos, stebimos ir peržiūrimos.**

Iš ko tai galima atpažinti: Nauja 2022 metų leidime. Įrodymas yra dokumentuotos bazinės konfigūracijos (apsaugos sugriežtinimo bazės) ir jų priverstinis taikymas, geriausia kaip infrastruktūra kodo pavidalu versijų valdyme arba per MDM profilius. Papildo nuokrypių aptikimas ir periodinis konfigūracijų palyginimas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.10 **Informacijos naikinimas: informacinėse sistemose, įrenginiuose ir laikmenose saugoma informacija yra sunaikinama, kai jos nebereikia.**

Iš ko tai galima atpažinti: Nauja 2022 metų leidime ir glaudžiai susieta su GDPR. Įrodymas yra naikinimo tvarka su saugojimo terminais kiekvienai duomenų kategorijai, techniškai įdiegtos saugojimo trukmės nuostatos debesijos paslaugose ir duomenų bazėse bei naikinimo žurnalai. Saugojimo terminas reikalingas ir atsarginėms kopijoms, ir žurnalų archyvams.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.11 **Duomenų slėpimas: duomenų slėpimas taikomas pagal teminę prieigos valdymo politiką ir pagal veiklos bei teisinius reikalavimus.**

Iš ko tai galima atpažinti: Nauja 2022 metų leidime. Praktiškai: jokių gamybinių duomenų testavimo ir kūrimo aplinkose, vietoj jų nuasmeninti arba sintetiniai duomenys; pseudonimų naudojimas analitikoje; sąskaitų numerių ir prisijungimo duomenų slėpimas žurnaluose ir palaikymo sąsajose. Įrodymas yra scenarijus arba procedūra, generuojanti testavimo duomenis.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.12 **Duomenų nutekėjimo prevencija: duomenų nutekėjimo prevencijos priemonės taikomos sistemoms, tinklams ir įrenginiams, kurie apdoroja, saugo arba perduoda jautrią informaciją.**

Iš ko tai galima atpažinti: Nauja 2022 metų leidime. Mažose organizacijose realu: bendrinimo nuorodų debesijos saugykloje valdymas, nepatvirtintų keičiamųjų laikmenų blokavimas, taisyklės, draudžiančios persiųsti į asmenines pašto dėžutes, konfidencialių duomenų įvedimo į išorės dirbtinio intelekto paslaugas patikros ir paslapčių paieška pirminiame kode. Įrodymas yra konfigūracija ir rastų atvejų peržiūros.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.13 **Informacijos atsarginės kopijos: duomenų, programinės įrangos ir sistemų atsarginės kopijos daromos pagal nustatytą taisyklę (apimtis, dažnumas, saugojimo trukmė, vieta), o atkūrimas iš jų reguliariais intervalais tikrai išbandomas.**

Iš ko tai galima atpažinti: Atsarginių kopijų politika su dažnumu, saugojimo trukme ir kopija kitoje vietoje pagal 3-2-1 principą, atsarginių kopijų šifravimas ir apsauga nuo perrašymo išpirkos reikalaujančia programine įranga (nekeičiamos atsarginės kopijos). Lemiama yra dokumentuota atkūrimo patikra su data ir rezultatu, nes neišbandyta atsarginė kopija audite prilygsta neegzistuojančiai.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.14 **Informacijos apdorojimo priemonių pertekliškumas: informacijos apdorojimo priemonės įrengtos su tokiu pertekliškumu, kokio reikia prieinamumo reikalavimams tenkinti.**

Iš ko tai galima atpažinti: Pertekliškumas derinamas prie prieinamumo tikslų, o ne prie didžiausio galimo lygio. Įrodymas yra architektūros aprašas su pertekliniais sistemos egzemplioriais arba zonomis, atsarginiais įrenginiais ir pagrįstu sprendimu, kur pertekliškumo sąmoningai nėra.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.15 **Įvykių registravimas: su saugumu susijusi veikla palieka pėdsaką. Žurnalai yra kuriami, saugomi, apsaugoti nuo pakeitimų ir tikrai analizuojami, o ne vien renkami.**

Iš ko tai galima atpažinti: Bent registruokite prisijungimus ir nesėkmingus bandymus, teisių pakeitimus, administravimo veiksmus ir prieigą prie konfidencialių duomenų. Žurnalai yra apsaugoti nuo pakeitimų ir turi nustatytą saugojimo trukmę; mažose organizacijose nekeičiami žurnalai kartu kompensuoja trūkstamą pareigų atskyrimą pagal A.5.3.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.16 **Stebėsenos veikla: tinklai, sistemos ir taikomosios programos yra stebimos dėl neįprasto elgesio, ir imamasi tinkamų veiksmų galimiems saugumo incidentams įvertinti.**

Iš ko tai galima atpažinti: Nauja 2022 metų leidime. Įgyvendinama ir be savo saugumo komandos: tapatybės teikėjo įspėjimai dėl neįmanomos kelionės ir dėl nesėkmingų bandymų serijų, debesijos platformos įspėjimai dėl neįprastų išlaidų arba teisių pakeitimų, persiunčiami į stebimą pašto dėžutę su nustatytu atsako laiku. Įrodymas yra įspėjimų taisyklės ir apdorotų įspėjimų pavyzdžiai.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.17 **Laikrodžių sinchronizavimas: visos žurnalus rašančios sistemos laiką ima iš nustatyto patikimo šaltinio, kad įvykius būtų galima išdėstyti teisinga eile per visas sistemas.**

