

ISO/IEC 27001:2022 + Amd 1:2024 Informācijas drošības pārvaldības sistēmas (ISMS)

Informācijas drošība, ISMS, sertificējama visā pasaulē

181 prasības. Pēc šī standarta ir iespējams sertificēties akreditētā sertifikācijas institūcijā. Redakcija 07/2026.

ISO/IEC 27001 nosaka prasības informācijas drošības pārvaldības sistēmai: uz risku balstītai, dokumentētai un pierādāmi rezultatīvai. Novērtēšana pret to ir akreditēts sertifikācijas audits divos posmos (dokumentu pārbaude, pēc tam rezultatīvātes pārbaude uz vietas), kam seko ikgadēji uzraudzības audiiti un atkārtota sertifikācija pēc trim gadiem.

Uzņēmums	Datums	Aizpildīja
----------	--------	------------

4 Organizācijas konteksts

8

4.1-1

Ārējie un iekšējie jautājumi, kas ietekmē organizācijas spēju sasniegt ISMS paredzētos rezultātus, ir noteikti un tiek uzturēti aktuāli.

Pēc kā to var atpazīt: Apliecināms ar konteksta analīzi kā atsevišķu dokumentu vai kā ISMS rokasgrāmatas sadaļu: tirgus vide, klientu un līgumu situācija, tiesiskais ietvars (GDPR, NIS2), tehnoloģiju kopums, darbinieku skaits, atkarība no mākoņpakalpojumu sniedzējiem. Maziem uzņēmumiem pietiek ar vienas lappuses tabulu, kurā ir datums un pārskatīšanas cikls, ja vadības pārskatīšana parāda, ka tā tiešām tiek aktualizēta.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

4.1-2

Organizācija ir noteikusi, vai klimata pārmaiņas tai ir būtisks jautājums. Konstatējums ir pamatots neatkarīgi no tā, vai atbilde ir apstiprinoša vai noliedzoša.

Pēc kā to var atpazīt: Šī prasība ir ieviesta ar Amd 1:2024, un auditori to jautā mērķtiecīgi. Konteksta analizē par to ir atsevišķa rinda: karstuma periodi ar ietekmi uz serveru telpām un pieejamību, ekstrēmi laikapstākļi ar ietekmi uz mākoņpakalpojumu sniedzēju datu centriem, elektrotīkla stabilitāte. Pamatots rezultāts, ka jautājums nav būtisks, ir pieļaujams, trūkstošs ieraksts nav.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

4.2-1

ISMS būtiskās ieinteresētās puses ir noteiktas.

Pēc kā to var atpazīt: Ieinteresēto pušu saraksts, kurā ir klienti, darbinieki, apstrādātāji un apakšapstrādātāji, uzraudzības iestādes, apdrošinātāji, sertifikācijas institūcija un īpašnieki. Mazos uzņēmumos pietiek ar tabulu, kurā ir norādīta puse, tās gaidas un šo gaidu avots.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

4.2-2

Šo ieinteresēto pušu būtiskās prasības ir noteiktas, tostarp prasības, kas saistītas ar klimata pārmaiņām.

Pēc kā to var atpazīt: Katrai pusei ir nosaukts konkrēts avots: līguma punkts, datu apstrādes līgums, klienta aptaujas anketa, tiesību aktā noteikts pienākums. Amd 1:2024 papildus norāda, ka ieinteresētajām pusēm var būt ar klimata pārmaiņām saistītas prasības. Tā nav atsevišķa obligāta prasība, taču auditori to regulāri skar, piemēram, ilgtspējas jautājumi liela klienta piegādātāju auditā. Pietiek ar vienu rindu ieinteresēto pušu tabulā, kurā ir norādīts rezultāts, tostarp tāds, ka šādu prasību nav.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

4.2-3

Ir izlemts un izsekojams, kuras no šīm prasībām tiek risinātas ar ISMS.

Pēc kā to var atpazīt: Ieinteresēto pušu tabulā pievieno sleju, kas norāda uz noteikumu, kurš prasību risina (politika, kontroles pasākums, līguma pielikums). Tas parāda, ka prasības ir ne tikai savāktas, bet arī tiešām apstrādātas.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

4.3-1 ISMS tvērums ir noteikts un ņem vērā 4.1 jautājumus, 4.2 prasības, kā arī saskarnes un atkarības no darbībām, ko veic trešās puses.

Pēc kā to var atpazīt: Tvērumā ir nosauktas atrašanās vietas, organizatoriskās vienības, produkti, sistēmas un tīkla robežas. Ārpakalpojumā nodotās daļas (mitināšana, maksājumu pakalpojumu sniedzēji, atbalsts) ir aprakstītas kā saskarnes ar skaidru atbildības robežu. Mākslīgi sašaurinātu tvērumu, kas izslēdz pamatprocesus, sertifikācijas institūcijas noraida.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

4.3-2 Tvērums ir pieejams kā dokumentēta informācija un nepārprotami norāda ISMS robežas.[Dokuments](#)

Pēc kā to var atpazīt: Apstiprināts tvēruma dokuments ar versiju, datumu un augstākās vadības parakstu. Tā formulējums vēlāk parādās sertifikātā, tāpēc to formulē precīzi un tā, lai to varētu citēt publiski.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

4.4-1 ISMS, tostarp nepieciešamie procesi un to mijiedarbība, ir izveidota, ieviesta, tiek uzturēta un nepārtraukti uzlabota.

Pēc kā to var atpazīt: Procesu karte vai procesu saraksts, kas sasaista risku pārvaldību, notikumu apstrādi, izmaiņu pārvaldību, auditēšanu un vadības pārskatīšanu ar īpašniekiem un biežumu. Dzīvi pierādījumi ir svarīgāki par shēmu: pieteikumi, protokoli, kalendāra ieraksti.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5 Līderība**8****5.1-1 Augstākā vadība uzņemas atbildību par ISMS rezultativitāti un nodrošina, ka politika un mērķi ir izveidoti un savietojami ar stratēģisko virzienu.**

Pēc kā to var atpazīt: Pierādījums ir parakstīti politikas, tvēruma un piemērojamības paziņojuma apstiprinājumi, vadības pārskatīšanas protokoli un dokumentēti budžeta lēmumi. Ļoti mazos uzņēmumos augstākā vadība bieži ir tā pati persona, kas ISMS īpašnieks; tas ir pieļaujams, taču lomu aprakstā to norāda atklāti.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.1-2 ISMS prasības ir integrētas darbības procesos, un tiek paziņots, cik svarīga ir rezultatīva informācijas drošība.

Pēc kā to var atpazīt: Vislabāk to parāda vietas, kur drošība nav atsevišķa mape: drošības kritērijs pabeigtības definīcijā, drošības pārbaude pārdošanas vai iepirkuma procesā, regulārs drošības punkts komandas sanāksmju protokolos.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.1-3 Vadība nodrošina nepieciešamos resursus, atbalsta cilvēkus, kas sniedz ieguldījumu ISMS rezultativitātē, un veicina nepārtrauktu uzlabošanu.

Pēc kā to var atpazīt: Apstiprināts drošības budžets, apmācībām atvēlēts laiks, ārēju auditoru vai ielaušanās testētāju piesaiste. Uzlabojumu vai darbību reģistrs ar ierakstiem vairāku ceturkšņu garumā parāda nepārtrauktību, nevis vienreizēju piepūli.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.2-1 Ir izveidota informācijas drošības politika, kas atbilst organizācijas mērķim un veido ietvaru informācijas drošības mērķiem.[Dokuments](#)

Pēc kā to var atpazīt: Īss apstiprināts politikas dokuments, pietiek ar divām vai trim lappusēm. Tajā ir nosaukti aizsardzības mērķi, tvērums, atbildības un uz risku balstītas pieejas princips. Vispārīgs veidnes teksts bez saiknes ar reālo darbību auditā uzreiz izceļas.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.2-2 Politikā ir iekļauta apņemšanās izpildīt piemērojamās prasības un apņemšanās nepārtraukti uzlabot ISMS. Dokuments

Pēc kā to var atpazīt: Abām apņemšanām politikā ir jāparādās kā skaidriem teikumiem, un 1. posma auditā tos lasa vārds vārdā. Papildus atsaucas uz pamatā esošajiem procesiem (tiesību aktu reģistrs, uzlabojumu reģistrs).

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.2-3 Politika ir paziņota organizācijā un attiecīgā apjomā pieejama ieinteresētajām pusēm. Dokuments

Pēc kā to var atpazīt: Pierādījums ir iekšējais vai wiki ieraksts ar pienākumu to izlasīt, ievadapmācības kontrolesaraksts ar apstiprinājumu vai publicēts kopsavilkums tīmekļa vietnē. Izplatīšanas saraksts ar apstiprinājuma atzīmēm ir vienkāršākais stabils pierādījums.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.3-1 Atbildības un pilnvaras drošībai būtiskajām lomām ir piešķirtas un paziņotas organizācijā.

Pēc kā to var atpazīt: Lomu matrica (RACI), kurā ir ISMS īpašnieks, risku īpašnieki, aktīvu īpašnieki, notikumu koordinators un datu aizsardzības kontaktpersona. Viena cilvēka vai ļoti mazās komandās katru lomu piešķir konkrētai personai un radušos lomu uzkrāšanos dokumentē atklāti, nevis slēpj.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.3-2 Pilnvaras nodrošināt ISMS atbilstību standartam un ziņot augstākajai vadībai par ISMS sniegumu ir piešķirtas noteiktai lomai.

Pēc kā to var atpazīt: Iecelšanas vēstule vai lomas apraksts ISMS īpašniekam ar skaidri noteiktu ziņošanas līniju vadībai. Ziņošanas līnijai ir jābūt tiešām apliecinātai ar vadības pārskatīšanas protokolliem.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6 Plānošana

21

6.1.1-1 Sākot no 4.1 jautājumiem un 4.2 prasībām, ir noteikti riski un iespējas, kas prasa rīcību, lai ISMS sasniegtu paredzētos rezultātus un nevēlama ietekme tiktu novērsta.

Pēc kā to var atpazīt: Reģistrs, kas sasaista konteksta jautājumus ar riskiem un iespējām, uzturēts atsevišķi vai risku reģistra ietvaros. Svarīga ir izsekojamība: katrs konteksta analīzes jautājums redzami noved pie novērtējuma vai pie pamatota lēmuma to neizskatīt.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.1-2 Darbības šo risku un iespēju risināšanai ir plānotas, integrētas ISMS procesos, un to rezultativitāte tiek novērtēta.

Pēc kā to var atpazīt: Rīcības plāns ar atbildīgo, termiņu un rezultativitātes kritēriju. Rezultativitātes novērtējumu uztur kā atsevišķu sleju, citādi auditā trūkst pierādījuma, ka darbība ir ne tikai ieviesta, bet arī pārbaudīta.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.2-1 Informācijas drošības risku novērtēšanas process ir noteikts un tiek piemērots; tajā ir riska pieņemšanas kritēriji un kritēriji risku novērtēšanas veikšanai. Dokuments

Pēc kā to var atpazīt: Risku pārvaldības politika ar iespējamības un ietekmes skalām, noteikta risku matrica un skaidrs pieņemšanas sliekšnis. Sliekšnim ir jābūt skaitlīam vai zonai, nevis frāzei, piemēram, pēc pašu ieskatiem.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.2-2 Process nodrošina, ka atkārtota risku novērtēšana dod konsekventus, derīgus un salīdzināmus rezultātus.

Pēc kā to var atpazīt: Apliecināms ar noteiktu metodiku, kurā ir definētas skalas, un salīdzinot divas novērtējuma versijas: tie paši riski, tā pati vērtēšanas loģika, izskaidrojamas atšķirības. Pagājušā gada risku reģistra versija ar datumu šeit ir spēcīgākais pierādījums.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.2-3 Informācijas drošības riski ir apzināti, lai tvērumā atklātu konfidencialitātes, integritātes un pieejamības zudumu, un katram riskam ir piešķirts riska īpašnieks.

Pēc kā to var atpazīt: Risku reģistrs ar atsauci uz aktīviem vai procesiem, trim aizsardzības mērķiem un nosauktu riska īpašnieku. Riska īpašniekam ir jābūt pilnvarām risku pieņemt; mazos uzņēmumos tas parasti ir uzņēmuma vadītājs.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.2-4 Apzinātie riski ir analizēti: ir noteiktas iespējamās sekas, reālistiska iespējamība un no tā izrietošais riska līmenis.

Pēc kā to var atpazīt: Slejas ietekmei, iespējamībai un no tām izrietošajam riska līmenim, katrai ar īsu pamatojumu. Viens pamatojuma teikums katram riskam novērš biežāko audita konstatējumu, proti, skaitļus bez atvasinājuma.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.2-5 Riski ir salīdzināti ar pieņemšanas kritērijiem un sakārtoti pēc prioritātes apstrādei.

Pēc kā to var atpazīt: Risku reģistram ir jāparāda, kuri riski ir virs pieņemšanas sliekšņa un kādā secībā tos apstrādās. Pietiek ar sakārtotu skatu vai prioritātes sleju.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.2-6 Risku novērtēšanas process ir pieejams kā dokumentēta informācija.[Dokuments](#)

Pēc kā to var atpazīt: Pati metodika ir obligāts dokuments, ne tikai tās rezultāts. Apstiprināta politika ar versiju un apstiprināšanas datumu, sasaistīta ar ISMS dokumentu rādītāju.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.3-1 Katram riskam virs pieņemšanas sliekšņa ir izraudzīta piemērota apstrādes iespēja (samazināt, izvairīties, nodot vai pieņemt).

Pēc kā to var atpazīt: Apstrādes iespējas sleja risku reģistrā. Ja risks ir pieņemts, reģistrē pamatojumu un riska īpašnieka formālo apstiprinājumu; ja tas ir nodots, nosauc līgumu vai apdrošināšanas polisi.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.3-2 Visi kontroles pasākumi, kas nepieciešami izraudzīto risku apstrādes iespēju īstenošanai, ir noteikti.

Pēc kā to var atpazīt: Kontroles pasākumus formulē konkrēti un pārbaudāmi, ar atbildīgo un termiņu. Atsauce uz jau notiekošu tehnisku darbu (MFA ieviešana, rezerves kopiju pārbaude) ir pieņemama, ja tā norāda uz pieteikumu vai konfigurācijas artefaktu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.3-3 Noteiktie kontroles pasākumi ir salīdzināti ar A pielikuma kontroles pasākumiem, lai pārliecinātos, ka neviens nepieciešams kontroles pasākums nav palaists garām.