Iš ko tai galima atpažinti: NTP konfigūracija serveriuose ir galiniuose įrenginiuose ir vienoda laiko juosta žurnaluose (geriausia UTC). Be sinchronizuoto laiko incidento atkūrimas pagal A.5.28 neatlaiko; kaip įrodymo pakanka konfigūracijos išrašo.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.18 **Privilegijuotų pagalbinių programų naudojimas: pagalbinių programų, galinčių apeiti sistemos apsaugas, naudojimas yra ribojamas ir griežtai kontroliuojamas.**

Iš ko tai galima atpažinti: Patvirtintų administravimo įrankių sąrašas, vietinių administratoriaus teisių ribojimas, taikomųjų programų valdymas (leidžiamųjų sąrašas), kur tai įmanoma, ir naudojimo registravimas. Įrodymas yra politika ir teisių valdymo konfigūracija.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.19 **Programinės įrangos diegimas veikiančiose sistemose: procedūros ir priemonės, skirtos saugiai valdyti programinės įrangos diegimą veikiančiose sistemose, yra įdiegtos.**

Iš ko tai galima atpažinti: Tik patvirtinta programinė įranga iš patikimų šaltinių, diegimas centriniu platinimu arba paketų tvarkykle, grįžimo į ankstesnę būseną kelias ir ankstesnės versijos išsaugojimas. Įrodymas yra patvirtinimų sąrašas ir diegimo žurnalai.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.20 **Tinklų saugumas: tinklai ir aktyvūs tinklo įrenginiai turi įvardytą savininką, sugriežtintą konfigūraciją ir atsekamą taisyklių rinkinį, nustatantį, koks srautas apskritai leidžiamas.**

Iš ko tai galima atpažinti: Užkardos taisyklių rinkinys pagal numatytojo draudimo principą, dokumentuoti atviri prievadai su pagrindimu, saugi belaidžio tinklo konfigūracija ir pakeisti numatytieji tinklo įrenginių prisijungimo duomenys. Įrodymas yra taisyklių rinkinio išrašas ir išorinis prievadų nuskaitymas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.21 **Tinklo paslaugų saugumas: tinklo paslaugų saugumo mechanizmai, paslaugų lygiai ir valdymo reikalavimai yra nustatyti, įdiegti ir stebimi.**

Iš ko tai galima atpažinti: Kiekvienai naudojamai tinklo paslaugai (VPN, DNS, paštas, CDN) dokumentuokite saugumo įsipareigojimus ir savo konfigūraciją, įskaitant šifravimą perdavimo metu ir teikėjo paslaugų lygio įsipareigojimus. Įrodymas yra konfigūracijos apžvalga ir sutartis arba paslaugos aprašas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.22 **Tinklų atskyrimas: tinklas yra padalytas į zonas taip, kad skirtingų apsaugos poreikių paslaugos, naudotojų grupės ir sistemos nepasiektų viena kitos be filtravimo.**

Iš ko tai galima atpažinti: Atskiri tinklo segmentai arba VLAN svečiams, administravimui ir gamybinei aplinkai; debesijoje atskiros paskyros arba virtualūs tinklai su saugumo grupėmis. Dirbant namuose įgyvendinamas sprendimas yra atskiras tinklas arba VLAN darbo įrenginiams, atskirtas nuo asmeninių įrenginių ir išmaniųjų namų technikos.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.23 **Žiniatinklio filtravimas: prieiga prie išorės svetainių yra valdoma, kad sumažėtų susidūrimas su kenkėjišku turiniu.**

Iš ko tai galima atpažinti: Nauja 2022 metų leidime. Pasiekiama nedidelėmis pastangomis per filtruojančią DNS paslaugą arba per galinių įrenginių apsaugoje esantį žiniatinklio filtravimą su blokuojamomis kategorijomis ir blokuotų užklausų registravimu. Įrodymas yra filtro konfigūracija ir ataskaitos išrašas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.24 **Kriptografijos naudojimas: yra nustatyta ir visiems galioja, kur taikomas šifravimas, kokiais algoritmais ir kaip raktai kuriami, saugomi, keičiami ir naikinami per visą jų būvio ciklą.** Dokumentas

Iš ko tai galima atpažinti: Kriptografijos politika su patvirtintais algoritmais ir mažiausiais raktų ilgiais, šifravimas perdavimo metu (TLS) ir saugojimo metu bei raktų valdymo procedūra, apimanti kūrimą, saugojimą, keitimą ir naikinimą. Įrodymas yra politika ir raktų paslaugos arba saugyklos konfigūracija.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.25 **Saugaus kūrimo būvio ciklas: taisyklės saugiam programinės įrangos ir sistemų kūrimui yra sukurtos ir taikomos.**

Iš ko tai galima atpažinti: Kūrimo proceso aprašas su saugumo sąlyčio taškais kiekviename etape: reikalavimai, projektavimas, įgyvendinimas, testavimas, laidos išleidimas, eksploatavimas. Mažoms komandoms pakanka vieno puslapio su nuoroda į konkrečius CI vartus ir peržiūros prievolę.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.26 **Taikomųjų programų saugumo reikalavimai: taikomųjų programų saugumo reikalavimai yra nustatyti, aprašyti ir patvirtinti kūrimo ir įsigijimo metu.**

Iš ko tai galima atpažinti: Saugumo reikalavimai kaip aiškūs punktai reikalavimų sąraše arba kaip pakartotinai naudojamas kontrolinis sąrašas, paremtas, pavyzdžiui, įprastais taikomųjų programų saugumo verifikavimo standartais. Įrodymas yra užduočių įrašai arba reikalavimų dokumentai su saugumo aspektu.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.27 **Saugios sistemų architektūros ir inžinerijos principai: saugios sistemų inžinerijos principai yra nustatyti, dokumentuoti ir taikomi kūrimo veikloje.**

Iš ko tai galima atpažinti: Dokumentuoti principai, tokie kaip mažiausia privilegija, daugiasluoksnė gynyba, saugios numatytosios nuostatos, duomenų kiekio mažinimas ir nulinio pasitikėjimo požiūris, kartu su matomu jų taikymu architektūros eskizuose arba sprendimų įrašuose.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

A.8.28 Saugus programavimas: saugaus programavimo principai taikomi kuriant programinę įrangą.

Iš ko tai galima atpažinti: Nauja 2022 metų leidime. Įrodymas yra įpareigojančios programavimo taisyklės, statinė kodo analizė ir paslapčių paieška kaip privalomi CI vartai, patikrintų bibliotekų naudojimas ir dokumentuotos kodo peržiūros. Kai pareigų atskyrimas neįmanomas, keturių akių peržiūrą pakeičia priverstiniai automatiniai vartai; tai pagrįskite ir įrodykite konvejerio konfigūracija.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.29 Saugumo testavimas kuriant ir priimant: saugumo testavimo procesai yra nustatyti ir įdiegti kūrimo būvio cikle.

Iš ko tai galima atpažinti: Automatiniai saugumo testai konvejeryje (priklausomybių patikros, statinė ir dinaminė analizė) ir periodinis įsilaužimo testas, kai apsaugos poreikiai yra padidinti. Įrodymas yra testų ataskaitos su datomis ir radinių sekimas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.30 Perduotas vykdyti kūrimas: perduota vykdyti kūrimo veikla yra valdoma, stebima ir peržiūrima.

Iš ko tai galima atpažinti: Kai kūrimas perduodamas vykdyti kitiems, saugumo reikalavimus įrašykite į sutartį, užsitikrinkite kodo nuosavybę ir peržiūros teisę ir prieš priimdami atlikite kodo peržiūras bei saugumo testus. Jeigu perduoto vykdyti kūrimo nėra, netaikymas SoA pagrindžiamas nuosekliai.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.31 Kūrimo, testavimo ir gamybinės aplinkos atskyrimas: kūrimo, testavimo ir gamybinė aplinkos yra atskirtos ir apsaugotos.

Iš ko tai galima atpažinti: Atskiros paskyros, projektai arba vardų sritys, atskiri prisijungimo duomenys ir atskiri duomenų rinkiniai. Kartu su A.8.11 pasirūpinkite, kad gamybiniai duomenys nepatektų į negamybines aplinkas. Įrodymas yra aplinkų apžvalga ir teisių priskyrimas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.32 Pakeitimų valdymas: informacijos apdorojimo priemonių ir informacinių sistemų pakeitimams taikomos pakeitimų valdymo procedūros.

Iš ko tai galima atpažinti: Pakeitimų procesas su paraiška, poveikio vertinimu, testavimu, pritarimu, įgyvendinimu ir grįžimo į ankstesnę būseną keliu. Kūrimo komandose šį punktą tenkina sujungimo prašymų konvejeris su privalomais patikrinimais ir registruojamais diegimais, jeigu istorija yra nekeičiama.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.33 Testavimo informacija: testavimo informacija yra tinkamai parinkta, apsaugota ir valdoma.

Iš ko tai galima atpažinti: Principas yra toks: jokių tikrų asmens duomenų testavimo sistemose. Kai to išvengti neįmanoma, dokumentuokite pritarimą, slėpimą, prieigos ribojimą ir naikinimą po testo. Įrodymas yra testavimo duomenų tvarka ir naikinimo žurnalai.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8.34 Informacinių sistemų apsauga audito bandymų metu: audito bandymai, susiję su prieiga prie veikiančių sistemų, yra suplanuoti ir suderinti su vadovybe, kad veikla nebūtų sutrikdyta.

Iš ko tai galima atpažinti: Audito susitarimas su laiko langu, apimtimi, tik skaitymo prieiga, kur tai įmanoma, audito prieigos registravimu ir vadovybės pritarimu. Tai galioja ir įsilaužimo testams: įrodymas yra rašytinis leidimas testuoti su laiko langu ir skubaus kontakto duomenimis.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

ISO/IEC 27018:2025, informacijos saugumas, kibernetinis saugumas ir privatumo apsauga: asmens duomenų (PII) apsaugos viešuosiuose debesyse, veikiančiuose kaip PII tvarkytojai, gairės (3 leidimas, 2025-08)

PII apsauga viešajame debesyje

36 reikalavimai. Šiam standartui nėra akredituoto sertifikato. Redakcija 07/2026.