Pēc kā to var atpazīt: Salīdzinājums ir atsevišķs, izsekojams solis, nevis blakusprodukts. Apliecināms ar sasaistes sleju risku reģistrā, kas atsaucas uz A pielikuma numuriem, un salīdzinājuma protokolu ar datumu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.3-4

Pastāv piemērojamības paziņojums (SoA). Tajā ir atsevišķi izvērtēti visi 93 A pielikuma kontroles pasākumi, katram ir norādīta piemērojamība ar pamatojumu, ieviešanas statuss un pamatojums katrai izslēgšanai.[Dokuments](#)

Pēc kā to var atpazīt: SoA ir galvenais obligātais dokuments un visa audita karte. Tam ir jābūt pilnīgam: arī nepiemērojamie kontroles pasākumi tajā parādās ar pamatojumu, nekad kā tukša rinda. Ieteicamās slejas: kontroles pasākuma numurs, nosaukums, piemērojams jā vai nē, pamatojums, ieviešanas statuss, atsaucē uz politiku vai pierādījumu, saite uz risku. Versija un vadības apstiprinājums ir obligāti, jo SoA katrā uzraudzības auditā salīdzina ar īstenību.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.3-5

Ir sagatavots risku apstrādes plāns, kas apvieno kontroles pasākumus, atbildības, termiņus un nepieciešamos resursus.[Dokuments](#)

Pēc kā to var atpazīt: Tā var būt cilne risku izklājlapā vai projekta tāfele. Svarīgi ir, lai termiņi būtu reālistiski un lai nokavētie termiņi būtu redzami pārplānoti, jo tieši to auditors pārbauda.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.3-6

Risku apstrādes plānu ir apstiprinājuši risku īpašnieki, un tie ir formāli pieņēmuši atlikušos paliekošos riskus.[Dokuments](#)

Pēc kā to var atpazīt: Paraksts, elektronisks apstiprinājums vai lēmums protokolā ar datumu. Pietiek ar vienu rindu vadības pārskatīšanas protokolā, kas atsaucas uz reģistra versiju, ja versija ir nepārprotama.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.1.3-7

Risku apstrādes process ir pieejams kā dokumentēta informācija.[Dokuments](#)

Pēc kā to var atpazīt: Parasti to aptver tas pats politikas dokuments, kas risku novērtēšanu. Ir jāapraksta ceļš no novērtēšanas caur iespējas izvēli līdz paliekošā riska pieņemšanai.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.2-1

Informācijas drošības mērķi ir izveidoti būtiskajām funkcijām un līmeņiem, saskan ar politiku un ir izmērāmi, kur tas ir praktiski iespējams.

Pēc kā to var atpazīt: Mērķu lapa ar trim līdz sešiem mērķiem, katram ar rādītāju, sākuma vērtību, mērķa vērtību un termiņu. Piemēram: sistēmu daļa ar MFA palielināta no 80 līdz 100 procentiem līdz ceturkšņa beigām. Mērķus bez skaitļa uzskata par neizmērāmiem.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.2-2

Mērķos ir ņemtas vērā piemērojamās informācijas drošības prasības, kā arī risku novērtēšanas un risku apstrādes rezultāti.

Pēc kā to var atpazīt: Mērķu lapā pievieno izcelsmes sleju: no kura riska, kuras klienta prasības vai kura tiesību aktā noteikta pienākuma mērķis nāk. Tas novērš mērķus, kas izskatās patvaļīgi.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.2-3

Mērķi tiek uzraudzīti, paziņoti un pēc vajadzības aktualizēti.

Pēc kā to var atpazīt: Ceturkšņa progresu sekošana mērķu lapā un paziņošana komandai, piemēram, īsa piezīme wiki vai darba kārtības punkts komandas sanāksmē. Vēsturiskās versijas apliecina, ka aktualizēšana notiek.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.2-4 Informācijas drošības mērķi ir pieejami kā dokumentēta informācija.[Dokuments](#)

Pēc kā to var atpazīt: Pietiek ar apstiprinātu mērķu dokumentu ar datumu. Tas var būt vadības pārskatīšanas daļa, taču tam tur ir jāpastāv kā atsevišķai atrodamai sadaļai.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.2-5 Katram mērķim ir plānots, kas tiks darīts, kādi resursi ir nepieciešami, kurš ir atbildīgs, kad tas tiks pabeigts un kā rezultāti tiks novērtēti.

Pēc kā to var atpazīt: Šie pieci punkti ir atsevišķi pārbaudāmi, un auditā tos pieprasa katru atsevišķi. Tos veido kā piecas slejas mērķu lapā, tad atbilstība ir redzama uzreiz.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

6.3-1 Ja organizācija konstatē, ka ISMS ir nepieciešamas izmaiņas, šīs izmaiņas tiek veiktas plānotā veidā.

Pēc kā to var atpazīt: Apliecināms ar izmaiņu pieprasījumiem, protokoliem vai pieteikumiem, kas parāda izraisītāju, ietekmes novērtējumu, apstiprinājumu un ieviešanu. Tipiski izraisītāji mazos uzņēmumos: mākoņpakalpojumu sniedzēja maiņa, jaunas atrašanās vietas, pirmais darbinieks.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7 Atbalsts

15

7.1-1 Resursi, kas nepieciešami ISMS izveidei, ieviešanai, uzturēšanai un nepārtrauktai uzlabošanai, ir noteikti un nodrošināti.

Pēc kā to var atpazīt: Drošības budžeta pozīcija, rīku licences (paroļu pārvaldnieks, MDM, žurnālu platforma), plānotās cilvēkdienas ISMS uzturēšanai un ārējie audita pakalpojumi. Rēķins vai budžeta apstiprinājums to pierāda ātrāk nekā jebkurš apraksts.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.2-1 Nepieciešamā kompetence cilvēkiem, kuru darbs ietekmē informācijas drošības sniegumu, ir noteikta.

Pēc kā to var atpazīt: Kompetenču matrica vai lomu apraksti, kuros ir uzskaitītas katrai lomai nepieciešamās zināšanas, piemēram, droša izstrāde izstrādātājiem, notikumu apstrāde koordinātoram. Ļoti mazās komandās pietiek ar vienu rindu katrai personai.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.2-2 Kompetence ir nodrošināta, pamatojoties uz atbilstošu izglītību, apmācību vai pieredzi.

Pēc kā to var atpazīt: Sertifikāti, kursu apliecinājumi, dzīves apraksti vai dokumentēta praktiskā pieredze. Pašmācība ir pieņemama, ja tā ir apliecināta, piemēram, ar tiešsaistes kursu pabeigšanas ierakstiem vai nokārtotiem iekšējiem zināšanu pārbaudījumiem.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.2-3 Ja pastāv kompetences trūkumi, ir veiktas darbības to novēršanai un šo darbību rezultativitāte ir novērtēta.

Pēc kā to var atpazīt: Apmācību plāns ar plānotā un faktiskā salīdzinājumu un rezultativitātes pārbaudi, piemēram, pārbaudījuma rezultāts, pikšķerēšanas simulācijas klikšķu īpatsvars vai novērošana darba vietā. Rezultativitātes pārbaudi bieži aizmirst, un tas ir klasisks neliels konstatējums.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.2-4 Atbilstoša dokumentēta informācija ir pieejama kā kompetences pierādījums.[Dokuments](#)

Pēc kā to var atpazīt: Kompetences vai apmācību mape katrai personai ar pierādījumiem un datumiem. Mazos uzņēmumos pietiek ar direktoriju, kurā glabājas PDF ieraksti, un pārskata tabulu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.3-1 Cilvēki, kas strādā tvērumā, pārzina informācijas drošības politiku.

Pēc kā to var atpazīt: Apstiprinājums ievadapmācībā un pēc katras politikas izmaiņas, ar datumu un versiju. Pietiek ar wiki lasīšanas apstiprinājuma funkciju vai parakstītu sarakstu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.3-2 Cilvēki zina savu ieguldījumu ISMS rezultativitātē un ieguvumus no labāka informācijas drošības snieguma.

Pēc kā to var atpazīt: Apmācību materiāli un dalībnieku saraksti, kuros ir redzama saikne ar personas paša darbu. Auditori runā ar darbiniekiem tieši, tāpēc apmāca ar konkrētiem ikdienas piemēriem, nevis abstraktiem standarta citātiem.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.3-3 Cilvēki zina sekas, kas iestājas, neievērojot ISMS prasības.

Pēc kā to var atpazīt: Sekas ir norādītas apmācību slaidos un darba instrukcijās un sasaistītas ar A.6.4 procesu. Arī uzņēmumiem bez darbiniekiem tas ir jāaptver līgumos ar līgumpartneriem un ārštata speciālistiem.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.4-1 ISMS būtiskā iekšējā un ārējā saziņa ir noteikta: kas tiek paziņots, kad, ar ko un ar kādiem līdzekļiem.

Pēc kā to var atpazīt: Saziņas matrica ar rindām, piemēram, drošības notikums klientiem, paziņojums uzraudzības iestādei 72 stundu laikā, ikmēneša statusa ziņojums vadībai. Tā ir krīzes komunikācijas pamats, un to pārskata pēc katra notikuma.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.5.1-1 ISMS ietver standarta prasīto dokumentēto informāciju, kā arī dokumentēto informāciju, ko organizācija ir atzinusi par nepieciešamu ISMS rezultativitātei.[Dokuments](#)

Pēc kā to var atpazīt: Dokumentu rādītājs, kurā ir uzskaitīts katrs ISMS dokuments ar mērķi, īpašnieku, versiju un glabāšanas vietu. Tas parāda, ka obligātie dokumenti ir pilnīgi, un ir ātrākais ieejas punkts auditoram.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.5.2-1 Veidojot un aktualizējot dokumentus, ir nodrošināta atbilstoša identifikācija, formāts un datu nesējs, un dokumenti tiek pārskatīti un apstiprināti kā piemēroti.

Pēc kā to var atpazīt: Vienota dokumenta galvene ar nosaukumu, versiju, datumu, autoru un apstiprinātāju. Uz Git balstītā vidē izmaiņu pieprasījumu pārskatīšana ar apstiprinājumu izpilda pārskatīšanas un apstiprināšanas prasību, ja vēsture ir nemaināma.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.5.3-1 Dokumentēta informācija ir pieejama un lietojama tur un tad, kad tā ir nepieciešama.

Pēc kā to var atpazīt: Centrāla glabāšanas vieta, sasniedzama visiem, kam ir tiesības, ar meklēšanas funkciju. Pārbaudāms ar izlasi: jebkura darba instrukcija ir atrodamā mazāk nekā minūtē.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

7.5.3-2 Dokumentēta informācija ir pietiekami aizsargāta, jo īpaši pret konfidencialitātes zudumu, nepareizu lietošanu un integritātes zudumu.

Pēc kā to var atpazīt: Uz lomām balstītas piekļuves tiesības ISMS dokumentiem, versiju veidošana ar vēsturi, rakstīšanas aizsardzība apstiprinātajām versijām un dokumentu krātuves rezerves kopija. Rezerves kopijas pierādījums ir tā daļa, ko visbiežāk aizmirst.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

7.5.3-3 Dokumentētas informācijas izplatīšana, piekļuve, atrašana, glabāšana, izmaiņu kontrole, kā arī saglabāšana un iznīcināšana ir noteiktas.

Pēc kā to var atpazīt: Īss dokumentu pārvaldības noteikums ar glabāšanas termiņiem un dzēšanas noteikumiem. Tas ir jāaskaņo ar tiesību aktos noteiktajiem pienākumiem (komerciesības, nodokļu tiesības, GDPR), un tas ir pamats A.5.33 un A.8.10.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

7.5.3-4 Ārējas izcelsmes dokumentēta informācija, kas nepieciešama ISMS plānošanai un darbībai, ir apzināta un pārvaldīta.

Pēc kā to var atpazīt: Ārējo dokumentu saraksts ar versiju un avotu: standarti, tiesību aktu teksti, ražotāju nostiprināšanas ceļveži, mākoņpakalpojumu drošības dokumentācija, datu apstrādes līgumi. Bez atsaucē uz versiju pārvaldību nav iespējams apliecināt.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

8 Darbība**8****8.1-1 Procesi, kas nepieciešami informācijas drošības prasību izpildei un 6. nodaļas darbību īstenošanai, ir plānoti, ieviesti un vadīti, un šiem procesiem ir noteikti kritēriji.**

Pēc kā to var atpazīt: Darbības rokasgrāmata vai izpildes apraksti ar skaidriem kritērijiem, piemēram, maksimālais laiks kritisku ielāpu ieviešanai, laidiena kritēriji izvietošanai, trauksmes sliekšņi. Kritēriji bez skaitļiem auditā neko nedod.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

8.1-2 Dokumentēta informācija ir pieejama tādā apjomā, lai būtu pārlicība, ka procesi ir izpildīti, kā plānots.[Dokuments](#)

Pēc kā to var atpazīt: Darbības ieraksti kā pierādījums: pieteikumu vēsture, CI konveijera izpildes, ielāpu ziņojumi, rezerves kopiju žurnāli, piekļuves pārskatīšanas. Šie ieraksti ir īstais rezultativitātes pierādījums 2. posma auditā.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

8.1-3 Plānotās izmaiņas tiek vadītas, un neplānotu izmaiņu sekas tiek pārskatītas; kur nepieciešams, nelabvēlīgā ietekme tiek mazināta.

Pēc kā to var atpazīt: Izmaiņu process ar apstiprinājumu un atgriešanās ceļu, saistīts ar A.8.32. Neplānotām izmaiņām (nepareiza konfigurācija, nejauša tiesību paaugstināšana) notikumu dokumentē un labojumu apliecina.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

8.1-4 Ārēji nodrošinātie procesi, produkti un pakalpojumi, kas ir būtiski ISMS, ir noteikti un pārvaldīti.

Pēc kā to var atpazīt: Piegādātāju saraksts ar kritiskumu, līguma atsauci un pierādījumu stāvokli (pakalpojuma sniedzēja ISO 27001 sertifikāts, SOC 2 ziņojums, datu apstrādes līgums). Mazos uzņēmumos tā ir lielākā svira, jo lielākā daļa IT tāpat darbojas ārēji.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

8.2-1 Risku novērtēšana tiek veikta plānotos intervālos un ikreiz, kad notiek būtiskas izmaiņas vai notikumi, ņemot vērā noteiktos kritērijus.

Pēc kā to var atpazīt: Ritms (parasti reizi gadā) un noteikti izraisītāji ārpuskārtas novērtēšanai. Apliecināms ar risku reģistra versijām ar datumiem un ierakstiem kalendārā vai pieteikumu sistēmā.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

8.2-2 Risku novērtēšanas rezultāti tiek saglabāti kā dokumentēta informācija.

[Dokuments](#)

Pēc kā to var atpazīt: Risku reģistra vēsturiskās versijas ar datumiem, nevis tikai pašreizējais stāvoklis. Pārrakstot datni, attīstību nav iespējams pierādīt; to atrisina versiju veidošana datņu sistēmā vai Git.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

8.3-1 Risku apstrādes plāns ir ieviests.

Pēc kā to var atpazīt: Salīdzina plānu ar īstenību: pabeigtās darbības ar ieviešanas datumu un konkrētu artefaktu (konfigurācija, politika, līgums). Atvērtām darbībām ir nepieciešams dokumentēts pamatojums un jauns mērķa datums.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

8.3-2 Risku apstrādes rezultāti tiek saglabāti kā dokumentēta informācija.

[Dokuments](#)

Pēc kā to var atpazīt: Statusa ziņojumi vai slēgtas darbības ar atsauci uz pierādījumu. Pietiek ar pašu reģistru, ja katrā rindā ir pabeigšanas datums un saite uz pierādījumu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9 Snieguma novērtēšana

21

9.1-1 Ir noteikts, ko uzrauga un mēra, tostarp informācijas drošības procesi un kontroles pasākumi.

Pēc kā to var atpazīt: Rādītāju lapa ar pārskatāmu skaitu stabilu mēru: ielāpu atlikums, MFA pārklājums, notikumu novēršanas laiks, pēdējās atjaunošanas pārbaudes rezultāts, atvērtie konstatējumi. Daži rādītāji, ko tiešām savāc, ir vērtīgāki par garu vēlmju sarakstu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.1-2 Uzraudzības, mērīšanas, analīzes un novērtēšanas metodes ir noteiktas un dod derīgus rezultātus.