ISO/IEC 27018 nėra vadybos sistemos standartas, o gairės su išplėstomis valdymo priemonėmis, papildančiomis ISO/IEC 27002:2022. Atskiro akredituoto sertifikato pagal ISO/IEC 27018 nėra. Valdymo priemonės įtraukiamos į ISO/IEC 27001 sistemos pritaikomumo pareiškimą, o sertifikatas tuomet išduodamas pagal ISO/IEC 27001 su nuoroda į ISO/IEC 27018. Standartas skirtas viešosios debesijos paslaugos teikėjui, kuris tvarko asmens duomenis savo debesijos paslaugos klientų pavedimu. Organizacija, kuri debesijos paslaugas tik naudoja, šio vaidmens neprisiima, todėl reikalavimus prasminga vertinti savo teikėjų, o ne savo pačios atžvilgiu. Leanshift atveju šis kontrolinis sąrašas pirmiausia yra tiekėjų vertinimo tinklelis. Kiekvieną punktą galima pateikti teikėjui kaip klausimą ir įtvirtinti duomenų tvarkymo sutartyje pagal GDPR 28 straipsnį. Tokio vertinimo rezultatas yra vidinis atitikties įrašas arba teikėjo vertinimo profilis, o ne sertifikatas. Dėl numeracijos: skyriai nuo A.2 iki A.12 atitinka standarto A priede pateiktus privatumo principus, o punktai su tokiais numeriais kaip A.11.6 yra ten išvardytos papildomos valdymo priemonės. Punktai su numeriais kaip 8.10 arba 5.34 nurodo ISO/IEC 27002:2022 valdymo priemones, kurias standartas sukonkretina debesijai. Punktai su prierašu (Grundsatz), reiškiančiu principą, kyla iš paties skyriaus principo tais atvejais, kai A priede atskiros papildomos valdymo priemonės nėra.

Įmonė	Data	Pildė

A.2 Sutikimas ir pasirinkimas 2

A.2.1 **Debesijos paslaugos teikėjas padeda debesijos paslaugos klientui įgyvendinti duomenų subjektų teises, tokias kaip susipažinimas, ištaisymas, ištrynimas ir prieštaravimas. Atsakomybės ir terminai yra nustatyti sutartyje.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra duomenų tvarkymo sutartis pagal GDPR 28 straipsnį su nuostata dėl pagalbos įgyvendinant duomenų subjektų teises, kartu su techninėmis priemonėmis pačioje paslaugoje: eksporto, taisymo ir trynimo funkcijomis arba dokumentuota palaikymo procedūra su atsako terminu. Klausimas tiekėjui: kokią funkciją ar procesą siūlote, kad prašymą susipažinti ar ištrinti galėtume įvykdyti per vieną mėnesį?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.2 (Grundsatz) **Debesijos paslaugos klientų asmens duomenys tvarkomi tik pagal dokumentuotus kliento nurodymus. Duomenų subjektų sutikimo gavimas lieka kliento kaip duomenų valdytojo užduotis, ir teikėjas šiuo klausimu savo iniciatyva neveikia.**

Iš ko tai galima atpažinti: Įrodymas yra nurodymų nuostata duomenų tvarkymo sutartyje ir įrodymas, kad teikėjas duomenų nenaudoja antriniais savo tikslais, pavyzdžiui paslaugos privatumo pranešimas ir produkto dokumentacija. Klausimas tiekėjui: ar mūsų klientų duomenis kokiu nors būdu tvarkote ne pagal mūsų nurodymus, pavyzdžiui produkto tobulinimui ar modelių mokymui?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.3 Tikslo teisėtumas ir apibrėžimas 2

A.3.1 **Tikslas, kuriuo teikėjas tvarko asmens duomenis, apsiriboja sutartos paslaugos teikimu ir yra įvardytas sutartyje. Tvarkymo savo paties tikslais teikėjas nevykdo.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra duomenų tvarkymo sutartis, kurioje nurodytas tvarkymo dalykas, pobūdis, tikslas ir trukmė bei duomenų subjektų kategorijos pagal GDPR 28 straipsnio 3 dalį. Klausimas tiekėjui: prašome pateikti sutarties priedą, kuris išsamiai aprašo tvarkymo tikslą. Mažoje įmonėje pakanka teikėjo standartinio duomenų tvarkymo priedo, jeigu jame yra ši informacija.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.3.2 **Teikėjui patikėti asmens duomenys be išankstinio aiškaus sutikimo nenaudojami reklamai, rinkodarai ar kitiems komerciniams teikėjo tikslams. Paslaugos teikimas nuo tokio sutikimo nepriklauso.**

Iš ko tai galima atpažinti: Įrodymas yra aiški sutarties nuostata, kuri atmeta komercinį antrinį naudojimą, kartu su paslaugos teikimo sąlygomis. Klausimas tiekėjui: raštu patvirtinkite, kad klientų duomenys nenaudojami reklamai, profiliavimui ar dirbtinio intelekto modelių mokymui. Jei tokio įsipareigojimo nėra, paslauga asmens duomenims netinka.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.4 Rinkimo ribojimas 1

A.4 (Grundsatz) **Be duomenų, kuriuos į paslaugą įkelia klientas, teikėjas savo tikslais nerenka jokių kitų asmens duomenų, tokių kaip telemetrija, naudojimo profiliai ar turinio analizė. Renkami veiklos duomenys ir metaduomenys yra įvardyti ir pagrįsti.**

Iš ko tai galima atpažinti: Įrodymas yra sąrašas duomenų, kuriuos paslauga fiksuoja šalia turinio duomenų (prieigos žurnalai, telemetrija, diagnostikos duomenys), su tikslu ir saugojimo terminu, ir nustatymo, kuriuo išjungiama pasirenkama telemetrija, ekrano nuotrauka. Klausimas tiekėjui: kokius papildomus naudojimo, telemetrijos ir diagnostikos duomenis renkate, kam juos naudojate ir ar galime rinkimą išjungti?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.5 Duomenų kiekio mažinimas 2

A.5.1 **Laikinieji failai, sukuriami tvarkant asmens duomenis, tokie kaip laikinoji saugykla, podėliai ar atstatymo žurnalai, saugiai ištrinami per nustatytą laikotarpį.**

Iš ko tai galima atpažinti: Įrodymas yra eksploatavimo arba trynimo procedūra su nurodytu laikinųjų duomenų saugojimo terminu, paremta sistemos konfigūracija, pavyzdžiui podėlio TTL arba suplanuota valymo užduotis su jos vykdymo žurnalu. Klausimas tiekėjui: po kokio laikotarpio ištrinami podėliai, laikinieji failai ir tarpinės būsenos ir kaip tai stebima?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

8.11 **Visur, kur eksploatavimui, testavimui ar palaikymui gyvi duomenys nereikalingi, asmens duomenys yra maskuojami, pseudonimizuojami arba anonimizuojami. Tvarkomų duomenų apimtis lieka apribota tuo, ko paslaugai iš tikrųjų reikia.**

Iš ko tai galima atpažinti: Įrodymas yra taisyklė, nustatanti, kurios aplinkos gali matyti gyvus duomenis, bei testavimo ir kūrimo sistemose naudojamo maskavimo ekrano nuotraukos arba scenarijai. Klausimas tiekėjui: ar palaikymo ir kūrimo komandos dirba su gamybos duomenimis ir jeigu taip, su kokiomis apsaugos priemonėmis? Mažoje įmonėje pakanka taisyklės, kad testavimo sistemos veikia tik su sugeneruotais pavyzdiniais duomenimis.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.6 Naudojimo, saugojimo ir atskleidimo ribojimas 3

A.6.1 **Gavęs teisiškai saistantį reikalavimą atskleisti asmens duomenis, pavyzdžiui iš valdžios institucijos, teikėjas iš anksto informuoja debesijos paslaugos klientą tiek, kiek leidžia teisės aktai.**

Iš ko tai galima atpažinti: Įrodymas yra sutartinė informavimo nuostata ir vidinis institucijų užklausų procesas su įvardytu atsakingu asmeniu. Klausimas tiekėjui: ar informuojate mus prieš perduodami duomenis ir ar skelbiate skaidrumo ataskaitą apie institucijų užklausas? Naujausia skaidrumo ataskaita yra stiprus įrodymas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.6.2 **Atskleisdamas asmens duomenis tretiesiems asmenims, teikėjas šį įvykį registruoja taip, kad jį būtų galima atsekti: kas duomenis gavo, kada tai įvyko, kokie duomenys buvo perduoti ir kokiu pagrindu atskleidimas remiasi.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra atskleidimų registras arba užklausų istorija su šiais laukais, net jeigu įrašų jame nėra. Tuščias, bet palaikomas registras yra priimtinas ir mažoje įmonėje yra praktiškiausias kelias. Klausimas tiekėjui: ar tvarkote duomenų atskleidimų registrą ir ar galime gauti iš jo išrašus?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

8.10 **Asmens duomenys ištrinami pasibaigus sutartam saugojimo terminui arba nutrūkus sutarčiai, įskaitant atsarginėse kopijose laikomus egzempliorius po jų rotacijos ciklo.**

Iš ko tai galima atpažinti: Įrodymas yra trynimo koncepcija su saugojimo terminais pagal duomenų kategorijas, atsarginių kopijų saugojimo terminas ir trynimo žurnalas arba trynimo patvirtinimas. Klausimas tiekėjui: kiek ilgai mūsų duomenys po sutarties nutraukimo lieka atsarginėse kopijose ir ar gauname raštišką jų ištrynimo patvirtinimą?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.7 Tikslumas ir kokybė 2

A.7 (Grundstein) **Teikėjas savo iniciatyva nekeičia jam patikėtų asmens duomenų. Pataisymai ir atnaujinimai atliekami tik pagal debesijos paslaugos kliento nurodymą arba per funkcijas, kurias klientas valdo pats.**

Iš ko tai galima atpažinti: Įrodymas yra paslaugos redagavimo funkcijos kartu su jų pakeitimų istorija ir nurodymų nuostata duomenų tvarkymo sutartyje. Klausimas tiekėjui: ar galime įrašus taisyti patys ir ar kiekvienas pakeitimas registruojamas taip, kad jį būtų galima atsekti?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

8.13 **Asmens duomenų vientisumas yra apsaugotas saugojimo, perdavimo ir atkūrimo metu. Atsarginės kopijos yra sukurtos, o jų atkuriamumas yra patikrintas.**