Pēc kā to var atpazīt: Katram rādītājam dokumentē datu avotu un aprēķinu, piemēram, eksportu no ievainojamību skenera vai no identitātes pakalpojuma sniedzēja ziņojuma. Avota izsekojamība ir derīguma kodols.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.1-3 Ir noteikts, kad un kurš veic uzraudzību un mērīšanu un kad rezultātus analizē un novērtē.

Pēc kā to var atpazīt: Rādītāju lapai pievieno slejas biežumam un atbildīgajam. Atkārtots kalendāra ieraksts novērtēšanai pierāda regularitāti labāk nekā jebkurš apraksts.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.1-4 Uzraudzības un mērīšanas rezultāti tiek saglabāti kā dokumentēta informācija.

[Dokuments](#)

Pēc kā to var atpazīt: Arhivēti novērtējumi, eksportēti informācijas paneļi vai rādītāju lapa, ko uztur kā laikrindu. Reāllaika skats bez vēstures prasību neizpilda.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.1-5 Informācijas drošības sniegums un ISMS rezultativitāte ir novērtēti, pamatojoties uz mērījumu rezultātiem.

Pēc kā to var atpazīt: Rakstisks novērtējums, ne tikai skaitļi: tendence, cēloņi, rīcības nepieciešamība. Šis novērtējuma teksts vienlaikus ir ievaddati vadības pārskatīšanai.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.2.1-1 Iekšējie auditi tiek veikti plānotos intervālos un sniedz informāciju par to, vai ISMS atbilst organizācijas pašas prasībām un standarta prasībām un vai tā ir rezultatīvi ieviesta.

Pēc kā to var atpazīt: Pirms sertifikācijas audita ir jāpabeidz vismaz viens pilns iekšējā audita cikls, kas aptver visu tvērumu. Bez tā sertifikācija nav sasniedzama; tas ir viens no biežākajiem kļūšanas akmeņiem pirmajās sertifikācijās.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.2.2-1 Audita programma ir plānota, izveidota un tiek uzturēta; tajā ir noteikts biežums, metodes, atbildības, plānošanas prasības un ziņošana, un tā ņem vērā attiecīgo procesu nozīmi un iepriekšējo auditu rezultātus.

Pēc kā to var atpazīt: Vairāku gadu audita programma, kas sertifikācijas ciklā aptver visas nodaļas un visus piemērojamos kontroles pasākumus, ar lielāku biežumu kritiskajās jomās. Pilnībā pietiek ar vienkāršu tabulu, kas aptver trīs gadus.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.2.2-2 Katram auditam ir noteikti audita kritēriji un audita tvērums.

Pēc kā to var atpazīt: Audita plāns katram datumam ar kritērijiem (standarts, iekšējās politikas, līgumi) un skaidru tvērumu. Pietiek ar vienas lappuses audita plānu katram auditam, un tas vienlaikus kalpo par pamatu ziņojumam.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.2.2-3 Auditori ir izraudzīti un auditi tiek veikti tā, lai nodrošinātu objektivitāti un neitralitāti. Nevienam neveic sava darba auditu.

Pēc kā to var atpazīt: Neatkarība šeit ir grūtākais šķērslis: kas rakstīja politikas un konfigurēja sistēmas, tas nedrīkst tās auditēt. Ļoti mazos uzņēmumos tas gandrīz vienmēr nozīmē ārēju iekšējo auditoru, piemēram, piesaistītu konsultantu vai kolēģi no partneruzņēmuma; pierādījums ir audita līgums un auditora neatkarības apliecinājums. Tikai pietiekami lielās komandās lomu var iekšēji rotēt uz personu, kas neatbild par auditējamo jomu, un tas tad ir jāparāda lomu matricā.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.2.2-4 Audita rezultāti ir paziņoti attiecīgajai vadībai.

Pēc kā to var atpazīt: Audita ziņojums ar konstatējumiem, neatbilstībām, ieteikumiem un izplatīšanas sarakstu, kā arī pierādījums par nodošanu vadībai, piemēram, protokolēts punkts vai nodošana ar e-pastu, kam ir datums.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.2.2-5 Dokumentēta informācija par audita programmu un audita rezultātiem tiek saglabāta.[Dokuments](#)

Pēc kā to var atpazīt: Audita programmu, audita plānus, audita ziņojumus un no tiem izrietošās darbības uztur vienuviet. Saitei no konstatējuma uz korektīvo darbību (10.2 nodaļa) ir jābūt redzamai no sākuma līdz beigām.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.3.1-1

Augstākā vadība pārskata ISMS plānotos intervālos, lai pārlicinātos par tās nepārtrauktu piemērotību, atbilstību un rezultativitāti.

Pēc kā to var atpazīt: Vismaz reizi gadā un iepļānots pirms ārējā audita. Arī ļoti mazos uzņēmumos ir jābūt protokolam ar datumu un parakstu, arī tad, ja vadība un ISMS īpašnieks ir viena persona.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.3.2-1

Vadības pārskatīšanā tiek izskatīts iepriekšējo vadības pārskatīšanu darbību statuss.

Pēc kā to var atpazīt: Protokols sākas ar pagājušā gada lēmumu un to pašreizējā statusa izsekošanas tabulu. Bez šīs atsaucē uz iepriekšējiem lēmumiem pārskatīšanu uzskata par nepilnīgu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.3.2-2

Vadības pārskatīšanā tiek izskatītas izmaiņas ārējos un iekšējos jautājumos, kas ir būtiski ISMS, tostarp būtiskie klimata pārmaiņu aspekti.

Pēc kā to var atpazīt: Atsevišķs darba kārtības punkts ar atsauci uz aktualizēto konteksta analīzi. Šīs nodaļas tekstā klimata pārmaiņas nav nosauktas tieši (Amd 1:2024 maina tikai 4.1 un 4.2), taču tās šeit ienāk caur izmaiņām 4.1 jautājumos, un auditori to sagaida. Arī rezultāts, ka jautājums nav būtisks un nav mainījies, pieder pie protokola.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.3.2-3

Vadības pārskatīšanā tiek izskatītas izmaiņas ieinteresēto pušu vajadzībās un gaidās, kas ir būtiskas ISMS.

Pēc kā to var atpazīt: Jaunas klientu prasības no līgumiem un drošības aptaujas anketām, jauni tiesību aktos noteikti pienākumi, sertifikācijas institūcijas prasības. Tās protokolā reģistrē kā sarakstu ar avotiem.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.3.2-4

Vadības pārskatīšanā tiek izskatīta atgriezeniskā saite par informācijas drošības sniegumu, tostarp neatbilstības un korektīvās darbības, uzraudzības un mērīšanas rezultāti, auditu rezultāti un informācijas drošības mērķu izpilde.

Pēc kā to var atpazīt: Šos četrus blokus izskata kā atsevišķus darba kārtības punktus, citādi vēlāk protokolā kāds no tiem trūks. Rādītāju lapu, audita ziņojumu un mērķu lapu pievieno kā pielikumus.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.3.2-5

Vadības pārskatīšanā tiek izskatīta ieinteresēto pušu atgriezeniskā saite.

Pēc kā to var atpazīt: Klientu sūdzības ar drošības aspektu, klientu auditu rezultāti, ziņojumi no trauksmes celšanas kanāla, pakalpojumu sniedzēju atsauksmes. To reģistrē protokolā arī tad, ja konstatējums ir, ka nekas nav saņemts.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.3.2-6

Vadības pārskatīšanā tiek izskatīti risku novērtēšanas rezultāti un risku apstrādes plāna statuss.

Pēc kā to var atpazīt: Pievieno pašreizējo risku reģistru un apstrādes plāna ieviešanas statusu ar skaidru risku īpašnieku apstiprinājumu par paliekošā riska pieņemšanu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

9.3.2-7 Vadības pārskatīšanā tiek izskatītas nepārtrauktas uzlabošanas iespējas.

Pēc kā to var atpazīt: Darba kārtības punkts ar konkrētām uzlabojumu idejām un lēmumu par katru no tām. Pieņemtās idejas nonāk uzlabojumu reģistrā kā ieraksti ar termiņiem.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

9.3.3-1 Vadības pārskatīšanas rezultātos ir lēmumi par nepārtrauktas uzlabošanas iespējām un par ISMS izmaiņu nepieciešamību.

Pēc kā to var atpazīt: Protokols beidzas ar lēmumu sadaļu: lēmums, atbildīgais, termiņš. Protokols bez lēmumiem auditā ir konstatējums, jo tad trūkst vadības ietekmes.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

9.3.3-2 Dokumentēta informācija tiek saglabāta kā pierādījums par vadības pārskatīšanas rezultātiem.[Dokuments](#)

Pēc kā to var atpazīt: Parakstīts protokols ar datumu, dalībniekiem, ievaddatiem, novērtējumu un lēmumiem. Tas ir viens no pirmajiem dokumentiem, ko sertifikācijas institūcija pieprasa 1. posmā.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

10 Uzlabošana**7****10.1-1 ISMS piemērotība, atbilstība un rezultativitāte tiek nepārtraukti uzlabota.**

Pēc kā to var atpazīt: Uzlabojumu reģistrs, ko papildina vairāki avoti (auditi, notikumi, idejas, rādītāju novirzes), ar laika gaitā redzamu virzību. Pierādījums ir nepārtrauktība vairāku mēnešu garumā, nevis ierakstu skaits.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

10.2-1 Kad rodas neatbilstība, organizācija uz to reaģē: to ierobežo un izlabo un risina tās sekas.

Pēc kā to var atpazīt: Neatbilstības ziņojums ar tūlītēju darbību un datumu. Avoti ir iekšējie auditi, ārējie auditi, notikumi un novērojumi ikdienas darbā; tie visi papildina vienu un to pašu reģistru.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

10.2-2 Ir novērtēts, vai ir nepieciešama darbība cēloņu novēršanai, lai neatbilstība neatkārtotos un nerastos citur; tas ietver pārbaudi, vai līdzīgas neatbilstības pastāv vai varētu rasties.

Pēc kā to var atpazīt: Pamatcēloņa analīzi dokumentē, piemēram, ar 5 kāpēc metodi vai Išikavas diagrammu, un papildina ar skaidru izteikumu par pārnēsāmību uz citām sistēmām vai procesiem. Pārnēsāmības solis ir tas, ko visbiežāk izlaiž.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

10.2-3 Visas nepieciešamās korektīvās darbības ir ieviestas, un to rezultativitāte ir pārskatīta.

Pēc kā to var atpazīt: Katrai darbībai reģistrē ieviešanas datumu, pierādījuma artefaktu un vēlāku rezultativitātes pārbaudi ar savu datumu. Divi datuma lauki katrā rindā ir vienkāršākais veids, kā nepazaudēt rezultativitātes pārbaudi.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

10.2-4 Kur nepieciešams, neatbilstības rezultātā ISMS tiek veiktas izmaiņas.

Pēc kā to var atpazīt: Ja neatbilstība ir izsekojama līdz robam politikā, risku reģistrā vai SoA, izmaiņām tur ir jābūt redzamām. Atsauce no neatbilstības uz aktualizēto dokumenta versiju noslēdz ķēdi.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

10.2-5 Korektīvās darbības ir samērīgas ar konstatēto neatbilstību ietekmi.

Pēc kā to var atpazīt: Smaguma pakāpes vērtējums reģistrā, no kura ir redzama darbības samērība. Sīkumus nerisina kā projektu, un uz nopietnām novirzēm neatbild ar vienkāršu atgādinājuma e-pastu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

10.2-6 Dokumentēta informācija tiek saglabāta par neatbilstību būtību, veiktajām darbībām un korektīvo darbību rezultātiem.

Dokuments

Pēc kā to var atpazīt: Neatbilstību un korektīvo darbību reģistrs ar slejām būtībai, cēlonim, darbībai, atbildīgajam, termiņam un rezultativitātes pārbaudes rezultātam. Tas ir obligāts pierādījums, un to pieprasa katrā uzraudzības auditā.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5 A pielikums: Organizatoriskie kontroles pasākumi 37

A.5.1 Informācijas drošības politikas: Ir noteikta visaptveroša informācijas drošības politika un tematiskās politikas, tās ir apstiprinājuši vadība, tās ir paziņotas un tiek pārskatītas plānotos intervālos un ikreiz, kad notiek būtiskas izmaiņas.

Dokuments

Pēc kā to var atpazīt: Politiku kopums ar versiju, apstiprināšanas datumu un nākamās pārskatīšanas datumu, kā arī iepazīšanās apliecinājums. Maziem uzņēmumiem pietiek ar ietvara politiku un dažām tematiskajām politikām (piekļuve, kriptogrāfija, attālinātais darbs, notikumi).

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.2 Informācijas drošības lomas un atbildības: Informācijas drošības lomas un atbildības ir noteiktas un piešķirtas atbilstoši organizācijas vajadzībām.

Pēc kā to var atpazīt: Lomu matrica ar konkrētām personām, aizvietotājiem un uzdevumiem. Ļoti mazos uzņēmumos atklāti norāda, kur vairākas lomas uzkrājas vienā personā, un sasaista to ar kompensējošajiem kontroles pasākumiem A.5.3.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.3 Pienākumu nodalīšana: Pienākumi un atbildības jomas, kas ir paredzētas savstarpējai kontrolei, nav vienas personas rokās. Mērķis ir tāds, ka neviens nevar patstāvīgi ierosināt, apstiprināt un noslēpt izmaiņu.

Pēc kā to var atpazīt: Mazos uzņēmumos pilnīga nodalīšana strukturāli nav iespējama; vispārīgs apgalvojums par atbilstību audita intervijā sabrūk uzreiz. Noturīga ir godīga analīze: kuras pienākumu kombinācijas ir kritiskas (izstrādāt un laist klajā, piešķirt tiesības un tās izmantot, ierosināt un apstiprināt maksājumus), kuras no tām ir vienas personas rokās un kuri kompensējošie kontroles pasākumi tiek piemēroti. Sevi pierādījušas pieejas ir nemaināmi audita žurnāli, kas pieejami trešajai personai, MFA privileģētajiem kontiem, automatizēti CI vārti un zaru aizsardzība četru acu principa vietā, periodiska žurnālu pārskatīšana, ko veic ārēja persona, un atsevišķs maksājumu apstiprinājums. Analīzi un kompensējošos kontroles pasākumus uztur kā atsevišķu dokumentu ar datumu un sasaista no SoA.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.4 Vadības atbildība: Vadība prasa visam personālam piemērot informācijas drošību saskaņā ar noteiktajām politikām un procedūrām.

Pēc kā to var atpazīt: Apņemšanās darba un uzņēmuma līgumos, politiku apstiprināšana ievadapmācībā un regulāri vadības atgādinājumi. Pierādījums: parakstītas apņemšanās un sanāksmju protokoli.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.5 Saziņa ar iestādēm: Ar attiecīgajām iestādēm tiek uzturēti atbilstoši kontakti, un tie ir sasniedzami, kad tas ir nepieciešams.

Pēc kā to var atpazīt: Kontakta saraksts ar kompetento datu aizsardzības iestādi, policiju vai kibernetizācijas vienību, valsts kibernetizācijas ziņošanas punktu un, ja tas ir tvērumā, NIS2 ziņošanas kanāliem. Termiņus (piemēram, 72 stundas saskaņā ar GDPR) atzīmē tieši sarakstā.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.6 Saziņa ar īpašu interešu grupām: Tiek uzturēti kontakti ar īpašu interešu grupām, drošības forumiem un profesionālajām apvienībām.