Iš ko tai galima atpažinti: Įrodymas yra atsarginių kopijų konfigūracija, kontrolinių sumų arba vientisumo mechanizmai ir bent viena dokumentuota atkūrimo patikra per metus su data ir rezultatu. Klausimas tiekėjui: kaip dažnai testuojate atkūrimą ir kokį atkūrimo laiką įsipareigojate užtikrinti paslaugos lygio susitarime?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8 Atvirumas, skaidrumas ir informavimas 2

A.8.1 **Pasitelktų duomenų tvarkytojų, kurie tvarko asmens duomenis, naudojimas atskleidžiamas prieš sudarant sutartį. Apie sąrašo pakeitimus klientas informuojamas laiku, kad galėtų prieštarauti arba nutraukti sutartį.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra naujausias pasitelktų duomenų tvarkytojų sąrašas, paskelbtas arba pateiktas pagal sutartį, su pavadinimu, šalimi ir tvarkymo tikslu, ir informavimo taisyklė pagal GDPR 28 straipsnio 2 dalį. Klausimas tiekėjui: kur rasti pasitelktų duomenų tvarkytojų sąrašą, prieš kiek laiko pranešate apie pakeitimus ir kaip galime prieštarauti?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.8 (Grundstein) **Prieš sudarant sutartį teikėjas pateikia suprantamą informaciją apie tai, kaip tvarkomi asmens duomenys, kokios apsaugos priemonės yra sukurtos ir kokiose jurisdikcijose vyksta tvarkymas.**

Iš ko tai galima atpažinti: Įrodymas yra privatumo pranešimas, saugumo aprašas, pasitikėjimo centro puslapis ir duomenų tvarkymo sutartis su techninėmis ir organizacinėmis priemonėmis kaip priedu. Klausimas tiekėjui: prašome pateikti naujausią techninių ir organizacinių priemonių sąrašą kaip sutarties priedą, o ne tik rinkodarinę medžiagą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.9 Asmens dalyvavimas ir prieiga 2

A.9 (Grundsatz) **Paslauga suteikia debesijos paslaugos klientui technines priemones savarankiškai įvykdyti duomenų subjektų prašymus susipažinti, ištaisyti ir ištrinti, pavyzdžiui per eksporto, paieškos ir trynimo funkcijas.**

Iš ko tai galima atpažinti: Įrodymas yra eksporto ir trynimo funkcijų produkto dokumentacija, paremta vidiniu bandymu: vienas prašymas susipažinti apdorojamas nuo pradžios iki galo ir užrašoma, kiek tai trunka. Klausimas tiekėjui: ar galime rasti, eksportuoti ir ištrinti visus vieno asmens duomenis be teikėjo pagalbos?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

5.34 **Kai klientas duomenų subjekto prašymo negali įvykdyti pats, teikėjas padeda per sutartą laikotarpį. Prašymai, kuriuos duomenų subjektai siunčia tiesiogiai teikėjui, perduodami klientui, o teikėjas į juos pats neatsako.**

Iš ko tai galima atpažinti: Įrodymas yra atitinkama duomenų tvarkymo sutarties nuostata su konkrečiu atsako terminu ir palaikymo užklausų istorija kaip tikras pavyzdys. Klausimas tiekėjui: kokį pagalbos įgyvendinant duomenų subjektų teises terminą įsipareigojate ir kiek tai kainuoja?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.10 Atskaitomybė 4

A.10.1 **Apie asmens duomenų saugumo pažeidimus debesijos paslaugos klientui pranešama nepagrįstai nedelsiant, nurodant mastą, paveiktus duomenis, priežastį ir taikytas priemones. Informavimo procesas su atsakomybėmis ir terminais yra nustatytas.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra reagavimo į incidentus planas su eskalavimo grandine, sutartinis informavimo terminas (praktikoje tinka nuo 24 iki 48 valandų, kad klientas dar spėtų laikytis 72 valandų termino pagal GDPR 33 straipsnį) ir įrašai apie buvusius incidentus arba apie pratybas. Klausimas tiekėjui: per kokį laikotarpį pranešate apie incidentą, kokiu kanalu ir kokią informaciją kartu pateikiate?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.10.2 **Saugumo politikos, eksploatavimo procedūros ir su jomis susiję įrašai saugomi nustatytą laikotarpį, kad tvarkymą būtų galima atkurti vėliau.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra saugojimo taisyklė su politikų versijų istorija, pavyzdžiui dokumentų registras arba versijų valdymo sistema su patvirtinimo data. Klausimas tiekėjui: kiek ilgai saugote politikų versijas ir su jomis susijusius įrašus ir ar audito atveju gauname prie jų prieigą?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.10.3 **Asmens duomenų grąžinimui, perdavimui ir sunaikinimui pasibaigus sutarčiai yra nustatyta tvarka, kurioje įvardyti formatai, terminai ir elgesys su kopijomis.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra duomenų tvarkymo sutarties pasitraukimo nuostata ir trynimo patvirtinimas pasibaigus sutarčiai. Klausimas tiekėjui: kokiu formatu ir per kokį laikotarpį atgauname savo duomenis, kada sunaikinamos visos kopijos ir ar gauname raštišką patvirtinimą?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

5.35 **Apsaugos priemonių rezultatyvumas nepriklausomai peržiūrimas reguliariais intervalais, pavyzdžiui per vidaus auditus, įsilaužimo testus ar trečiųjų šalių užtikrinimo ataskaitas. Rezultatai tinkama forma pateikiami debesijos paslaugos klientui.**