Pēc kā to var atpazīt: Dalība organizācijās, abonēti brīdinājumi (valsts CERT, ražotāju plūsmas), līdzdalība īpašu interešu grupās. Vienkāršs pierādījums: abonementu saraksts un viens piemērs, kā brīdinājums noveda pie darbības.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.7 Informācija par apdraudējumiem: Informācija par informācijas drošības apdraudējumiem tiek vākta un analizēta, lai no tās atvasinātu atbilstošas darbības.

Pēc kā to var atpazīt: Jauns 2022. gada izdevumā. Maziem uzņēmumiem īstenojams tā: abonē valsts CERT un ražotāju brīdinājumus, pēc tam reizi mēnesī veic īsu pārskatīšanu ar lēmumu par nozīmīgumu un no tā atvasinātiem pieteikumiem. Pierādījums ir analīze, nevis abonements.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.8 Informācijas drošība projektu vadībā: Informācijas drošība ir integrēta projektu vadībā neatkarīgi no projekta veida.

Pēc kā to var atpazīt: Drošības punkti projekta kontrolesarakstā: aizsardzības vajadzības, risku pārskatīšana, datu aizsardzības pārbaude, drošības apstiprinājums pirms nodošanas ekspluatācijā. Elastīgās komandās tos nostiprina kā pastāvīgus punktus gatavības definīcijā un pabeigšanas definīcijā.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.9 Informācijas un citu saistīto aktīvu uzskaitē: Ir izveidota un tiek uzturēta informācijas un citu saistīto aktīvu uzskaitē ar nosauktiem īpašniekiem.

Pēc kā to var atpazīt: Aktīvu uzskaitē, kas aptver aparatūru, programmatūru, mākoņpakalpojumus, datu krātuves, domēnus un kontus, katram ar īpašnieku un aizsardzības vajadzībām. Mazos uzņēmumos to var automatiski salikt no MDM eksporta, licenču saraksta un mākoņa konsoles; aktuāls datums ir obligāts.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.10 Informācijas un citu saistīto aktīvu pieļaujamā lietošana: Noteikumi par informācijas un citu saistīto aktīvu pieļaujamu lietošanu un rīcību ar tiem ir apzināti, dokumentēti un ieviesti.[Dokuments](#)

Pēc kā to var atpazīt: Pieļaujamās lietošanas politika ierīcēm, tīkliem, mākoņa kontiem un mākslīgā intelekta rīkiem, ar iepazīšanās apliecinājumu. Personiskās ierīces un ārējie mākslīgā intelekta pakalpojumi ir jāaptver skaidri, jo tieši tur notiek lielākā daļa noplūžu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.11 Aktīvu atdošana: Kad darba attiecības beidzas vai mainās, ir noteikts un rakstiski apstiprināts, ka visas izsniegtās ierīces, atslēgas, konti un dokumenti ir atdoti.

Pēc kā to var atpazīt: Aiziešanas kontrolesaraksts ar atdošanas apliecinājumu klēpj datoram, marķieriem, atslēgām, sertifikātiem un datu nesējiem, kā arī kontu atslēgšana tajā pašā dienā. Tas tāpat attiecas uz ārštata speciālistiem un praktiskantiem.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.12 Informācijas klasificēšana: Informācija ir klasificēta atbilstoši tās aizsardzības vajadzībām attiecībā uz konfidencialitāti, integritāti, pieejamību un tiesību aktu prasībām.

Pēc kā to var atpazīt: Vienkārša shēma ar trim vai četriem līmeņiem (publiska, iekšējs, konfidenciāls, stingri konfidenciāls) un konkrētiem rīcības noteikumiem katram līmenim. Piešķirumu reģistrē aktīvu uzskaitē vai apstrādes darbību reģistrā.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.5.13 Informācijas marķēšana: Klasifikācijas līmenis ir atpazīstams uz paša dokumenta, datnes vai ziņojuma, tāpēc saņēmēji zina, kā ar to rīkoties, bez papildu jautājumiem.

Pēc kā to var atpazīt: Marķējums dokumenta galvenē, datnes nosaukumā, e-pasta tēmā vai ar jutīguma marķējumiem mākoņa biroja komplektā. Pierādījums ar tiešām marķētu dokumentu paraugiem, nevis tikai ar noteikumu.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.5.14 Informācijas nodošana: Pastāv noteikumi, procedūras un vienošanās informācijas nodošanai organizācijā un ar ārējām pusēm.

Pēc kā to var atpazīt: Noteikums, kurā ir pateikts, kurš kanāls ir atļauts kuram klasifikācijas līmenim: šifrēts e-pasts vai datu telpa konfidencialam saturam, nekādas sūtīšanas ar privātiem ziņojumapmaiņas rīkiem. Konfidencialu nodošanu nostiprina ar neizpaušanas līgumiem.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.5.15 Piekļuves pārvaldība: Noteikumi fiziskas un loģiskas piekļuves pārvaldībai informācijai un citiem saistītajiem aktīviem ir izveidoti un ieviesti, pamatojoties uz darbības un drošības prasībām.

Pēc kā to var atpazīt: Piekļuves pārvaldības politika, kas seko principiem zināt tikai nepieciešamo un mazākās nepieciešamās tiesības, ar lomu un tiesību sasaisti. Pierādījums ar faktisko tiesību konfigurāciju identitātes pakalpojuma sniedzējā, nevis tikai ar politiku.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.5.16 Identitātes pārvaldība: Tiek pārvaldīts pilns identitāšu dzīves cikls.

Pēc kā to var atpazīt: Process no izveides caur izmaiņām līdz atslēgšanai, vēlams centralizēts identitātes pakalpojuma sniedzējā ar vienotu pieteikšanos. Nekādu koplietotu grupas kontu; kur tehniski nav citas iespējas, kontu nosauc, pamato un tā lietošanu žurnālē.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.5.17 Autentifikācijas informācija: Autentifikācijas informācijas piešķiršanu un pārvaldību vada pārvaldības process, kas prasa, lai cilvēki ar to rīkojas pareizi.

Pēc kā to var atpazīt: Paroļu pārvaldnieks kā obligāts rīks, politika par parolu kvalitāti un MFA, droša sākotnējā piekļuve un atiestatīšanas procedūra ar identitātes pārbaudi. Pierādījums ar konfigurācijas ekrānattēliem un parolu pārvaldnieka ziņojumu.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.5.18 Piekļuves tiesības: Piekļuves tiesības tiek piešķirtas, pārskatītas, mainītas un atceltas saskaņā ar piekļuves pārvaldības politiku.

Pēc kā to var atpazīt: Periodiska piekļuves pārskatīšana vismaz reizi gadā ar dokumentētu rezultātu katram kontam un pierādījumu par atceltajām tiesībām. Tiesību atcelšana aiziešanas dienā ir punkts, ko auditori labprāt izseko konkrētā gadījumā.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.5.19

Informācijas drošība attiecībā ar piegādātājiem: Procesi un procedūras drošības risku pārvaldībai, kas rodas no trešo pušu produktu un pakalpojumu izmantošanas, ir noteikti un ieviesti.

Pēc kā to var atpazīt: Piegādātāju saraksts ar kritiskuma līmeni un novērtēšanas dziļumu. Kritiskajiem pakalpojumu sniedzējiem iegūst pierādījumus (ISO 27001 sertifikāts, SOC 2 ziņojums), nevis veic pašu auditus, un maziem uzņēmumiem tas ir vienīgais reālistiskais ceļš.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.20

Informācijas drošība piegādātāju līgumos: Ar katru piegādātāju ir saskaņotas būtiskās drošības prasības, un tās ir iekļautas līgumos.

Pēc kā to var atpazīt: Informācijas drošības līguma pielikums ar pienākumu ziņot par notikumiem, noteikumiem par apakšapstrādātājiem, dzēšanas pienākumiem un audita tiesībām. Standarta pakalpojumiem pietiek ar pakalpojuma sniedzēja noteikumiem un datu apstrādes līgumu, ja to saturis ir pārskatīts un dokumentēts.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.21

Informācijas drošības pārvaldība IKT piegādes ķēdē: Procesi drošības risku pārvaldībai informācijas un komunikācijas tehnoloģiju piegādes ķēdē ir noteikti un ieviesti.

Pēc kā to var atpazīt: Tas aptver programmatūras atkarības un pašu pakalpojumu sniedzēju apakšpiegādātājus. Praksē: programmatūras sastāvdaļu saraksts (SBOM) vai atkarību saraksts, automatizētas ievainojamu pakotņu pārbaudes CI un programmatūras iegāde tikai no parakstītiem vai oficiāliem kanāliem.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.22

Piegādātāju pakalpojumu uzraudzība, pārskatīšana un izmaiņu pārvaldība: Piegādātāju pakalpojumu izmaiņas tiek regulāri uzraudzītas, pārskatītas un pārvaldītas.

Pēc kā to var atpazīt: Ikgadēja piegādātāju pārskatīšana, kurā aplūko notikumus, pieejamības ziņojumus un sertifikātu derīgumu, kā arī kanāls pakalpojuma sniedzēja paziņojumiem par izmaiņām. Rezultātu reģistrē kā īsu piezīmi katram piegādātājam.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.23

Informācijas drošība mākoņpakalpojumu izmantošanā: Procesi mākoņpakalpojumu iegādei, izmantošanai, pārvaldībai un izbeigšanai ir izveidoti saskaņā ar drošības prasībām.

Pēc kā to var atpazīt: Jauns 2022. gada izdevumā un galvenais kontroles pasākums maziem uzņēmumiem, kas balstās uz mākonī. Pierādījums ar mākoņa politiku, kurā ir jaunu pakalpojumu apstiprināšanas process, dokumentēts dalītās atbildības modelis katram pakalpojumam, nostiprināšanas iestatījumi un izbeigšanas stratēģija, tostarp datu atgriešana un dzēšanas apstiprinājums.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.24

Informācijas drošības notikumu pārvaldības plānošana un sagatavošana: Procesi, lomas un atbildības notikumu apstrādei ir plānoti un izveidoti.

Dokuments

Pēc kā to var atpazīt: Reaģēšanas plāns ar ziņošanas ceļu, lomām, eskalācijas līmeņiem, ārpus darba laika kontaktiem un saziņas veidnēm. Mazām komandām reālistiski: viena lappuse, bet nostrādāta.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.25

Informācijas drošības atgadījumu novērtēšana un lēmums par tiem: Drošības atgadījumi tiek novērtēti, un tiek pieņemts lēmums, vai tos klasificē kā informācijas drošības notikumus.

Pēc kā to var atpazīt: Triāžas kritēriji ar smaguma matricu un atgadījumu reģistrs, kurā ar pamatojumu parādās arī noraidītie atgadījumi. Nošķīrumam starp atgadījumu un notikumu ir jābūt redzamam reģistrā.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.26 Reaģēšana uz informācijas drošības notikumiem: Notikumi tiek apstrādāti saskaņā ar dokumentētajām procedūrām.

Pēc kā to var atpazīt: Notikumu lietas ar laika grafiku, veiktajām darbībām, iesaistītajiem cilvēkiem un slēgšanas lēmumu. Ja īsta notikuma vēl nav bijis, labākais pieejamais pierādījums ir dokumentēts galda vingrinājums.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.27 Mācīšanās no informācijas drošības notikumiem: No notikumiem gūtās zināšanas tiek izmantotas drošības kontroles pasākumu stiprināšanai.

Pēc kā to var atpazīt: Bezvainas pēcnotikuma pārskatīšana ar pamatcēloņa analīzi un atvasinātām darbībām, sasaistīta ar uzlabojumu reģistru un, kur nepieciešams, ar risku reģistru.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.28 Pierādījumu vākšana: Ir noteikts, kā ar drošības atgadījumu saistītās pēdas tiek apzinātas, nodrošinātas un saglabātas, lai tās vēlāk paliktu izmantojamas.

Pēc kā to var atpazīt: Īsa pierādījumu saglabāšanas procedūra: sistēmas priekšlaicīgi neatjauno, nodrošina disku attēlus un žurnālus, dokumentē glabāšanas ķēdi. Maziem uzņēmumiem pietiek noteikt, no kura smaguma līmeņa piesaista ārēju kriminālistikas pakalpojumu sniedzēju, un pierakstīt kontaktinformāciju.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.29 Informācijas drošība traucējuma laikā: Organizācija plāno, kā traucējuma laikā informācijas drošība tiek uzturēta atbilstošā līmenī.

Pēc kā to var atpazīt: Ārkārtas risinājumi nedrīkst izslēgt drošību. Dokumentē, ka MFA, žurnālēšana un piekļuves ierobežojumi darbojas arī rezerves režīmā un ka ārkārtas konti (break-glass konti) ir aizzīmogoti, dokumentēti un pēc tam pārskatīti.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.30 IKT gatavība darbības nepārtrauktībai: IKT gatavība ir plānota, ieviesta, tiek uzturēta un pārbaudīta, pamatojoties uz darbības nepārtrauktības mērķiem un IKT nepārtrauktības prasībām.

Pēc kā to var atpazīt: Jauns 2022. gada izdevumā. Pierādījums ar noteikumiem atjaunošanas laika mērķiem (RTO) un atjaunošanas punkta mērķiem (RPO) katrai kritiskajai sistēmai, atjaunošanas procedūru un vismaz vienu dokumentētu pārbaudi gadā. Veiksmīga atjaunošanas pārbaude ar datumu un ilgumu ir spēcīgākais atsevišķais pierādījums.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.31 Juridiskās, likumā noteiktās, regulatīvās un līgumiskās prasības: Būtiskās prasības un to izpildes pieeja ir apzinātas, dokumentētas un tiek uzturētas aktuālas.[Dokuments](#)

Pēc kā to var atpazīt: Tiesību aktu reģistrs, kas aptver GDPR, elektronisko sakaru tiesības, komerciesības un nodokļu tiesības un, kur piemērojams, NIS2 vai nozares noteikumus, katram ar noteikumu, kas to īsteno, un pārskatīšanas datumu. Pietiek ar ikgadēju pārskatīšanu, taču tai ir jābūt ar datumu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.32 Intelektuālā īpašuma tiesības: Ir ieviestas atbilstošas procedūras intelektuālā īpašuma tiesību aizsardzībai.

Pēc kā to var atpazīt: Izmantotās programmatūras licenču uzskaitē, atvērtā pirmkoda licenču pārbaude produktā (licenču skeneris CI) un noteikums rīcībai ar trešo pušu kodu un ģenerētu kodu. Pierādījums: licenču ziņojums no būvējuma.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5.33 Ierakstu aizsardzība: Darbības un pierādījuma ieraksti tiek glabāti tā, ka tie nevar pazust, nevar tikt nemanāmi mainīti un nevar nonākt nepareizās rokās, un tas attiecas uz visu glabāšanas periodu.

Pēc kā to var atpazīt: Glabāšanas grafiks ar tiesību aktos noteiktajiem termiņiem, pret viltošanu noturīga glabāšana, ierobežota piekļuve un rezerves kopija. Nodokļiem būtiskiem ierakstiem tiesību aktos noteiktos glabāšanas termiņus nosauc tieši, jo auditori to labprāt pārbauda mērķtiecīgi.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.5.34 Privātums un personas datu aizsardzība: Prasības privātumam un personas datu (PII) aizsardzībai ir apzinātas un izpildītas saskaņā ar piemērojamiem tiesību aktiem.

Pēc kā to var atpazīt: Apstrādes darbību reģistrs, datu apstrādes līgumi, dzēšanas koncepcija, datu subjektu tiesību process un, kur nepieciešams, novērtējums par ietekmi uz datu aizsardzību. Sasaiste ar ISMS caur kopīgu aktīvu sarakstu ļauj neuzturēt visu divreiz.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.5.35 Neatkarīga informācijas drošības pārskatīšana: Organizācijas pieeja informācijas drošības pārvaldībai tiek neatkarīgi pārskatīta plānotos intervālos un ikreiz, kad notiek būtiskas izmaiņas.

Pēc kā to var atpazīt: Apliecināms ar iekšējo auditu, ko veic neatkarīgs auditors, ar ārējiem ielaušanās testiem vai ar pašu sertifikācijas auditu. Neatkarīgs nozīmē, ka to neveic persona, kas atbild par pārskatāmo jomu.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.5.36 Atbilstība informācijas drošības politikām, noteikumiem un standartiem: Atbilstība organizācijas pašas drošības politikām un piemērojamiem noteikumiem tiek regulāri pārskatīta.

Pēc kā to var atpazīt: Atbilstības pārbaudes ar datumu un rezultātu, piemēram, konfigurācijas salīdzinājums ar pašu nostiprināšanas bāzlīniju, dokumentu marķēšanas izlases pārbaude, automatizētas politiku pārbaudes mākonī. Novirzes nonāk korektīvo darbību reģistrā.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.5.37 Dokumentētas darbības procedūras: Informācijas apstrādes iekārtu darbības procedūras ir dokumentētas un pieejamas cilvēkiem, kam tās ir vajadzīgas.

[Dokuments](#)

Pēc kā to var atpazīt: Izpildes apraksti rezerves kopiju veidošanai un atjaunošanai, izvietojumam, lietotāju administrēšanai, ielāpošanai un notikumu apstrādei. Īss un aktuāls ir labāk nekā plašs un novecojis; pēdējo izmaiņu datums katram izpildes aprakstam ir obligāts.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.6 A pielikums: Personāla kontroles pasākumi

8

A.6.1 Kandidātu pārbaude: Kandidāti, kam paredzēts strādāt organizācijā, tiek iepriekš pārbaudīti tiesību aktu robežās un samērīgi ar aizsardzības vajadzībām; jutīgām lomām pārbaudi atkārtoti arī nodarbinātības laikā.

Pēc kā to var atpazīt: Ja darbinieku nav, šo kontroles pasākumu var pamatot kā pašlaik nepiemērojamu, taču procedūra pieņemšanas darbā gadījumam tomēr ir jānosaka un jāieraksta piemērojamības paziņojumā kā plānota. Īstenojams tvērums: identitātes, dzīves apraksta un atsauksmju pārbaude, kā arī sertifikāti; sodāmības pārbaude tikai tad, ja to attaisno aizsardzības vajadzības un pieļauj tiesību akti. To pašu standartu no ārštata speciālistiem un līgumpartneriem prasa līgumos, citādi tieši tur veidojas robs.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.6.2 Nodarbinātības noteikumi: Līgumiskās vienošanās nosaka personāla un organizācijas informācijas drošības atbildības.

Pēc kā to var atpazīt: Drošības punkts darba vai pakalpojuma līgumā ar atsauci uz piemērojamām politikām. Ārštata speciālistiem tas pats punkts pakalpojuma līgumā, kā arī neizpaušanas līgums.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.6.3 Informācijas drošības izpratne, izglītošana un apmācība: Personāls un attiecīgās ārējās puses saņem atbilstošu izpratnes veidošanu un apmācību, kā arī regulārus organizācijas politiku aktualizējumus.

Pēc kā to var atpazīt: Ikgadēja apmācība ar dalības pierādījumu un datumu, papildināta ar pikšķerēšanas simulācijām un novērtētu klikšķu īpatnību. Arī pašnodarbinātajiem, kas strādā vieni, ir vajadzīgs pierādījums par pašu tālākizglītību, piemēram, kursu apliecinājumi.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.6.4 Disciplinārais process: Pastāv formāls un paziņots process darbībām pret cilvēkiem, kas ir pārkāpuši drošības politikas.

Pēc kā to var atpazīt: Ja darbinieku nav, to var pamatot kā pašlaik nepiemērojamu, taču process pieņemšanas darbā gadījumam tomēr ir jānosaka; zūd tikai tā piemērošana, nevis pats noteikums. Nepieciešama pakāpeniska, paziņota reakcija kārtība (saruna, aizrādījums, formāls brīdinājums, atļaušana) saskaņā ar darba tiesībām un darbinieku pārstāvības noteikumiem. Līgumpartneriem sankciju līmeni atspoguļo līgumā, piemēram, līgumsods vai tiesības izbeigt līgumu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.6.5 Atbildības pēc darba attiecību izbeigšanas vai maiņas: Drošības atbildības un pienākumi, kas paliek spēkā pēc darba attiecību izbeigšanas vai lomas maiņas, ir noteikti, tiek īstenoti un paziņoti attiecīgajiem cilvēkiem.

Pēc kā to var atpazīt: Aiziešanas kontrolsaraksts ar tiesību atcelšanu, aktīvu atdošanu, nodošanu un skaidru atgādinājumu par saglabātajiem konfidencialitātes pienākumiem. Vienkāršākais pierādījums ir parakstīts aiziešanas pārrunu ieraksts.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.6.6 Konfidencialitātes vai neizpaušanas līgumi: Ir noteikts, kurš paraksta konfidencialitātes līgumu. Saturs atbilst informācijas aizsardzības vajadzībām, līgumi ir parakstīti, uzglabāti un tiek regulāri pārskatīti, lai tie paliktu aktuāli.

Pēc kā to var atpazīt: Parakstīti konfidencialitātes līgumi darbiniekiem, ārštata speciālistiem, pakalpojumu sniedzējiem un praktiskajiem, ar spēkā palikšanas periodu. Pārskata tabula ar līgumslēdzēju, datumu un derīgumu padara kopumu auditējamu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.6.7 Attālinātais darbs: Drošības pasākumi ir ieviesti tur, kur cilvēki strādā ārpus organizācijas telpām un vienlaikus piekļūst organizācijas informācijai.

Pēc kā to var atpazīt: Mājas biroja un attālinātā darba politika ar prasībām par diska šifrēšanu, ekrāna bloķēšanu, drošu bezvadu tīklu, VPN vai nulles uzticēšanās piekļuves lietošanu, blakusskata aizsargiem un aizliegumu bez apstiprinājuma lietot personiskās ierīces. Pierādījums ar MDM atbilstības ziņojumu par galiekārtām.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.6.8 Ziņošana par informācijas drošības atgadījumiem: Pastāv mehānisms, ar kuru cilvēki var laikus ziņot par novērotiem vai iespējamajiem drošības atgadījumiem.

Pēc kā to var atpazīt: Skaidri paziņots ziņošanas kanāls (pastaste, tērēšanas kanāls, tālruņa numurs) ar apliecinājumu, ka par labticīgiem ziņojumiem sankciju nav. Pierādījums: ziņojumu apjoms atgadījumu reģistrā; pastāvīgi tukšs reģistrs auditā ir brīdinājuma zīme.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7 A pielikums: Fiziskie kontroles pasākumi

14

A.7.1 Fiziskās drošības perimetri: Drošības perimetri ir noteikti un tiek izmantoti, lai aizsargātu zonas, kurās atrodas informācija un informācijas apstrādes iekārtas.

Pēc kā to var atpazīt: Perimetru apraksts ar skici vai fotoattēliem: ēka, birojs, serveru skapis. Mājas birojā perimetrs ir aizslēdzama darba telpa vai, ja tādas nav, aizslēdzams skapis; to apraksta, nevis atstāj neminētu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.2 Fiziska iekļūšana: Drošās zonas ir aizsargātas ar atbilstošu iekļūšanas kontroli un piekļuves punktiem.

Pēc kā to var atpazīt: Atslēgu vai caurlaižu reģistrs ar izsniegšanu un atdošanu, kā arī apmeklētāju noteikums ar pavadīšanu un žurnālu. Ja izmanto koplietošanas biroju vai datu centru, par pierādījumu ņem operatora iekļūšanas kontroli un nostiprina to līgumā.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.3 Biroju, telpu un iekārtu nodrošināšana: Biroju, telpu un iekārtu fiziskā drošība ir izstrādāta un ieviesta.

Pēc kā to var atpazīt: Aizslēdzamas durvis, logu aizsardzība pirmajā stāvā, no ārpuses neredzami ekrāni ar konfidenciālu saturu, nekādu uzņēmuma izkārtnu pie jutīgām zonām. Par pierādījumu pietiek ar īsu aprakstu un fotoattēlu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.4 Fiziskās drošības uzraudzība: Telpas tiek nepārtraukti uzraudzītas, lai atklātu neatļautu fizisku piekļuvi.

Pēc kā to var atpazīt: Jauns 2022. gada izdevumā. Iespējas ir signalizācija, kustības detektori, videonovērošana vai iekļūšanas žurnāli. Videonovērošanas atbilstība datu aizsardzības prasībām ir jāpārbauda; mājas birojā pamatota alternatīva ir signalizācijas, aizslēgtas telpas un konstatējums, ka tur netiek turēti jutīgi serveri, apvienojums.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.5 Aizsardzība pret fiziskiem un vides apdraudējumiem: Pastāv aizsardzība pret fiziskiem un vides apdraudējumiem, piemēram, dabas katastrofām un tīšiem vai netīšiem bojājumiem.

Pēc kā to var atpazīt: Ugunsgrēka, ūdens, karstuma, elektroapgādes pārtraukuma un ielaušanās pārskatīšana kopā ar ieviestajiem pasākumiem (dūmu detektori, ugunsdzēsāmie aparāti, iekārtas ne zem ūdensvada caurulēm, rezerves kopija citā atrašanās vietā). Šeit pieslēdzas 4.1 konstatējums par klimata pārmaiņām.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.6 Darbs drošās zonās: Pasākumi darbam drošās zonās ir izstrādāti un ieviesti.

Pēc kā to var atpazīt: Noteikumi serveru telpai vai augstas konfidencialitātes zonām: nekādas nepieskatītas trešo pušu piekļuves, nekādas ierakstīšanas ar kamerām vai mobilajām ierīcēm, veikta darba žurnālēšana. Ja drošu zonu nav, to var pamatot ar atsauci uz darbību tikai mākonī.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.7 Tīra galda un tīra ekrāna princips: Noteikumi par tīru galdu attiecībā uz papīriem un noņemamiem datu nesējiem un par bloķētiem ekrāniem ir noteikti un tiek ievēroti.

Pēc kā to var atpazīt: Tas pilnībā attiecas arī uz mājas biroju, tāpēc to nedrīkst atzīt par nepiemērojamu. Apliecināms ar īsu noteikumu (dokumentus noglabāt, ekrāna bloķēšana pēc piecām minūtēm, nekādu līmlapiņu ar piekļuves datiem) un tehniski uzspiestu bloķēšanu ar ierīču politiku, kuras konfigurāciju var eksportēt.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.8 Iekārtu izvietošana un aizsardzība: Iekārtas ir izvietotas droši un aizsargātas.

Pēc kā to var atpazīt: Izvietojums prom no gaiteniem un publiskām zonām, bez ieskata no ārpuses, aizsardzība pret karstumu un mitrumu, kabeļa slēdzenes mobilajām ierīcēm. Pietiek ar īsu aprakstu mājas biroja vai biroja politikā.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.9 Aktīvu drošība ārpus telpām: Aktīvi, kas atrodas ārpus telpām, ir aizsargāti.

Pēc kā to var atpazīt: Mazos uzņēmumos tas galvenokārt ir klēpjdators, viedtālrunis un ārējie datu nesēji, un no tā nevar izvairīties ar pamatojumu. Pierādījums: uzspiesta diska šifrēšana, ar MDM iespējota attālināta dzēšana, noteikums neatstāt ierīces transportlīdzekļos un nelietot publiskos tīklus bez VPN, kā arī nozaudēšanas ziņošanas ceļš. MDM atbilstības ziņojums ar šifrēšanas statusu katrai ierīcei ir stabilākais atsevišķais pierādījums.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.10 Datu nesēji: Datu nesēji tiek pārvaldīti visā to dzīves ciklā saskaņā ar klasifikācijas shēmu un rīcības prasībām, no iegādes caur lietošanu un pārvadāšanu līdz iznīcināšanai.

Pēc kā to var atpazīt: Tas attiecas arī uz tīri mobilu darbu, jo USB atmiņas, ārējie diski un rezerves kopiju nesēji pastāv. Pierādījums: datu nesēju reģistrs, šifrēti nesēji, tehniski uzspiests aizliegums lietot neapstiprinātus noņemamus nesējus, droša glabāšana aizslēdzamā vietā un nodošana A.7.14 dzīves cikla beigās.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.11 Atbalsta komunālie pakalpojumi: Informācijas apstrādes iekārtas ir aizsargātas pret atbalsta komunālo pakalpojumu, jo īpaši elektroapgādes, atteici.

Pēc kā to var atpazīt: Ja serverus uztur uz vietas, nepārtrauktās barošanas avots ar dokumentētu pārbaudi. Ja darbība notiek tikai mākonī, pierādījums ir atsauce uz pakalpojuma sniedzēja saistībām un noteikums, kā turpināt darbu vietēja elektroapgādes vai interneta pārtraukuma laikā (mobīlā piesaiste, rezerves atrašanās vieta).

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.12 Kabeļu drošība: Elektroapgādes, datu un sakaru kabeļi ir aizsargāti pret pārtveršanu, traucējumiem un bojājumiem.

Pēc kā to var atpazīt: Ja kabeļi ir pašu īpašumā, aizsardzība pret bojājumiem un pret neatļautu piekļuvi komutācijas paneļiem. Mazos birojos un mājas birojos pamatojums ir īss, taču tas ir jāsniedz: maršrutētājs un tīkla rozetes nav publiski pieejamas, neizmanto tie portu ir atslēgti.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.13 Iekārtu uzturēšana: Iekārtas tiek pareizi uzturētas, lai nodrošinātu informācijas pieejamību, integritāti un konfidencialitāti.

Pēc kā to var atpazīt: Uzturēšanas plāns vai ražotāja atbalsta statuss katrai ierīcei un noteikums remontam, ko veic trešās puses (vispirms izņemt datu nesēju vai dzēst datus un noslēgt konfidencialitātes līgumu ar pakalpojuma sniedzēju). Atbalsta beigu datumam seko līdzīgi aktīvu uzskaitē.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7.14 Droša iekārtu iznīcināšana vai atkārtota lietošana: Pirms ierīci, kurā ir datu nesējs, nodod tālāk, pārdod vai utilizē, ir jāpārbauda un jāreģistrē, ka uz tās vairs nevar atjaunot ne aizsargātus datus, ne licencētu programmatūru.

Pēc kā to var atpazīt: Tas attiecas arī uz mājas biroju un uz izņemtajām personiskajām ierīcēm, kas tika lietotas darbam. Pierādījums: dzēšanas ieraksts katrai ierīcei ar sērijas numuru, datumu un metodi (kriptogrāfiska dzēšana šifrētiem SSD, pārrakstīšana, fiziska iznīcināšana) vai pakalpojuma sniedzēja iznīcināšanas apliecība. Šifrētām ierīcēm pietiek ar dokumentētu atslēgas iznīcināšanu, ja procedūra ir aprakstīta.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8 A pielikums: Tehnoloģiskie kontroles pasākumi

34

A.8.1 Lietotāju galiekārtas: Informācija, kas ir uzglabāta galiekārtās, tiek tajās apstrādāta vai ir caur tām pieejama, ir aizsargāta.