Iš ko tai galima atpažinti: Įrodymas yra ISO/IEC 27001 sertifikatas su pritaikomumo pareiškimu, kuriame yra ISO/IEC 27018 valdymo priemonės, arba SOC 2 ataskaita kartu su naujausiomis įsilaužimo testų santraukomis. Klausimas tiekėjui: prašome pateikti sertifikatą, jo taikymo sritį ir patvirtinimą, kad ISO/IEC 27018 atsispindi pritaikomumo pareiškime. Verta patikrinti, ar taikymo sritis iš tikrųjų apima naudojamą paslaugą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11 Informacijos saugumas 13

A.11.1 **Kiekvienas asmuo, turintis prieigą prie asmens duomenų, yra įpareigotas laikytis konfidencialumo, nesvarbu, ar dirba pagal darbo sutartį, ar yra pasitelktas iš išorės.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra pasirašytos konfidencialumo sutartys arba pasižadėjimai, galiojantys ir pasibaigus bendradarbiavimui. Klausimas tiekėjui: ar visi darbuotojai ir paslaugų teikėjai, turintys prieigą prie duomenų, raštu įpareigoti laikytis konfidencialumo?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.2 **Spaudiniai ir kitos popierinės kopijos su asmens duomenimis kuriami tik tada, kai tai būtinai reikalinga. Leistina apimtis yra reglamentuota taisyklėje.**

Iš ko tai galima atpažinti: Įrodymas yra elgesio su spaudiniais taisyklė, kuri duomenų centruose paprastai yra visiškas spausdinimo draudimas zonose su klientų duomenimis. Klausimas tiekėjui: ar klientų duomenys apskritai spausdinami veikloje ir jeigu taip, kokiomis sąlygomis?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.3 **Atkūrimai iš atsarginių kopijų yra iš anksto autorizuoti ir registruojami, nurodant asmenį, kuris atkūrimą inicijavo, ir paveiktus duomenis.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra atkūrimo žurnalas su laiko žyma, iniciatoriumi ir apimtimi, kurį atsarginių kopijų įrankis paprastai sukuria automatiškai. Klausimas tiekėjui: ar registruojate kiekvieną atkūrimą ir ar audito atveju galime šiuos žurnalus peržiūrėti?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.4 **Laikmenos su asmens duomenimis, kurios išgabenamos iš patalpų, yra apsaugotos nuo neteisėtos prieigos ir praradimo, paprastai šifravimu ir gabenimo įrašu.**

Iš ko tai galima atpažinti: Įrodymas yra šifravimo įrodymas (visos laikmenos šifravimas), gabenimo ir perdavimo įrašai bei laikmenų inventorius. Klausimas tiekėjui: ar laikmenos su klientų duomenimis kada nors išgabenamos iš teikėjo objektų, pavyzdžiui dėl atsarginių kopijų, ir kaip jos apsaugotos gabenimo metu?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.5 **Nešifruotų nešiojamųjų laikmenų ir įrenginių naudojimas asmens duomenims yra draudžiamas arba apribotas pagrįstomis išimtimis su dokumentuotu patvirtinimu.**

Iš ko tai galima atpažinti: Įrodymas yra keičiamųjų laikmenų politika ir techninis jos įgyvendinimas, pavyzdžiui priverstinis įrenginių šifravimas arba per įrenginių valdymą užblokuoti USB prievadai. Klausimas tiekėjui: ar darbuotojai gali kopijuoti klientų duomenis į nešifruotus įrenginius ir kas tam techniškai užkerta kelią?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.6 **Viešaisiais tinklais perduodami asmens duomenys yra šifruojami. Naudojami mechanizmai atitinka dabartinį technikos lygį.**

Iš ko tai galima atpažinti: Įrodymas yra TLS konfigūracija (naujausia protokolo versija, jokių pasenusių šifrų) ir išorinis konfigūracijos patikrinimas kaip ataskaita. Mažoje įmonėje praktiška kartą per metus atlikti nemokamą TLS patikrą ir rezultatą įsegti į bylą. Klausimas tiekėjui: kokį perdavimo šifravimą taikote ir ar įjungtas saugomų duomenų šifravimas?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.7 **Popieriniai įrašai su asmens duomenimis sunaikinami taip, kad jų atkurti nebūtų įmanoma.**

Iš ko tai galima atpažinti: Įrodymas yra tinkamo saugumo lygio smulkintuvai arba sunaikinimo pažymos iš paslaugų teikėjo, dirbančio pagal DIN 66399 ar lygiavertį standartą. Klausimas tiekėjui: kaip sunaikinate su klientais susijusius popierinius įrašus ir ar sunaikinimo pažymos saugomos byloje?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.8 **Naudotojų identifikatoriai vienareikšmiškai priskiriami vienam asmeniui ir nėra nei pakartotinai išduodami, nei bendrai naudojami. Bendros paskyros egzistuoja tik pagrįstomis išimtimis ir su papildomu atsekamumu.**