Pēc kā to var atpazīt: Nostiprināšanas bāzlīnija katrai operētājsistēmai, centrāla pārvaldība ar MDM, diska šifrēšana, automātiski atjauninājumi un ekrāna bloķēšana. MDM atbilstības ziņojums ar statusu katrai ierīcei apliecina to visu uzreiz.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.2 Privileģētās piekļuves tiesības: Privileģētās piekļuves tiesību piešķiršana un lietošana ir ierobežota un pārvaldīta.

Pēc kā to var atpazīt: Visu administratora kontu saraksts ar pamatojumu, atsevišķi administratora konti, ko nelieto ikdienas darbam, uzspiesta MFA, laikā ierobežota tiesību paaugstināšana, kur tas iespējams, un periodiska pārskatīšana. Mazos uzņēmumos tas ir svarīgākais kompensējošais kontroles pasākums A.5.3.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.3 Piekļuves ierobežošana informācijai: Piekļuve informācijai un citiem saistītajiem aktīviem ir ierobežota saskaņā ar noteikto piekļuves pārvaldības politiku.

Pēc kā to var atpazīt: Pilnvarojumu koncepcija, kas balstās uz lomām un grupām, nevis uz atsevišķiem piešķirumiem, apliecināta ar grupu dalības eksportu. Publiskās koplietošanas saites mākoņa krātuvē regulāri pārskata un ļauj tām beigties.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.4 Piekļuve pirmkodam: Lasīšanas un rakstīšanas piekļuve pirmkodam, izstrādes rīkiem un programmatūras bibliotēkām ir atbilstoši pārvaldīta.

Pēc kā to var atpazīt: Repozitorija tiesības pēc lomām, aizsargāti galvenie zari, uzspiestas pārskatīšanas vai uzspiestas statusa pārbaudes, nekādas tiešas ierakstīšanas galvenajā zarā. Pierādījums ar zaru aizsardzības konfigurāciju un organizācijas dalībnieku sarakstu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.5 Droša autentifikācija: Drošas autentifikācijas tehnoloģijas un procedūras ir ieviestas, pamatojoties uz piekļuves ierobežojumiem un tematisko politiku.

Pēc kā to var atpazīt: MFA visai ārējai piekļuvei un visiem administratora kontiem, pret pikšķerēšanu noturīgas metodes (piekļuves atslēgas, FIDO2), kur tas iespējams, un bloķēšana pēc neveiksmīgiem mēģinājumiem. Pierādījums ar identitātes pakalpojuma sniedzēja MFA pārklājuma ziņojumu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.6 Jaudas pārvaldība: Krātuve, skaitļošana, joslas platums un licences tiek uzraudzītas, un pieprasījumu pielāgo pietiekami savlaicīgi, lai sastrēgumi nekad neapdraudētu pieejamību.

Pēc kā to var atpazīt: Krātuves, skaitļošanas slodzes, licenču kvotu un mākoņa budžetu uzraudzība ar sliekšņa trauksmēm. Mazos uzņēmumos pietiek ar trauksmi par diska aizpildījumu un izmaksu robežām un ikgadēju jaudas apskatu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.7 Aizsardzība pret ļaunatūru: Tehniskā aizsardzība pret ļaunatūru ir aktīva un aktuāla, un cilvēki, kas lieto ierīces, ir pietiekami apmācīti, lai šo aizsardzību nepadarītu neefektīvu.

Pēc kā to var atpazīt: Aktīva galiekārtu aizsardzība ar centrālu statusa pārskatu, pasta filtrs, kas pārbauda pielikumus un saites, un noteikums, kas aizliedz izpildīt neapstiprinātu programmatūru. Tiešais pierādījums ir aizsardzības risinājuma statusa ziņojums ar datumu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.8 Tehnisko ievainojamību pārvaldība: Organizācija aktīvi uzzina par ievainojamībām izmantotajās tehnoloģijās, katram konstatējumam izlemj, cik lielā mērā organizācija ir apdraudēta, un novērš robu noteiktajos termiņos vai pamato citu rīcību.

Pēc kā to var atpazīt: Ievainojamību pārvaldība ar avotu (skeneris, atkarību pārbaude CI, ražotāju brīdinājumi), smaguma vērtējumu un noteiktiem termiņiem katram līmenim, piemēram, kritiskās 7 dienu laikā. Pierādījums: skenēšanas ziņojumi no vairākiem laika punktiem, kas parāda atvērto konstatējumu samazināšanos.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.9 Konfigurācijas pārvaldība: Aparatūras, programmatūras, pakalpojumu un tīklu konfigurācijas, tostarp drošības konfigurācijas, ir noteiktas, dokumentētas, ieviestas, tiek uzraudzītas un pārskatītas.

Pēc kā to var atpazīt: Jauns 2022. gada izdevumā. Pierādījums ar dokumentētām bāzlinijas konfigurācijām (nostiprināšanas bāzlinijas) un to uzspiešanu, vēlams kā infrastruktūra koda veidā versiju kontrolē vai ar MDM profiliem. Noviržu atklāšana un periodisks konfigurāciju salīdzinājums to papildina.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.10 Informācijas dzēšana: Informācija, kas glabājas informācijas sistēmās, ierīcēs un datu nesējos, tiek dzēsta, tiklīdz tā vairs nav vajadzīga.

Pēc kā to var atpazīt: Jauns 2022. gada izdevumā un cieši saistīts ar GDPR. Pierādījums ar dzēšanas koncepciju, kurā ir glabāšanas termiņi katrai datu kategorijai, ar tehniski ieviestām glabāšanas politikām mākoņpakalpojumos un datubāzēs un ar dzēšanas žurnāliem. Arī rezerves kopijām un žurnālu arhīviem ir vajadzīgs glabāšanas termiņš.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.11 Datu maskēšana: Datu maskēšanu piemēro saskaņā ar tematisko piekļuves pārvaldības politiku un ar darbības un tiesību aktu prasībām.

Pēc kā to var atpazīt: Jauns 2022. gada izdevumā. Praksē: nekādu ražošanas datu testa un izstrādes vidēs, bet gan anonimizēti vai sintētiski dati; pseidonimizācija analītikā; kontu numuru un piekļuves datu maskēšana žurnālos un atbalsta saskarnēs. Pierādījums ar skriptu vai procedūru, kas ģenerē testa datus.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.12 Datu noplūdes novēršana: Datu noplūdes novēršanas pasākumi tiek piemēroti sistēmās, tīklos un ierīcēs, kas apstrādā, glabā vai pārraida jutīgu informāciju.

Pēc kā to var atpazīt: Jauns 2022. gada izdevumā. Mazos uzņēmumos reālistiski: koplietošanas saišu kontrole mākoņa krātuvē, neapstiprinātu noņemamu datu nesēju bloķēšana, noteikumi pret pārsūtīšanu uz privātām pastkastēm, konfidencialu datu ievades ārējos mākslīgā intelekta pakalpojumos pārbaude un noslēpumu skenēšana pirmkodā. Pierādījums ar konfigurāciju un ar atradumu pārskatīšanu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.13 Informācijas rezerves kopijas: Datu, programmatūras un sistēmu rezerves kopijas pastāv saskaņā ar noteiktu kārtību (tvērums, biežums, glabāšana, atrašanās vieta), un atjaunošanu no tām regulāri arī tiešām pārbauda.

Pēc kā to var atpazīt: Rezerves kopiju politika ar biežumu, glabāšanas termiņu un kopiju citā vietā pēc 3-2-1 principa, rezerves kopiju šifrēšana un aizsardzība pret pārrakstīšanu ar izspiedējprogrammatūru (nemaināmas rezerves kopijas). Izšķiroša ir dokumentēta atjaunošanas pārbaude ar datumu un rezultātu, jo nepārbaudīta rezerves kopija auditā skaitās neesoša.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.14 Informācijas apstrādes iekārtu redundance: Informācijas apstrādes iekārtas ir ieviestas ar pietiekamu redundanci, lai izpildītu pieejamības prasības.

Pēc kā to var atpazīt: Redundancei ir jāatbilst pieejamības mērķiem, nevis maksimāli iespējamajam. Pierādījums ar arhitektūras aprakstu, kurā ir redundantas instances vai zonas, rezerves ierīces un pamatots lēmums par to, kur redundances apzināti nav.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.15 Žurnālēšana: Drošībai būtiskās darbības atstāj pēdas. Žurnāli tiek veidoti, saglabāti, aizsargāti pret izmaiņām un arī tiešām analizēti, nevis tikai vākti.

Pēc kā to var atpazīt: Vismaz žurnālē pieteikšanās un neveiksmīgu mēģinājumus, tiesību izmaiņas, administratīvās darbības un piekļuvi konfidencialiem datiem. Žurnāli ir aizsargāti pret izmaiņām, un tiem ir noteikts glabāšanas termiņš; mazos uzņēmumos nemaināmi žurnāli vienlaikus kompensē trūkstošo pienākumu nodalīšanu A.5.3.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.16 Uzraudzības darbības: Tīklus, sistēmas un lietotnes uzrauga, lai atklātu neparastu uzvedību, un veic atbilstošas darbības iespējamo drošības notikumu novērtēšanai.

Pēc kā to var atpazīt: Jauns 2022. gada izdevumā. Īstenojams arī bez pašu drošības komandas: identitātes pakalpojuma sniedzēja trauksmes par neiespējamu ceļošanu un neveiksmīgu mēģinājumu virknēm, mākoņa platformas trauksmes par neparastiem izdevumiem vai tiesību izmaiņām, pārsūtītas uz uzraudzītu pastkasti ar noteiktu reaģēšanas laiku. Pierādījums ar trauksmes noteikumiem un apstrādāto trauksmju piemēriem.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.17 Pulksteņu sinhronizācija: Visas sistēmas, kas raksta žurnālus, ņem laiku no noteikta uzticama avota, lai atgadījumus varētu sakārtot pareizā secībā starp sistēmām.

Pēc kā to var atpazīt: NTP konfigurācija serveros un galiekārtās un vienota laika josla žurnālos (vēlams UTC). Bez sinhronizēta laika notikuma rekonstrukcija saskaņā ar A.5.28 nav noturīga; par pierādījumu pietiek ar konfigurācijas izrakstu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.18 Privileģētu utilitārogrammu lietošana: Tādu utilitārogrammu lietošana, kas var apiet sistēmas aizsardzību, ir ierobežota un cieši kontrolēta.

Pēc kā to var atpazīt: Apstiprināto administrēšanas rīku saraksts, vietējo administratora tiesību ierobežošana, lietotņu kontrole (atļauto saraksts), kur tas iespējams, un lietošanas žurnālēšana. Pierādījums: politika un tiesību pārvaldības konfigurācija.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.19 Programmatūras uzstādīšana ekspluatācijā esošās sistēmās: Procedūras un pasākumi drošai programmatūras uzstādīšanas pārvaldībai ekspluatācijā esošās sistēmās ir ieviesti.

Pēc kā to var atpazīt: Tikai apstiprināta programmatūra no uzticamiem avotiem, uzstādīšana ar centrālu izplatīšanu vai pakotņu pārvaldnieku, atgriešanās ceļš un iepriekšējās versijas saglabāšana. Pierādījums ar apstiprinājumu sarakstu un izvietojuma žurnāliem.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.20 Tīklu drošība: Tīkliem un aktīvajām tīkla ierīcēm ir nosaukts īpašnieks, nostiprināta konfigurācija un izsekojams noteikumu kopums, kas nosaka, kāda datu plūsma vispār ir atļauta.

Pēc kā to var atpazīt: Ugunsgrāvis noteikumu kopums pēc principa aizliegts pēc noklusējuma, dokumentēti atvērtie porti ar pamatojumu, droša bezvadu tīkla konfigurācija un nomainīti noklusējuma piekļuves dati tīkla ierīcēs. Pierādījums ar noteikumu kopuma eksportu un ārēju portu skenēšanu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.21 Tīkla pakalpojumu drošība: Tīkla pakalpojumu drošības mehānismi, pakalpojumu līmeņi un pārvaldības prasības ir apzinātas, ieviestas un tiek uzraudzītas.

Pēc kā to var atpazīt: Katram izmantotajam tīkla pakalpojumam (VPN, DNS, pasts, CDN) dokumentē drošības saistības un pašu konfigurāciju, tostarp šifrēšanu pārraides laikā un pakalpojuma sniedzēja pakalpojumu līmeņa saistības. Pierādījums: konfigurācijas pārskats un līgums vai pakalpojuma apraksts.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.22 Tīklu nodalīšana: Tīkls ir sadalīts zonās tā, ka pakalpojumi, lietotāju grupas un sistēmas ar atšķirīgām aizsardzības vajadzībām nevar sasniegt cita citu bez filtrēšanas.

Pēc kā to var atpazīt: Atsevišķi tīkla segmenti vai VLAN viesiem, administrēšanai un ražošanai; mākonī atsevišķi konti vai virtuālie tīkli ar drošības grupām. Mājas birojā īstenojams risinājums ir atsevišķs tīkls vai VLAN darba ierīcēm, nodalīts no personiskajām ierīcēm un viedās mājas tehnikas.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.23 Tīmekļa filtrēšana: Piekļūvi ārējām tīmekļa vietnēm pārvalda, lai samazinātu saskari ar ļaunprātīgu saturu.

Pēc kā to var atpazīt: Jauns 2022. gada izdevumā. Sasniedzams ar nelielu piepūli, izmantojot filtrējošu DNS pakalpojumu vai galiekārtu aizsardzībā iekļauto tīmekļa filtrēšanu, ar bloķētām kategorijām un bloķēto pieprasījumu žurnālēšanu. Pierādījums ar filtra konfigurāciju un ziņojuma izrakstu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.24 Kriptogrāfijas lietošana: Ir saistoši noteikts, kur šifrēšanu piemēro, ar kādiem algoritmiem un kā atslēgas visā to dzīves ciklā ģenerē, glabā, nomaina un iznīcina.[Dokuments](#)

Pēc kā to var atpazīt: Kriptogrāfijas politika ar apstiprinātiem algoritmiem un minimālajiem atslēgu garumiem, šifrēšana pārraides laikā (TLS) un glabāšanā, kā arī atslēgu pārvaldības procedūra, kas aptver ģenerēšanu, glabāšanu, nomaiņu un iznīcināšanu. Pierādījums ar politiku un atslēgu pakalpojuma vai glabāšanas konfigurāciju.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.25 Drošas izstrādes dzīves cikls: Noteikumi drošai programmatūras un sistēmu izstrādei ir izveidoti un tiek piemēroti.

Pēc kā to var atpazīt: Izstrādes procesa apraksts ar drošības saskarpunktiem katrā posmā: prasības, projektēšana, ieviešana, testēšana, laidieni, darbība. Mazām komandām pietiek ar vienu lappusi, kas atsaucas uz konkrētajiem CI vārtiem un pārskatīšanas pienākumu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.26 Lietotņu drošības prasības: Lietotņu drošības prasības ir apzinātas, specificētas un apstiprinātas izstrādes un iegādes laikā.

Pēc kā to var atpazīt: Drošības prasības kā skaidri punkti prasību sarakstā vai kā atkārtoti lietojams kontrolsaraksts, orientēts, piemēram, uz izplatītiem lietotņu drošības verifikācijas standartiem. Pierādījums ar pieteikumiem vai prasību dokumentiem, kuros ir drošības aspekts.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.27 Droša sistēmu arhitektūra un projektēšanas principi: Drošas sistēmu projektēšanas principi ir izveidoti, dokumentēti un tiek piemēroti izstrādes darbībās.

Pēc kā to var atpazīt: Dokumentēti principi, piemēram, mazākās nepieciešamās tiesības, aizsardzība vairākos slāņos, drošas noklusējuma vērtības, datu minimizēšana un nulles uzticēšanās pieeja, kopā ar redzamu to piemērošanu arhitektūras skicēs vai lēmumu ierakstos.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.28 Droša kodēšana: Drošas kodēšanas principi tiek piemēroti programmatūras izstrādē.

Pēc kā to var atpazīt: Jauns 2022. gada izdevumā. Pierādījums ar saistošiem kodēšanas noteikumiem, statistiku koda analīzi un noslēpumu skenēšanu kā obligātiem CI vārtiem, pārbaudītu bibliotēku lietošanu un dokumentētām koda pārskatīšanām. Kur pienākumu nodalīšana nav iespējama, četru acu principa vietu ieņem uzspiesti automatizēti vārti; to pamato un apliecina ar konveijera konfigurāciju.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.29 Drošības testēšana izstrādē un pieņemšanā: Drošības testēšanas procesi ir noteikti un ieviesti izstrādes dzīves ciklā.

Pēc kā to var atpazīt: Automatizēti drošības testi konveijerā (atkarību pārbaudes, statistiska un dinamiska analīze) un periodisks ielaušanās tests, kur aizsardzības vajadzības ir paaugstinātas. Pierādījums ar testu ziņojumiem, kuriem ir datums, un ar konstatējumu izsekošanu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.30 Ārpakalpojumā nodota izstrāde: Ārpakalpojumā nodotās izstrādes darbības tiek vadītas, uzraudzītas un pārskatītas.

Pēc kā to var atpazīt: Ja izstrādi nodod ārpakalpojumā, drošības prasības nosaka līgumā, nostiprina koda īpašumtiesības un pārskatīšanas tiesības un pirms pieņemšanas veic koda pārskatīšanas un drošības testus. Ja ārpakalpojumā nodotas izstrādes nav, nepiemērojamība ir saskanīgi jāpamato SoA.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.31 Izstrādes, testa un ražošanas vižu nodalīšana: Izstrādes, testa un ražošanas vides ir nodalītas un aizsargātas.

Pēc kā to var atpazīt: Atsevišķi konti, projekti vai nosaukumtelpas, atsevišķi piekļuves dati un atsevišķas datu kopas. Kopā ar A.8.11 nodrošina, ka ražošanas dati nenonāk vidēs ārpus ražošanas. Pierādījums ar vižu pārskatu un tiesību piešķirumu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.32 Izmaiņu pārvaldība: Informācijas apstrādes iekārtu un informācijas sistēmu izmaiņām piemēro izmaiņu pārvaldības procedūras.

Pēc kā to var atpazīt: Izmaiņu process ar pieprasījumu, ietekmes novērtējumu, testēšanu, apstiprinājumu, ieviešanu un atgriešanās ceļu. Izstrādes komandās šo punktu izpilda izmaiņu pieprasījumu konveijers ar uzspiestām pārbaudēm un žurnālētām izvietošanām, ja vēsture ir nemaināma.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.33 Testa informācija: Testa informācija ir atbilstoši izraudzīta, aizsargāta un pārvaldīta.

Pēc kā to var atpazīt: Princips: nekādu īstu personas datu testa sistēmās. Kur no tā nevar izvairīties, dokumentē apstiprinājumu, maskēšanu, piekļuves ierobežojumu un dzēšanu pēc testa. Pierādījums ar testa datu koncepciju un dzēšanas žurnāliem.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8.34 Informācijas sistēmu aizsardzība audita testēšanas laikā: Audita testi, kas ietver piekļuvi ekspluatācijā esošām sistēmām, ir plānoti un saskaņoti ar vadību, lai izvairītos no darbības traucējumiem.

Pēc kā to var atpazīt: Audita vienošanās ar laika logu, tvērumu, tikai lasīšanas piekļuvi, kur tas iespējams, audita piekļuves žurnālēšanu un vadības apstiprinājumu. Tas attiecas arī uz ielaušanās testiem: pierādījums ir rakstiska testa atļauja ar laika logu un ārkārtas kontaktpersonu.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

ISO/IEC 27018:2025, Informācijas drošība, kiberdrošība un privātuma aizsardzība: vadlīnijas personas datu (PII) aizsardzībai publiskajos mākoņos, kas darbojas kā PII apstrādātāji (3. izdevums, 2025-08)

Personas datu aizsardzība publiskajā mākonī

36 prasības. Šim standartam nav akreditēta sertifikāta. Redakcija 07/2026.

ISO/IEC 27018 nav pārvaldības sistēmas standarts, bet vadlīniju kopums ar paplašinātiem kontroles pasākumiem papildus ISO/IEC 27002:2022. Atsevišķa akreditēta sertifikāta par atbilstību ISO/IEC 27018 nav. Kontroles pasākumus iekļauj ISO/IEC 27001 sistēmas piemērojamības paziņojumā, un sertifikātu pēc tam izsniedz par atbilstību ISO/IEC 27001 ar atsauci uz ISO/IEC 27018. Standarts ir vērsts uz publiska mākoņpakalpojuma piegādātāju, kas apstrādā personas datus savu mākoņpakalpojuma klientu uzdevumā. Organizācija, kas mākoņpakalpojumus tikai izmanto, šo lomu neuzņemas, un tai ir lietderīgi novērtēt prasības attiecībā uz saviem piegādātājiem, nevis attiecībā uz sevi pašu. Leanshift gadījumā šis saraksts tāpēc galvenokārt ir piegādātāju novērtēšanas shēma. Katru punktu var uzdot piegādātājam kā jautājumu un nostiprināt datu apstrādes līgumā saskaņā ar GDPR 28. pantu. Šāda novērtējuma rezultāts ir iekšējs atbilstības ieraksts vai piegādātāja novērtējuma profils, nevis sertifikāts. Par numerāciju: nodaļas no A.2 līdz A.12 seko standarta A pielikuma privātuma principiem, bet punkti ar numuru, piemēram, A.11.6, ir tur uzskaitītie papildu kontroles pasākumi. Punkti ar numuru, piemēram, 8.10 vai 5.34, attiecas uz ISO/IEC 27002:2022 kontroles pasākumiem, kurus standarts precīzē mākoņa videi. Punkti ar apzīmējumu (Grundsatz), kas nozīmē principu, ir atvasināti no pašas nodaļas principa tur, kur A pielikumā nav atsevišķa papildu kontroles pasākuma.

Uzņēmums	Datums	Aizpildīja

A.2 Piekrišana un izvēle2

A.2.1 Mākoņpakalpojuma piegādātājs atbalsta mākoņpakalpojuma klientu datu subjektu tiesību izpildē, tostarp piekļuves, labošanas, dzēšanas un iebilduma tiesību izpildē. Atbildība un termiņi ir noteikti līgumā.

Dokuments

Pēc kā to var atpazīt: Pierādījums ir datu apstrādes līgums saskaņā ar GDPR 28. pantu ar klauzulu par atbalstu datu subjektu tiesību izpildē, kopā ar tehniskajiem līdzekļiem pašā pakalpojumā: eksporta, labošanas un dzēšanas funkcijām vai dokumentētu atbalsta procedūru ar atbildes termiņu. Jautājums piegādātājam: kāda funkcija vai process ir pieejams, lai piekļuves vai dzēšanas pieprasījumu varētu izpildīt viena mēneša laikā?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.2 (Grundsatz) Mākoņpakalpojuma klientu personas datus apstrādā tikai saskaņā ar klienta dokumentētiem norādījumiem. Datu subjektu piekrišanas iegūšana paliek klienta kā pārziņa uzdevums, un piegādātājs to nepārņem.

Pēc kā to var atpazīt: Pierādījums ir norādījumu klauzula datu apstrādes līgumā un apliecinājums, ka piegādātājs datus sekundāri neizmanto, piemēram, pakalpojuma privātuma paziņojums un produkta dokumentācija. Jautājums piegādātājam: vai mūsu klientu dati kaut kādā veidā tiek apstrādāti ārpus mūsu norādījumiem, piemēram, produkta uzlabošanai vai modeļu apmācībai?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.3 Nolūka leģitimitāte un noteikšana2

A.3.1 Nolūks, kādā piegādātājs apstrādā personas datus, aprobežojas ar nolīgta pakalpojuma sniegšanu un ir nosaukts līgumā. Apstrāde piegādātāja paša nolūkiem nenotiek.

Dokuments

Pēc kā to var atpazīt: Pierādījums ir datu apstrādes līgums, kurā norādīts apstrādes priekšmets, raksturs, nolūks un ilgums, kā arī datu subjektu kategorijas saskaņā ar GDPR 28. panta 3. punktu. Jautājums piegādātājam: lūgums iesniegt līguma pielikumu, kurā apstrādes nolūks aprakstīts izsmeljoši. Mazam uzņēmumam pietiek ar piegādātāja standarta datu apstrādes pielikumu, ja tajā ir šī informācija.

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.3.2 **Piegādātājam uzticētos personas datus bez iepriekšējas skaidras piekrišanas neizmanto reklāmai, mārketingam vai citiem piegādātāja komerciāliem nolūkiem. Pakalpojuma sniegšana nav atkarīga no šādas piekrišanas.**

Pēc kā to var atpazīt: Pierādījums ir skaidra līguma klauzula, kas izslēdz komerciālu sekundāro izmantošanu, kopā ar pakalpojuma lietošanas noteikumiem. Jautājums piegādātājam: rakstisks apliecinājums, ka klientu dati netiek izmantoti reklāmai, profilēšanai vai mākslīgā intelekta modeļu apmācībai. Ja šādas apņemšanās nav, pakalpojums personas datiem nav piemērots.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.4 Vākšanas ierobežošana

1

A.4 (Grund) **Papildus datiem, ko klients ievada pakalpojumā, piegādātājs savām vajadzībām nevāc citus personas datus, tostarp telemetriju, lietošanas profilus vai satura analīzi. Darbības dati un metadati, kas tiek vākti, ir nosaukti un pamatoti.**

Pēc kā to var atpazīt: Pierādījums ir saraksts ar datiem, kurus pakalpojums reģistrē papildus satura datiem (piekļuves žurnāli, telemetrija, diagnostikas dati), ar nolūku un glabāšanas termiņu, kā arī ekrānu uzņēmums ar iestatījumu, kas izslēdz izvēles telemetriju. Jautājums piegādātājam: kādi lietošanas, telemetrijas un diagnostikas dati tiek vākti papildus, kādam nolūkam tie tiek izmantoti un vai vākšanu var izslēgt?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.5 Datu minimizēšana

2

A.5.1 **Pagaidu faili, kas rodas personas datu apstrādes laikā, tostarp pagaidu krātuve, kešatmiņa vai atcelšanas žurnāli, tiek droši dzēsti noteiktā termiņā.**

Pēc kā to var atpazīt: Pierādījums ir darbības vai dzēšanas procedūra ar noteiktu pagaidu datu glabāšanas termiņu, ko apstiprina sistēmas konfigurācija, piemēram, kešatmiņas TTL vai plānots tīrīšanas uzdevums ar tā izpildes žurnālu. Jautājums piegādātājam: pēc kāda termiņa tiek dzēsta kešatmiņa, pagaidu faili un starpstāvokļi, un kā to uzrauga?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

8.11 **Visur, kur darbībai, testēšanai vai atbalstam nav nepieciešami reāli dati, personas dati ir maskēti, pseidonimizēti vai anonimizēti. Apstrādāto datu apjoms paliek ierobežots līdz tam, kas pakalpojumam patiešām nepieciešams.**

Pēc kā to var atpazīt: Pierādījums ir noteikums par to, kurās vidēs drīkst būt reāli dati, kā arī ekrānu uzņēmumi vai skripti par maskēšanu, ko izmanto testa un izstrādes sistēmās. Jautājums piegādātājam: vai atbalsta un izstrādes komandas strādā ar produkcijas vides datiem, un ja jā, ar kādiem aizsardzības pasākumiem? Mazam uzņēmumam pietiek ar noteikumu, ka testa sistēmas darbojas tikai ar ģenerētiem paraugdatiem.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.6 Izmantošanas, glabāšanas un izpaušanas ierobežošana

3

A.6.1 **Ja piegādātājs saņem juridiski saistošu pieprasījumu izpaust personas datus, piemēram, no valsts iestādes, tas iepriekš informē mākonpakalpojuma klientu, ciktāl to atļauj tiesību akti.**

Pēc kā to var atpazīt: Pierādījums ir līgumiska paziņošanas klauzula un iekšējs process iestāžu pieprasījumiem ar nosauktu atbildīgo. Jautājums piegādātājam: vai pirms datu nodošanas tiek nosūtīts paziņojums, un vai tiek publicēts pārredzamības ziņojums par iestāžu pieprasījumiem? Aktuāls pārredzamības ziņojums ir spēcīgs pierādījums.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.6.2 Ja piegādātājs izpauž personas datus trešām personām, tas notikumu reģistrē izsekojami: kas datus saņēma, kad tas notika, kuri dati bija iesaistīti un uz kāda pamata izpaušana balstās.

[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir izpaušanas reģistrs vai pieteikumu vēsture ar šiem laukiem, arī tad, ja tajā nav neviena ieraksta. Tukšs, bet uzturēts reģistrs ir pieņemams un ir praktiskais ceļš mazam uzņēmumam. Jautājums piegādātājam: vai tiek uzturēts datu izpaušanas reģistrs un vai no tā var saņemt izrakstus?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

8.10 Personas datus dzēš, tiklīdz beidzas līgumā noteiktais glabāšanas termiņš vai līgums, tostarp kopijas rezerves kopijās pēc to rotācijas cikla.

Pēc kā to var atpazīt: Pierādījums ir dzēšanas koncepcija ar glabāšanas termiņiem katrai datu kategorijai, rezerves kopiju glabāšanas termiņš un dzēšanas žurnāls vai dzēšanas apliecinājums. Jautājums piegādātājam: cik ilgi mūsu dati saglabājas rezerves kopijās pēc līguma izbeigšanas, un vai par to dzēšanu tiek izsniegts rakstisks apliecinājums?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.7 Precizitāte un kvalitāte

2

A.7 (Grunds) Piegādātājs pēc savas iniciatīvas negroza tam uzticētos personas datus. Labojumus un atjauninājumus veic vienīgi pēc mākoņpakalpojuma klienta norādījuma vai ar funkcijām, ko klients izmanto pats.

Pēc kā to var atpazīt: Pierādījums ir pakalpojuma rediģēšanas funkcijas kopā ar to izmaiņu vēsturi, kā arī norādījumu klauzula datu apstrādes līgumā. Jautājums piegādātājam: vai ierakstus var labot pašu spēkiem, un vai katra izmaiņa tiek žurnālēta izsekojami?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

8.13 Personas datu integritāte ir aizsargāta glabāšanā, pārraidē un atjaunošanā. Rezerves kopijas pastāv, un to atjaunojamība ir pārbaudīta.

Pēc kā to var atpazīt: Pierādījums ir rezerves kopiju konfigurācija, kontrolsummu vai integritātes mehānismi un vismaz viena dokumentēta atjaunošanas pārbaude gadā ar datumu un rezultātu. Jautājums piegādātājam: cik bieži tiek pārbaudīta atjaunošana un kāds atjaunošanas laiks ir noteikts pakalpojuma līmeņa līgumā?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8 Atklātība, pārredzamība un informēšana

2

A.8.1 Apakšuzņēmēju izmantošana personas datu apstrādē ir atklāta pirms līguma noslēgšanas. Par saraksta izmaiņām klientam paziņo savlaicīgi, lai klients varētu iebilst vai izbeigt līgumu.

[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir aktuāls apakšapstrādātāju saraksts, publicēts vai darīts pieejams līgumiski, ar nosaukumu, valsti un apstrādes nolūku, kā arī paziņošanas noteikums saskaņā ar GDPR 28. panta 2. punktu. Jautājums piegādātājam: kur ir atrodams apakšapstrādātāju saraksts, cik ilgu laiku iepriekš tiek paziņots par izmaiņām un kā var iebilst?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.8 (Grunds) Pirms līguma noslēgšanas piegādātājs dara pieejamu saprotamu informāciju par to, kā personas dati tiek apstrādāti, kādi aizsardzības pasākumi pastāv un kurās jurisdikcijās apstrāde notiek.

Pēc kā to var atpazīt: Pierādījums ir privātuma paziņojums, drošības apraksts, uzticības centra lapa un datu apstrādes līgums kopā ar tehniskajiem un organizatoriskajiem pasākumiem pielikumā. Jautājums piegādātājam: lūgums iesniegt aktuālo tehnisko un organizatorisko pasākumu sarakstu kā līguma pielikumu, nevis tikai mārketinga materiālu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.9 Personas līdzdalība un piekļuve

2

A.9 (Grundsatz) Pakalpojums dod mākoņpakalpojuma klientam tehniskus līdzekļus, lai datu subjektu piekļuves, labošanas un dzēšanas pieprasījumus izpildītu pašu spēkiem, piemēram, ar eksporta, meklēšanas un dzēšanas funkcijām.

Pēc kā to var atpazīt: Pierādījums ir eksporta un dzēšanas funkciju produkta dokumentācija, ko apstiprina iekšējs izmēģinājums: viens piekļuves pieprasījums tiek izpildīts no sākuma līdz beigām un tiek pierakstīts, cik ilgu laiku tas prasa. Jautājums piegādātājam: vai visus datus par vienu personu var atrast, eksportēt un dzēst bez piegādātāja atbalsta?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.34 Ja klients datu subjekta pieprasījumu nevar apstrādāt pats, piegādātājs sniedz atbalstu līgumā noteiktā termiņā. Pieprasījumus, ko datu subjekti nosūta tieši piegādātājam, nodod klientam, nevis atbild uz tiem pats piegādātājs.

Pēc kā to var atpazīt: Pierādījums ir attiecīgā klauzula datu apstrādes līgumā ar konkrētu atbildes termiņu, kā arī atbalsta pieteikumu vēsture kā reāls piemērs. Jautājums piegādātājam: kāds termiņš ir noteikts atbalstam datu subjektu tiesību izpildē un kādas ir tā izmaksas?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.10 Pārskatatbildība

4

A.10.1 Par personas datu aizsardzības pārkāpumiem mākoņpakalpojuma klientam ziņo bez nepamatotas kavēšanās, norādot apmēru, skartos datus, cēloni un veiktos pasākumus. Paziņošanas process ar atbildību un termiņiem ir noteikts.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir notikumu reaģēšanas plāns ar eskalācijas kādi, līgumā noteiktais paziņošanas termiņš (praksē darbojas 24 līdz 48 stundas, lai klients vēl spējtu ievērot 72 stundu termiņu saskaņā ar GDPR 33. pantu) un ieraksti par iepriekšējiem notikumiem vai par mācībām. Jautājums piegādātājam: kādā termiņā tiek ziņots par notikumu, pa kuru kanālu un kāda informācija tiek sniegta līdzī?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.10.2 Drošības politikas, darbības procedūras un ar tām saistītie ieraksti tiek saglabāti noteiktu laiku, lai apstrādi varētu rekonstruēt arī vēlāk.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir glabāšanas noteikums kopā ar politiku versiju vēsturi, piemēram, dokumentu reģistrā vai versiju kontroles sistēmā ar apstiprināšanas datumu. Jautājums piegādātājam: cik ilgi tiek glabātas politiku versijas un ar tām saistītie ieraksti, un vai audita gadījumā tiem var piekļūt?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.10.3 Pastāv noteikta kārtība personas datu atdošanai, pārņemšanai un iznīcināšanai līguma beigās, nosaucot formātus, termiņus un rīcību ar kopijām.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir izbeigšanas klauzula datu apstrādes līgumā un dzēšanas apliecinājums pēc līguma beigām. Jautājums piegādātājam: kādā formātā un kādā termiņā dati tiek atdoti, kad tiek iznīcinātas visas kopijas un vai par to tiek izsniegts rakstisks apliecinājums?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.35 Aizsardzības pasākumu rezultativitāte tiek regulāri neatkarīgi pārskatīta, piemēram, ar iekšējiem auditiem, ielaušanās testiem vai trešās puses apliecinājuma ziņojumiem. Rezultāti piemērotā veidā ir pieejami mākoņpakalpojuma klientam.

Pēc kā to var atpazīt: Pierādījums ir ISO/IEC 27001 sertifikāts ar piemērojamības paziņojumu, kurā iekļauti ISO/IEC 27018 kontroles pasākumi, vai SOC 2 ziņojums, kopā ar aktuāliem ielaušanās testu kopsavilkumiem. Jautājums piegādātājam: lūgums iesniegt sertifikātu, tā tvērumu un apliecinājumu, ka ISO/IEC 27018 ir atspoguļots piemērojamības paziņojumā. Svarīgi ir pārbaudīt, vai tvērums patiešām aptver izmantoto pakalpojumu.

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11 Informācijas drošība

13

A.11.1 Ikvienam, kam ir piekļuve personas datiem, ir saistošs konfidencialitātes pienākums neatkarīgi no tā, vai persona ir nodarbināta tieši vai piesaistīta no ārpuses.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir parakstītas konfidencialitātes vienošanās vai apliecinājumi, kas paliek spēkā arī pēc sadarbības beigām. Jautājums piegādātājam: vai visi darbinieki un pakalpojumu sniedzēji ar piekļuvi datiem ir rakstiski uzņēmušies konfidencialitātes pienākumu?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.2 Izdrukas un citas papīra kopijas ar personas datiem tiek veidotas tikai tur, kur tas ir absolūti nepieciešams. Pieļaujamo apjomu nosaka noteikums.

Pēc kā to var atpazīt: Pierādījums ir noteikums par rīcību ar izdrukām, kas datu centros parasti ir vispārējs drukāšanas aizliegums zonās ar klientu datiem. Jautājums piegādātājam: vai klientu dati vispār tiek drukāti, un ja jā, ar kādiem nosacījumiem?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.3 Atjaunošana no rezerves kopijām ir iepriekš atļauta, un žurnālā ir norādīta persona, kas atjaunošanu uzsākusi, un skartie dati.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir atjaunošanas žurnāls ar laika zīmogu, ierosinātāju un apjomu, ko rezerves kopiju rīks parasti veido automātiski. Jautājums piegādātājam: vai katra atjaunošana tiek žurnālā un vai audita gadījumā šie žurnāli ir apskatāmi?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.4 Datu nesēji ar personas datiem, kas atstāj telpas, ir aizsargāti pret neatļautu piekļuvi un nozaudēšanu, parasti ar šifrēšanu un transporta ierakstu.

Pēc kā to var atpazīt: Pierādījums ir šifrēšanas apliecinājums (pilna datu nesēja šifrēšana), transporta un nodošanas ieraksti un datu nesēju uzskaitē. Jautājums piegādātājam: vai datu nesēji ar klientu datiem kādreiz atstāj objektus, piemēram, rezerves kopiju vajadzībām, un kā tie ir aizsargāti pārvadāšanas laikā?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.5 Nešifrētu pārnēsājamu datu nesēju un ierīču izmantošana personas datiem ir aizliegta vai ierobežota līdz pamatotiem izņēmumiem ar dokumentētu apstiprinājumu.

Pēc kā to var atpazīt: Pierādījums ir noņemamo datu nesēju politika kopā ar tehnisku ieviešanu, piemēram, piespiedu ierīču šifrēšanu vai USB portiem, kas bloķēti ar ierīču pārvaldību. Jautājums piegādātājam: vai darbinieki var kopēt klientu datus uz nešifrētām ierīcēm un kas to tehniski novērš?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.6 Personas dati, kas tiek pārraidīti publiskajos tīklos, ir šifrēti. Izmantotie mehānismi atbilst pašreizējam tehnikas līmenim.

Pēc kā to var atpazīt: Pierādījums ir TLS konfigurācija (aktuāla protokola versija, bez novecojušiem šifru komplektiem) un ārējs konfigurācijas tests kā ziņojums. Praktiski mazam uzņēmumam: reizi gadā tiek veikta bezmaksas TLS skenēšana un rezultāts tiek saglabāts. Jautājums piegādātājam: kāda pārraides šifrēšana tiek piemērota un vai ir aktīva šifrēšana miera stāvoklī?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.7 Papīra ieraksti ar personas datiem tiek iznīcināti tā, ka to atjaunošana nav iespējama.

Pēc kā to var atpazīt: Pierādījums ir atbilstoša drošības līmeņa dokumentu smalcinātāji vai iznīcināšanas apliecinājumi no pakalpojuma sniedzēja, kas strādā saskaņā ar DIN 66399 vai līdzvērtīgu standartu. Jautājums piegādātājam: kā tiek iznīcināti papīra ieraksti par klientiem un vai iznīcināšanas apliecinājumi ir saglabāti?

Atvērtā	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.11.8 Lietotāju identifikatori ir piešķirti unikāli vienai personai, tos neizsniedz atkārtoti un nekopīgo. Koplietoti konti pastāv tikai pamatos izņēmumos un ar papildu izsekojamību.

Pēc kā to var atpazīt: Pierādījums ir lietotāju saraksts no identitātes sistēmas bez grupu kontiem, kopā ar noteikumu, ka administratīvais darbs notiek ar personisku kontu. Jautājums piegādātājam: vai ekspluatācijas personāls strādā ar personiskiem kontiem un vai daudzfaktoru autentifikācija ir obligāta?

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.11.9 Piegādātājs jebkurā brīdī var norādīt, kurām personām vai lomām ir atļauta piekļuve personas datiem, un uztur šo pārskatu aktuālu.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir piekļuves tiesību pārskats pa lomām, ko apstiprina regulāra piekļuves pārskatīšana ar datumu un rezultātu. Mazam uzņēmumam pietiek ar reizi pusgadā veiktu lietotāju saraksta eksportu ar apstiprinājumu. Jautājums piegādātājam: cik darbinieku var piekļūt mūsu datiem un cik bieži tas tiek pārskatīts?

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.11.10 Lietotāju konti tiek pārvaldīti visā to dzīves ciklā: izveide, izmaiņas un tūlītēja deaktivēšana, kad persona aiziet vai maina lomu.

Pēc kā to var atpazīt: Pierādījums ir darba uzsākšanas un izbeigšanas procedūra ar kontrolsarakstu, kā arī deaktivēto kontu žurnāli ar laika zīmogiem. Jautājums piegādātājam: kādā termiņā tiek atņemta piekļuve darbiniekiem, kas aiziet, un kā tas tiek pierādīts?

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.11.11 Piegādātāja drošības un privātuma pienākumi ir noteikti līgumā, tostarp tehniskie un organizatoriskie pasākumi, klienta norādījumu saistošais spēks un klienta tiesības veikt auditu.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir parakstīts datu apstrādes līgums saskaņā ar GDPR 28. pantu ar pasākumu pielikumu un audita vai informācijas tiesībām. Jautājums piegādātājam: līgums iesniedz parakstītu datu apstrādes līgumu kopā ar pielikumiem, nevis tikai atsauci uz vispārīgiem pakalpojuma noteikumiem.

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.11.12 Apakšuzņēmējiem, kas apstrādā personas datus, ir vismaz tie paši pienākumi, kas pašam piegādātājam. To izvēli un pastāvīgu uzraudzību nosaka noteikts process.

Pēc kā to var atpazīt: Pierādījums ir pienākumu pārņemšana līgumos ar apakšuzņēmējiem (GDPR 28. panta 4. punkts) un piegādātāju novērtēšana ar datumu. Jautājums piegādātājam: kā tiek novērtēti apakšuzņēmēji un kādus pierādījumus no tiem pieprasa?

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.11.13 Pirms krātuves vietas atkārtotas izmantošanas ir nodrošināts, ka iepriekšējo lietotāju dati nepaliek pieejami ne fiziskajos datu nesējos, ne virtualizētās vidēs.

Pēc kā to var atpazīt: Pierādījums ir attīrīšanas vai pārrakstīšanas procedūra, ko piemēro krātuves atbrīvošanas brīdī, ieraksti par datu nesēju iznīcināšanu un klientu nodalīšanu, kas aprakstīta arhitektūras dokumentā. Jautājums piegādātājam: kā tiek nodrošināts, ka atkārtoti izmantotā krātuvē nav citu klientu atlikušo datu?

Atvērta Procesā Izpildīta Neattiecas

Pierādījums / pamatojums

A.12 Privātuma atbilstība

3

A.12.1 Valstis, kurās personas dati tiek glabāti un apstrādāti, ir nosauktas un mākoņpakalpojuma klientam zināmas. Par glabāšanas vietu izmaiņām tiek paziņots.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir piegādātāja pārskats par objektiem un reģioniem līgumā vai dokumentācijā, kā arī ekrānuzņēmums ar izmantotā pakalpojuma reģiona iestatījumu. Jautājums piegādātājam: kurās valstīs mūsu dati atrodas miera stāvoklī, no kurām valstīm tiem piekļūst, piemēram, atbalsta darbā, un vai reģionu var fiksēt?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

A.12.2 Personas datu nodošana uz trešām valstīm ir zināma, pamatota un nodrošināta ar atbilstošiem aizsardzības pasākumiem.[Dokuments](#)

Pēc kā to var atpazīt: Pierādījums ir līguma standartklauzulas vai lēmums par aizsardzības līmeņa pietiekamību, ko apstiprina nodošanas ietekmes novērtējums, kas mazam uzņēmumam var būt īss: skartās datu kategorijas, saņēmēja valsts, risks, veiktie papildu pasākumi. Jautājums piegādātājam: uz kāda tiesiskā pamata dati tiek nodoti trešām valstīm un kādi papildu pasākumi tiek piemēroti?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums

5.31 Juridiskās un līgumiskās prasības, kas attiecas uz personas datu apstrādi, ir apzinātas un tiek uzturētas aktuālas, mainoties tiesiskajai situācijai. Pretrunīgas jurisdikcijas ir novērtētas.

Pēc kā to var atpazīt: Pierādījums ir pārskats par piemērojamajām prasībām (GDPR, valsts noteikumi, nozarei specifiski pienākumi) ar atbildīgo un pārskatīšanas datumu. Mazā uzņēmumā pietiek ar vienas lappuses sarakstu, ko pārskata reizi gadā. Jautājums piegādātājam: vai piegādātājs vai tā apakšuzņēmēji ir pakļauti jurisdikcijām, kas ļauj iestādēm piekļūt mūsu datiem, un kā ar to rīkojas?

Atvērta	Procesā	Izpildīta	Neattiecas
---------	---------	-----------	------------

Pierādījums / pamatojums