Iš ko tai galima atpažinti: Įrodymas yra naudotojų sąrašas iš tapatybės valdymo sistemos be grupinių paskyrų kartu su taisykle, kad administravimo darbai atliekami iš asmeninės paskyros. Klausimas tiekėjui: ar eksploatavimo darbuotojai dirba su asmeninėmis paskyromis ir ar daugiaveiksnis autentiškumo patvirtinimas yra būtinas?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.9 **Teikėjas bet kuriuo metu gali nurodyti, kurie asmenys ar vaidmenys turi teisę pasiekti asmens duomenis, ir šią apžvalgą nuolat atnaujina.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra prieigos teisių apžvalga pagal vaidmenis, paremta pasikartojančia prieigos peržiūra su data ir rezultatu. Mažoje įmonėje pakanka kas pusmetį eksportuoto ir pasirašyto naudotojų sąrašo. Klausimas tiekėjui: kiek darbuotojų gali pasiekti mūsų duomenis ir kaip dažnai tai peržiūrite?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.10 **Naudotojų paskyros valdomos per visą jų būvio ciklą: sukūrimas, keitimas ir nedelsiamas išjungimas, kai asmuo išeina ar keičia vaidmenį.**

Iš ko tai galima atpažinti: Įrodymas yra darbuotojų priėmimo ir atleidimo procedūra su kontroliniu sąrašu ir išjungtų paskyrų žurnalai su laiko žymomis. Klausimas tiekėjui: per kokį laikotarpį atimate prieigą iš išeinančių darbuotojų ir kaip tai įrodote?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.11 **Teikėjo saugumo ir privatumo įsipareigojimai yra įtvirtinti sutartyje, įskaitant technines ir organizacines priemones, kliento nurodymų saistantį pobūdį ir kliento teisę atlikti auditą.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra pasirašyta duomenų tvarkymo sutartis pagal GDPR 28 straipsnį su priemonių priedu ir audito arba informavimo teise. Klausimas tiekėjui: prašome pateikti pasirašytą duomenų tvarkymo sutartį su visais priedais, o ne vien nuorodą į bendrąsias paslaugų teikimo sąlygas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.12 **Pasitelktiems duomenų tvarkytojams, kurie tvarko asmens duomenis, taikomi bent tokie patys įsipareigojimai kaip ir pačiam teikėjui. Jų atranka ir nuolatinė stebėsena vyksta pagal nustatytą procesą.**

Iš ko tai galima atpažinti: Įrodymas yra įsipareigojimų perkėlimas į sutartis su pasitelktais duomenų tvarkytojais (GDPR 28 straipsnio 4 dalis) ir tiekėjų vertinimas su data. Klausimas tiekėjui: kaip vertinate pasitelktus duomenų tvarkytojus ir kokių įrodymų iš jų reikalaujate?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.11.13 **Prieš pakartotinai naudojant saugyklos vietą, užtikrinama, kad ankstesnių naudotojų duomenys neliktų pasiekiami nei fizinėse laikmenose, nei virtualizuotose aplinkose.**

Iš ko tai galima atpažinti: Įrodymas yra valymo arba perrašymo procedūra, taikoma atlaisvinant saugyklą, laikmenų sunaikinimo įrašai ir architektūros dokumente aprašytas nuomininkų atskyrimas. Klausimas tiekėjui: kaip užtikrinate, kad pakartotinai naudojamoje saugykloje nelieka kitų klientų liekamųjų duomenų?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.12 Privatumo atitiktis 3

A.12.1 **Šalys, kuriose asmens duomenys saugomi ir tvarkomi, yra įvardytos ir žinomos debesijos paslaugos klientui. Apie saugojimo vietų pakeitimus pranešama.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra teikėjo objektų ir regionų apžvalga sutartyje arba dokumentacijoje ir naudojamos paslaugos regiono nustatymo ekrano nuotrauka. Klausimas tiekėjui: kokiose šalyse mūsų duomenys saugomi, iš kokių šalių prie jų prieinama, pavyzdžiui teikiant palaikymą, ir ar galime regioną užfiksuoti?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

A.12.2 **Asmens duomenų perdavimai į trečiąsias valstybes yra žinomi, pagrįsti ir užtikrinti tinkamomis apsaugos priemonėmis.** Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra standartinės sutarčių sąlygos arba sprendimas dėl tinkamumo, paremtas perdavimo poveikio vertinimu, kuris mažoje įmonėje gali būti trumpas: paveiktos duomenų kategorijos, paskirties šalis, rizika, taikytos papildomos priemonės. Klausimas tiekėjui: kokiu teisiniu pagrindu perduodate duomenis į trečiąsias valstybes ir kokias papildomas priemones taikote?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

5.31 **Teisiniai ir sutartiniai reikalavimai, taikomi asmens duomenų tvarkymui, yra nustatyti ir atnaujinami keičiantis teisinei padėčiai. Prieštaraujančios jurisdikcijos yra įvertintos.**

Iš ko tai galima atpažinti: Įrodymas yra taikomų reikalavimų apžvalga (GDPR, nacionalinės taisyklės, sektoriui būdingos pareigos) su atsakingu asmeniu ir peržiūros data. Mažoje įmonėje pakanka vieno puslapio sąrašo, peržiūrimo kartą per metus. Klausimas tiekėjui: ar teikėjui arba pasitelktiems duomenų tvarkytojams taikomos jurisdikcijos, kurios leidžia institucijoms pasiekti mūsų duomenis, ir kaip tai sprendžiama?

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas