Nacionālais kiberdrošības centrs

https://cyber.gov.lv, NIS2@mod.gov.lv, 67335131

Informācijas sistēmas un resursu drošības klašu noteikšanas vadlīnijas

Saskaņā ar Ministru kabineta 2025. gada 25. jūnija noteikumu Nr. 397 38. punktu

Šīs vadlīnijas izstrādātas, lai palīdzētu Nacionālās kiberdrošības likuma subjektiem (būtisko pakalpojumu sniedzējiem, svarīgo pakalpojumu sniedzējiem un IKT kritiskās infrastruktūras īpašniekiem) noteikt savu IKT resursu un informācijas un to sistēmu drošības klases.

Versija 2.0, 07.09.2026

SATURS

1. IEVADS

1.1. MĒRĶIS UN PIEMĒROŠANAS JOMA

Šo vadlīniju mērķis ir nodrošināt vienotu pieeju informācijas un komunikācijas tehnoloģiju (IKT) resursu, informācijas un to sistēmu drošības klašu noteikšanai, kas ir būtiska daļa no kiberdrošības pārvaldības procesa.

Vadlīnijas piedāvā metodiku, kuru var piemērot visi Nacionālās kiberdrošības likuma (turpmāk - NKDL) subjekti, lai klasificētu informācijas sistēmas atbilstoši to konfidencialitātes, integritātes un pieejamības zuduma riskam un nodrošinātu atbilstību Eiropas Savienības NIS2 direktīvas (Direktīva (ES) 2022/2555) prasībām par vienādi augsta kiberdrošības līmeņa sasniegšanu visā Eiropas Savienībā.

1.2. NORMATĪVAIS KONTEKSTS

Vadlīnijas ir izstrādātas, pamatojoties uz Nacionālo kiberdrošības likumu, Ministru kabineta 2025. gada 25. jūnija noteikumiem Nr. 397 "Minimālās kiberdrošības prasības", kā arī Eiropas Savienības kiberdrošības regulējumu.

NIS2 direktīva (Direktīva (ES) 2022/2555) nosaka vienoti augsta kiberdrošības līmeņa prasības Eiropas Savienībā, paredzot pienākumus risku pārvaldības, incidentu ziņošanas, piegāžu ķēdes drošības un pārvaldības jomās.

Komisijas Īstenošanas regula (ES) 2024/2690 nosaka kiberdrošības risku pārvaldības un būtisku incidentu identificēšanas prasības konkrētiem digitālo un IKT pakalpojumu sniedzējiem (DNS un TLD reģistru, mākoņdatošanas, datu centru, satura piegādes tīklu, pārvaldītu un pārvaldītu drošības pakalpojumu, tiešsaistes platformu un uzticamības pakalpojumu sniedzējiem).

Ministru kabineta noteikumi Nr. 397 "Minimālās kiberdrošības prasības" (turpmāk – MK 397) nosaka uz risku balstītu kiberdrošības pārvaldības ietvaru, definējot organizatoriskos, tehniskos un fiziskos drošības pasākumus, kas īstenojami atbilstoši informācijas sistēmu un IKT resursu drošības klasifikācijai. Prasības aptver kiberdrošības pārvaldību visā informācijas sistēmu dzīves ciklā, tostarp risku un incidentu pārvaldību, aktīvu aizsardzību, piekļuves tiesību administrēšanu, rezerves kopiju pārvaldību, darbības nepārtrauktības nodrošināšanu, piegāžu ķēdes un ārpakalpojumu risku pārvaldību, kā arī drošības pasākumu uzraudzību un pilnveidošanu.

Vadlīnijas adresētas NKDL 20., 21. un 24. pantā noteiktajiem subjektiem:

- būtisko pakalpojumu sniedzējiem (NKDL 20. pants);
- svarīgo pakalpojumu sniedzējiem (NKDL 21. pants);
- IKT kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem (NKDL 24. pants).

Vadlīnijas ir noderīgas arī domēnu vārdu reģistrācijas pakalpojumu sniedzējiem (NKDL 23. pants) un citām organizācijām, kas brīvprātīgi piemēro MK 397 prasības.

Kāpēc drošības klase ir svarīga?

Drošības klase nav uzskaites formalitāte - no tās tieši izriet MK 397 prasību piemērošanas apjoms un IKT resursu vai informācijas sistēmu nepieciešamais aizsardzības līmenis un pārskatīšanas regularitāte**.**

2. TERMINI UN DEFINĪCIJAS[1]

Termins	Apraksts
Informācijas resurss	Strukturēts digitālo datu kopums, kas tiek elektroniski apstrādāts informācijas sistēmā (piem., datubāzes, dokumentu krājumi, reģistru ieraksti). Piezīme: Kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā drošības klase ir tieši piemērojama, izvērtējot riska līmeni, atbilstoši MK 397 5. pielikumam.
IKT resursi	Tehnisko resursu un informācijas resursu kopums. Piemēram: Serveri, datortīkli, ugunsmūri, datu glabāšanas iekārtas, darba stacijas, tīkla aktīvie elementi utt. Piezīme: Kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā drošības klase ir tieši piemērojama, izvērtējot riska līmeni, atbilstoši MK 397 5. pielikumam.
Tehniskais resurss	Aparatūra, iekārta, kas ir tīkla vai informācijas sistēmas sastāvdaļa vai IKT infrastruktūrā izmantota iekārta, kas veic datu apmaiņu ar informācijas sistēmu, un programmatūra, tostarp operētājsistēmas, sistēmfaili, sistēmprogrammas, lietojumprogrammas un palīgprogrammas. Piezīme: Kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā drošības klase nav tieši piemērojama, bet, ja uzskaite ir būtiska, tad tā piešķirama no informācijas sistēmas drošības klases.
Resursu kategorija	Resursu kategoriju piemēri nav tieši definēti MK 397, taču tās saprot kā informācijas veidus vai kā grupu ar līdzīgu aizsardzības līmeni.
Informācijas sistēma	Organizēta sistēma, kas paredzēta informācijas resursu pārvaldībai un elektroniskajai apstrādei, izmantojot tehniskos resursus. Piezīme: Kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu katalogā drošības klase ir tieši piemērojama, izvērtējot riska līmeni, atbilstoši MK 397 5. pielikumam. Informācijas sistēmas drošības klase nosaka, kāds minimālais drošības pasākumu līmenis ir jāievieš, t. sk. tehnisko un organizatorisko un administratīvo kontroļu detalizācijas pakāpi, incidentu pārvaldības kārtību un atbilstības nodrošināšanas mehānismus. Zemākā piešķiramā klase kiberdrošības riskam pakļautam IKT resursam, informācijas sistēmai vai informācijai ir C (minimālās drošības).
Drošības pasākumi	Tehniski vai organizatoriski pasākumi, kas tiek noteikti risku pārvaldības ietvaros un samazina risku līdz pieņemamam līmenim.

[1] https://likumi.lv/ta/id/361481-minimalas-kiberdrosibas-prasibas#p2 Ministru kabineta noteikumos Nr. 397 lietotie termini

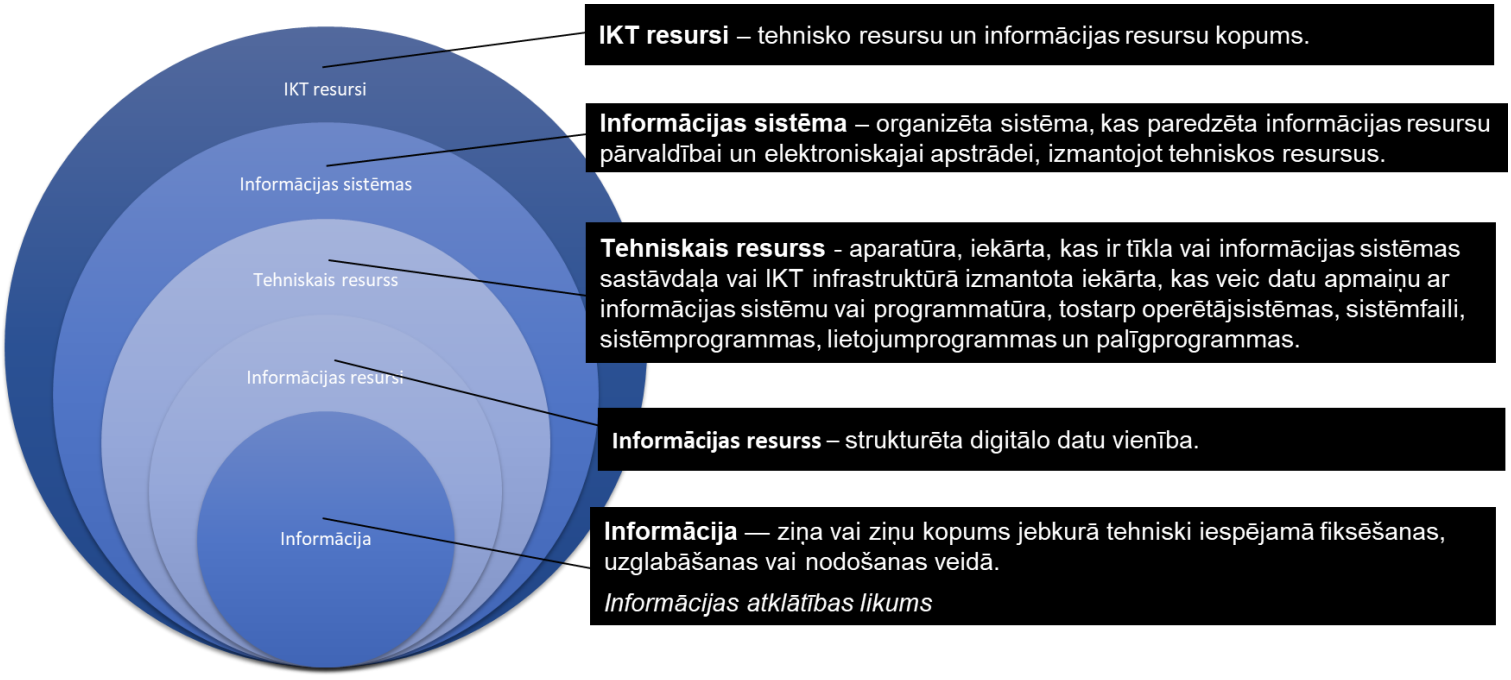
Drošības klase	IKT resursu un informācijas sistēmu kataloga informācijas resursa/sistēmas kritiskuma (ietekme uz kritisku, būstisku vai svarīgu pakalpojumu, valstiskiem procesiem, atbilstoši MK 397 5. pielikumam) pakāpe konfidencialitātes, integritātes un pieejamības riska dimensijās: drošības klasēs A (augsta), B (vidēja), C (zema). Piezīme: noteikumos nav tieši aprakstīts drošības klases termins, taču ir aprakstīta noteikšanas metodika.
Ārpakalpojums	Jebkura veida vienošanās starp subjektu un pakalpojuma sniedzēju IKT jomā, saskaņā ar kuru šis pakalpojuma sniedzējs nodrošina procesu, sniedz pakalpojumu, veic tehnisko resursu piegādi vai veic citu darbību subjekta uzdevumā IKT infrastruktūrā.

IKT resurss = kopums (tehnoloģija + dati).

Informācijas resurss = dati un saturs - tas kas jāaizsargā (piem., datubāzes, dokumentu krājumi, reģistru ieraksti).

Tehniskais resurss = vide (vieta, kur dati atrodas un ar ko tie tiek apstrādāti).

Informācijas sistēma = organizēta sistēma, kas paredzēta informācijas resursu pārvaldībai un elektroniskajai apstrādei, izmantojot tehniskos resursus.



3. DROŠĪBAS KLAŠU NOTEIKŠANAS METODIKA (MK 397, 5. PIELIKUMS)

3.1. VISPĀRĪGIE PRINCIPI

Informācijas sistēmas drošības klase sakrīt ar augstāko riska līmeņa konfidencialitātes, integritātes un pieejamības (angļu val. *Confidentiality, Integrity, Availability* jeb CIA) riska līmeņa dimensiju.

Klasifikācija notiek divos soļos. **Pirmajā solī** katrai informācijas sistēmai un katrai tās apstrādāto informācijas resursu kategorijai piešķir atsevišķu klasi trijās riska dimensijās - konfidencialitātē, integritātē un pieejamībā (MK 397 32. punkts). **Otrajā solī** no šīm trim dimensijām atvasina informācijas sistēmas kopējo klasi (MK 397 33. punkts).

MK 397 33. punkts nosaka kā sistēma tiek klasificēta kopumā (A, B vai C klase) atkarībā no piešķirtajām klasēm konfidencialitātes, integritātes un pieejamības aspektos:

- **33.1.** **A** drošības klases **(paaugstinātas drošības)** informācijas sistēmu, ja tai ir noteikta vismaz viena A konfidencialitātes, integritātes vai pieejamības drošības klase;
- **33.2.** **B** drošības klases **(pamata drošības)** informācijas sistēmu, ja tai ir noteikta vismaz viena B konfidencialitātes, integritātes vai pieejamības drošības klase, bet nav noteikta neviena A konfidencialitātes, integritātes vai pieejamības drošības klase;
- **33.3.** **C** drošības klases **(minimālās drošības)** informācijas sistēmu, ja tai ir noteiktas tikai C konfidencialitātes, integritātes un pieejamības drošības klases.

3.2. VIENKĀRŠOTS SKAIDROJOŠS LĒMUMA PRINCIPS

(neatspēko MK 397 5. pielikuma metodiku).

Novērtējuma jautājums	Ja sekas ir augsta riska	Ja sekas ir vidēja riska	Ja sekas nav zemas riska
Kas notiktu, ja IKT resursa vai informācijas sistēmas informācija tiktu izpausta vai nopludināta?	**A klase**	**B klase**	**C klase**
Kas notiktu, ja IKT resursa vai informācijas sistēmas informācija tiktu sagrozīta, bojāta vai dzēsta?	**A klase**	**B klase**	**C klase**
Kas notiktu, ja IKT resursa vai informācijas sistēmas informācija nebūtu pieejama?	**A klase**	**B klase**	**C klase**
		Kopējā (augstākā) **drošības klase**	**A**

Praktiski tas nozīmē, ka kopējā klase sakrīt ar **augstāko** no trim dimensiju klasēm. Apzīmējumu lieto konsekventi: **A - paaugstinātas drošības, B - pamata drošības, C - minimālās drošības** informācijas sistēma.

Dimensiju klases (K/I/P)	Kopējā klase	Apzīmējums
A / C / C	**A**	paaugstinātas drošības
C / A / B	**A**	paaugstinātas drošības
B / C / C	**B**	pamata drošības
C / B / B	**B**	pamata drošības
C / C / C	**C**	minimālās drošības

Tehniskie resursi

Tehniskajiem resursiem drošības klasi patstāvīgi nenosaka. MK 397 32. punkts klasifikācijas pienākumu attiecina uz informācijas sistēmām un informācijas resursu kategorijām. Tehniskais resurss manto tās informācijas sistēmas klasi, kuras darbību tas nodrošina - ja resurss apkalpo vairākas sistēmas, tas manto augstāko no tām.

No mantotās klases izriet, piemēram, žurnālfailu glabāšanas termiņš (MK 397 57. punkts, kas tieši min operētājsistēmas, pakalpes, tīklu un serveru iekārtas) un ārpakalpojuma prasības.

3.3. DETALIZĒTĀKS DROŠĪBAS KLAŠU IZVĒRTĒJUMS

Konfidencialitāte

Informācijas veids	Apjoms vai iespējamās sekas	Konfidencialitātes klase
Personas dati	≥ 1 000 000 datu subjektu	A
Īpašu kategoriju personas dati	≥ 500 000 datu subjektu	A
Īpašu kategoriju personas dati	5 000 līdz 499 999 datu subjektu	B
Ierobežotas pieejamības informācija	Neatkarīgi no apjoma	B, ja nav A pazīmes
Informācijas izpaušana	Kaitētu nacionālās drošības interesēm	A
Informācijas izpaušana	Kaitētu Latvijas Republikas reputācijai	B
Informācijas izpaušana	Neradītu minēto kaitējumu un nav citu A vai B pazīmju	C

Integritāte

Ietekmes līmenis	Praktiskais skaidrojums	Integritātes klase
Valsts mēroga vai katastrofāla ietekme	Tiek pārtrauktas vai būtiski apgrūtinātas valsts vai pašvaldības pamatfunkcijas, kritiskā infrastruktūra vai iespējama katastrofa	A
Būtiska ietekme uz subjektu	Tiek būtiski traucēta organizācijas darbība vai tās būtiskā vai svarīgā pakalpojuma sniegšana	B
Būtiska ietekme uz citu subjektu	Pārkāpuma sekas izplatās ārpus organizācijas un būtiski traucē cita NKDL subjekta darbību vai pakalpojumu	B
Nebūtiska ietekme	Kļūdu var novērst, būtiski neietekmējot funkcijas vai pakalpojumus	C

Pieejamība

Paredzētais darbības laiks	Stundas mēnesī, vidēji	A klase: ne vairāk kā 0,1 %	B klase: ne vairāk kā 1 %
24h × 7, nepārtraukti	~ 730 h	~ 44 min	~ 7 h 18 min
12h × 7	~ 365 h	~ 22 min	~ 3 h 39 min
8h × 5, darba dienās	~ 176 h	~ 11 min	~ 1 h 46 min

3.4. KO DROŠĪBAS KLASE NOSAKA – KĀDS IR PRASĪBU APJOMS?

Prasība	A klase	B klase	C klase	MK 397
Daudzfaktoru autentifikācija	administratora un standarta lietotāja kontam	administratora vai standarta lietotāja kontam, ja attālinātai piekļuvei no ārējā tīkla netiek izmantots VPN ar daudzfaktoru autentifikāciju.	nav noteikta (ieteicama pēc riska izvērtējuma)	52.1.–52.3.
Tīkla segmentēšana pēc informācijas resursu drošības klasēm	jā	jā	jā	55.1., 56.
Žurnālfailu glabāšanas termiņš	vismaz 18 mēneši	vismaz 12 mēneši	vismaz 6 mēneši	57.1.–57.3.

Prasība	A klase	B klase	C klase	MK 397
Rezerves kopiju atjaunošanas punkti	iepriekšējā dienā, pirms nedēļas, pirms mēneša, iepriekšējā gadā	pēdējās nedēļas laikā, pirms nedēļas, pirms mēneša, iepriekšējā gadā	pirms pēdējām nozīmīgajām izmaiņām, bet ne senāk kā pirms 6 mēnešiem	70.1.–70.3.
Rezerves kopijas kontrolsumma pēc izveides	jā, ja netiek izmantotas citas integritātes pārbaudes metodes	-	-	71.3.
Pilna rezerves kopija atdalītos tehniskajos resursos, ģeogrāfiski attālinātā vietā, aizsargātās telpās ar automātisko ugunsgrēka atklāšanas un trauksmes signalizācijas sistēmu	jā	-	-	72.2.
Integritātes pārbaude pēc kopijas pārvietošanas citā datu nesējā	jā	jā	-	72.3.
Rezerves kopiju nolasīšanas izlases pārbaude	ne retāk kā reizi 6 mēnešos	ne retāk kā reizi gadā vai pēc būtiskām izmaiņām	-	74.2.
Testa vidē tikai sintētiski dati, līguma izpilde ne produkcijas vidē	jā (A konfidencialitātes klase)	jā (B konfidencialitātes klase)	-	88.3.
Funkcionālā apraksta iesniegšana SAB pirms jaunas IS izveides (tikai IKT KI)	jā	jā	-	36.
SAB atzinums pirms ārpakalpojuma līguma noslēgšanas (tikai IKT KI)	jā	-	-	93.
Tehnisko resursu iegādes jurisdikcijas prasības NATO / ES / EBTA / IP4 (tikai IKT KI)	jā	-	-	94., 95.

Prasība	A klase	B klase	C klase	MK 397
Pašvērtējuma biežums (subjekta līmenī)	reizi gadā, ja subjekta īpašumā vai valdījumā ir vismaz viena A klases IS	reizi trijos gados	reizi trijos gados	141.1., 141.2.

3.5. KLASIFICĒŠANAS PĀRSKATĪŠANA UN AKTUALIZĒŠANA

— **Jauns notikums:** Kataloga ieraksts, tostarp drošības klase, aktualizējams nekavējoties, bet ne vēlāk kā viena mēneša laikā pēc izmaiņām (MK 397 31. punkts).

— **Periodiski:** Klasifikāciju pārskata vismaz reizi gadā, ņemot vērā normatīvo aktu izmaiņas un aktīva vērtības, jutīguma un kritiskuma izmaiņas tā dzīves ciklā.

— **Notikumi, kas prasa pārvērtēšanu:** Jaunas informācijas resursu kategorijas pievienošana, datu subjektu skaita pārsniegšana pār slieksni, jauna integrācija vai atkarība, informācijas sistēmas iekļaušana kritiskās infrastruktūras kopumā, ārpakalpojuma modeļa maiņa, būtiskas izmaiņas sistēmas paredzētajā darbības laikā.

— **Atbildība:** Klasi nosaka informācijas sistēmas vai informācijas resursa īpašnieks vai tiesiskais valdītājs, un šī atbildība fiksējama kataloga ierakstā. Kiberdrošības pārvaldnieks pārbauda klasifikācijas atbilstību metodikai un tās sekas prasību piemērošanā.

3.5. UZRAUDZĪBA

Uzraudzības dalījumu nosaka Nacionālās kiberdrošības likuma 41. pants. Tas nosaka arī, kam iesniedzams pašvērtējuma ziņojums (MK 397 142. punkts).

Iestāde	Uzraudzības tvērums	Juridiskais pamats
Nacionālais kiberdrošības centrs (NKDC)	Būtisko pakalpojumu un svarīgo pakalpojumu sniedzēji, **izņemot** informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru	NKDL 41. panta 1. punkts
Satversmes aizsardzības birojs (SAB)	Informācijas un komunikācijas tehnoloģiju kritiskā infrastruktūra	NKDL 41. panta 2. Punkts
Nozares regulatori	Atsevišķās nozarēs – (piemēram, finanšu, enerģētikas, elektronisko sakaru vai veselības aprūpes) darbojas arī nozares regulatoru prasības, kas noteiktas citos normatīvajos aktos.	NKDL 41. panta izpratnē un neaizstāj MK 397 prasības, bet var noteikt papildu vai stingrākus pienākumus.

4. PRAKTISKIE PIEMĒRI

4.1. DROŠĪBAS KLAŠU PIEMĒROŠANA

Piemērs 1. Valsts iestādes publisks tīmekļa portāls

Publisks portāls, kurā iedzīvotāji lasa jaunākās ziņas un piekļūst publiskiem dokumentiem un instrukcijām. E-pakalpojumi caur portālu netiek sniegti.

Dimensija	Vērtējums	Klase
Konfidencialitāte	Viss saturs paredzēts publiskai piekļuvei. Nav ierobežotas pieejamības informācijas, nav personas datu virs sliekšņa. Noplūde neradītu kaitējumu Latvijas Republikas reputācijai.	**C**
Integritāte	Satura sagrozīšana kaitētu iestādes reputācijai, bet neapturētu un būtiski neapgrūtinātu pamatfunkciju īstenošanu - atļauju izsniegšana un pakalpojumu sniegšana caur portālu nenotiek. Sekas ir viegli labojamas.	**C**
Pieejamība	Portāla nepieejamība dažu stundu vai dienas garumā ir nepatīkama, bet informācija iegūstama citur vai vēlāk. No portāla pieejamības nav atkarīga citas informācijas sistēmas darbība. Pieļaujams neplānots pārtraukums virs 1 % no paredzētā darbības laika.	**C**

Rezultāts: C / C / C. Kopējā klase — C (minimālās drošības informācijas sistēma, MK 397 33.3. apakšpunkts).

Piemērs 2. Privāta uzņēmuma iekšējā dokumentu vadības sistēma

Vidēja izmēra ražošanas uzņēmums, kas ir svarīgo pakalpojumu sniedzējs, bet nav kritiskā infrastruktūra. Sistēmā glabā rīkojumus, līgumprojektus, komercnoslēpuma informāciju un darbinieku personu lietas.

Dimensija	Vērtējums	Klase
Konfidencialitāte	Saturs nav publisks - darbinieku personas dati un komercinformācija. Tā ir ierobežotas pieejamības informācija. Īpašu kategoriju personas dati nesasniedz 5000 datu subjektu slieksni, bet ierobežotas pieejamības informācijas esamība pati par sevi izpilda B pazīmi.	**B**
Integritāte	Dokumentu sagrozīšana radītu juridiskas un operacionālas problēmas, bet neapturētu ražošanu - svarīgā pakalpojuma sniegšana turpinātos. Citi subjekti necieš.	**C**
Pieejamība	Informācijas sistēmas nepieejamība nedēļu bremzētu administrāciju, bet ražošana turpinātos. No sistēmas pieejamības nav atkarīga citas informācijas sistēmas darbība. Pieļaujams neplānots pārtraukums virs 1 %.	**C**

Rezultāts: B / C / C. Kopējā klase — B (pamata drošības informācijas sistēma, MK 397 33.2. apakšpunkts)**.**

Piemērs 3. Iedzīvotāju reģistra valsts informācijas sistēma

Valsts mēroga informācijas sistēma, kurā glabā visu Latvijas iedzīvotāju personas datus un kuras datus izmanto citas valsts iestādes.

Dimensija	Vērtējums	Klase
Konfidencialitāte	Informācijas resurss satur vairāk nekā 1 000 000 datu subjektu personas datus (vārds, uzvārds, personas kods, dzīvesvietas adrese, pilsonība, ģimenes stāvoklis). Izpildās A pazīme par 1 000 000 datu subjektu slieksni.	**A**
Integritāte	Dati tiek ievadīti un atjaunināti pēc oficiāliem dokumentiem un izmantoti citās valsts informācijas sistēmās (vēlēšanu saraksti, personu apliecinošu dokumentu izsniegšana). Integritātes pārkāpums var pārtraukt vai būtiski apgrūtināt valsts pamatfunkciju īstenošanu.	**A**

Dimensija	Vērtējums	Klase
Pieejamība	Nepieejamība liedz izsniegt personu apliecinošus dokumentus, reģistrēt dzīvesvietu un ģimenes stāvokļa izmaiņas; ietekmēts arī citu iestāžu darbs (PMLP, pašvaldības, Valsts policija). Izpildās A pazīme par valsts pamatfunkciju būtisku apgrūtināšanu, un no sistēmas ir atkarīgas citas A pieejamības klases sistēmas.	**A**

Rezultāts: A / A / A. Kopējā klase - A (paaugstinātas drošības informācijas sistēma, MK 397 33.1. apakšpunkts).

Piemēri ilustrē metodikas piemērošanu un nav paraugs. Vienāda nosaukuma sistēmām dažādos subjektos drošības klase var atšķirties atkarībā no apstrādāto informācijas resursu kategorijām, atkarību ķēdes un paredzētā darbības laika.

4.2. ĀRPAKALPOJUMA UN ĀRĒJI PĀRVALDĪTAS INFORMĀCIJAS SISTĒMAS

Kataloga tvērums - Kiberdrošības riskam pakļauto IKT resursu un informācijas sistēmu kataloga tvērumu nosaka MK 397 30. punkts, un klasifikācijas pienākuma tvērumu - 32. punkts. Abās normās kritērijs ir viens un tas pats: **subjekta īpašums un valdījums.**

Pārvaldnieka atbildības apjoms ir tieši saistīts ar viņam piešķirto tiesību un pilnvaru robežām, kas uzraudzības kontekstā atbilst noteikumu 54. punktam un spējai reaģēt uz incidentiem, tāpat arī vai nodrošināt ārpakalpojumu pārvaldību vai sakārtot līgumu attiecības tādā mērā, ka MK 397 prasības (atbilstoši resursa kategorijas drošības klases aizsardzības prasībām) tiek īstenotas.

Subjekta īpašumā vai tiesiskajā valdījumā esošos IKT resursus un informācijas sistēmas iekļauj IKT resursu un informācijas sistēmu katalogā.

Ārpakalpojumus, kuru informācijas sistēmu konfigurācija un žurnālfailu pārvaldība neatrodas subjekta tiesiskā īpašnieka vai valdītāja **pārvaldībā vai kontrolē**, un piegāžu ķēdes papildus **uzskaita reģistrā / sarakstā**, **bet to drošības, uzraudzības un pakalpojuma līmeņa prasības nosaka līgumā vai tā pielikumos**. Ja informācijas sistēmas konfigurāciju vai žurnālfailus pārvalda ārpakalpojuma sniedzējs, līgumā nodrošina kiberdrošības pārvaldniekam MK 397 54. un 87. - 92. punktā paredzētās piekļuves, informācijas saņemšanas, incidentu pārvaldības un kontroles tiesības.

Savukārt ārpakalpojumi, kuru informācijas sistēmu konfigurācija un žurnālfailu pārvaldība atrodas subjekta tiesiskā īpašnieka vai valdītāja pārvaldībā vai kontrolē, un kas atbilst un spēj īstenot MK 397 54. punktā noteiktās prasības, **ir uzskaitāmi IKT resursu un informācijas sistēmu katalogā.**

No vadlīniju ārpakalpojumu izklāsta izriet trīs situācijas:

Situācija	Katalogā	Klase	Ko dara
Informācijas sistēma ir subjekta **īpašumā vai valdījumā** - arī tad, ja to izvieto vai uztur ārpakalpojuma sniedzējs (piemēram, mitināšana datu centrā, uzturēšana pēc līguma)	**Jā**	Nosakāma	**Uzskaita un klasificē parastajā kārtībā.** Ārpakalpojuma sniedzēja pienākumus nosaka līgumā pēc MK 397 87. punkta.
Informācijas sistēma nav subjekta īpašumā vai valdījumā - subjektam ir tikai lietotāja tiesības uz pakalpojuma sniedzēja pārvaldītu risinājumu (tipiski nozares koplietošanas sistēma vai SaaS)	**Nē**	Nenosaka	**Iekļauj ārpakalpojumu reģistrā**. Risku pārvalda ar līgumu un organizatoriskajām kontrolēm.
Subjekta pārvaldībā esoša informācijas sistēma **nodrošina autentifikāciju vai identitātes pārvaldību** piekļuvei ārēji pārvaldītam risinājumam	**Jā**	Nosakāma	**Uzskaita un klasificē šo sistēmu**, ierakstā aprakstot tās funkcionalitāti un saskarni ar ārējo risinājumu.

4.2. ĀRPAKALPOJUMU PIEMĒROŠANA

Piemērs	Raksturojums	Rezultāts
1. Pašvaldības lietvedības sistēma, izvietota pašvaldības serverī	Īpašnieks un tiesiskais valdītājs - pašvaldības dome. Izvietota pašvaldības infrastruktūrā. Lomas: lietvedis, vadītājs, administrators. Lokāli nodrošināts MFA. Rezerves kopijas nodrošina pašvaldības IKT struktūrvienība. Saskarne ar ārēju e-pakalpojumu risinājumu.	**Katalogā: Jā.** Drošības klase nosakāma (piemērā- satur personas datus un ietekmē būtiskus procesus → B konfidencialitāte, C integritāte, C pieejamība → kopējā klase **B**). Saskarne ar ārējo risinājumu fiksējama kataloga ierakstā.
2. Grāmatvedības un algu aprēķina SaaS risinājums	Risinājumu pārvalda pakalpojuma sniedzējs savā infrastruktūrā. Subjektam ir tikai lietotāja tiesības - sistēmas konfigurācija un žurnālfailu pārvaldība nav subjekta īpašumā vai valdījumā.	**Katalogā: Nē.** Drošības klase netiek noteikta. Iekļaujams ārpakalpojumu reģistrā. Ja piekļuvei izmanto subjekta pārvaldītu identitātes sistēmu, **šī sistēma** iekļaujama katalogā.

Piemērs	Raksturojums	Rezultāts
3. Nozares koplietošanas informācijas sistēma	Lietojumprogrammas tiesiskais īpašnieks ir cita persona vai deleģēta institūcija - subjektam ir lietotāja tiesības.	**Katalogā: Nē** (subjekta katalogā). Iekļaujams ārpakalpojumu reģistrā. Klasi nosaka sistēmas īpašnieks vai tiesiskais valdītājs savā katalogā.
4. Pašvaldības tīkla infrastruktūras iekārta	Tīkla ierīce, kas nodrošina datu plūsmas vadību starp tīkla segmentiem, vai ugunsmūris. Īpašnieks - pašvaldības dome. Resursu tips: tehniskais resurss.	**Katalogā: Jā.** Patstāvīga drošības klase netiek noteikta - resurss manto augstāko no to informācijas sistēmu klasēm, kuru darbību tas nodrošina.

5. BUJ

1. **Saskaņā ar MK 397 34. punktu: "Kritiskās infrastruktūras kopumā iekļautu informācijas sistēmu uzskata par A drošības klases informācijas sistēmu, nepiemērojot šo noteikumu 32. un 33. punktā minēto kārtību." Ja sistēmas (piemēram, video novērošana, piekļuves punkti, apsardzes sistēmas) tiek uzskatītas par neatņemamu kritiskās infrastruktūras daļu, tās automātiski kvalificējas kā A drošības klases informācijas sistēmas. Vai šādā gadījumā ir nepieciešams aizpildīt 5. pielikumu, kas paredzēts drošības klases izvērtēšanai?**

   Atbilde: Vēršam uzmanību uz MK 397 35. punktā noteikto, proti, ja kritiskās infrastruktūras kopumā ir iekļauta visa subjekta IKT infrastruktūra, subjekts informācijas sistēmām nosakāmās drošības klases saskaņo ar SAB. Subjekta informācijas sistēmu drošības klases nosakāmas saskaņā ar noteikumu 5. pielikumā ietverto metodiku. Ņemot vērā norādīto subjektam nepieciešams noteikt konfidencialitātes, integritātes un pieejamības drošības klasi (A, B vai C) atbilstoši šo noteikumu 5. pielikumā ietvertajai metodikai katrai subjekta īpašumā un valdījumā esošajai informācijas sistēmai un informācijas resursu kategorijai, un saskaņā ar MK 397 35. punktā noteikto, nosūtīt tās saskaņošanai SAB.

2. **Kritiskās infrastruktūras objektā atrodas sistēmas serveris un daļa aprīkojuma, kas ir klasificēti kā A klase. Vai ir pareizi uzskatīt, ka arī pārējās šīs sistēmas iekārtas, kas atrodas citos reģionos un kalpo kā datu pārsūtītāji, automātiski jāuzskata par A drošības klases iekārtām?**

Atbilde: Skaidrojam, ka Ministru kabineta 2021. gada 6. jūlija noteikumi Nr. 508 "Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas, drošības pasākumu un darbības nepārtrauktības plānošanas un īstenošanas kārtība" (turpmāk - MK noteikumi Nr. 508) nosaka, ka valsts drošības iestādes apzina iespējamo A, B un C kategorijas kritisko infrastruktūru un šie noteikumi nenosaka informācijas sistēmas konfidencialitātes, integritātes un pieejamības drošības klases. MK noteikumos Nr. 508 ietvertā kritiskās infrastruktūras klasifikācija izriet no Nacionālās drošības likuma $22.^2$ panta otrajā daļā ietvertās klasifikācijas. Skaidrojam, ka,

piemēram, gadījumā, ja MK noteikumu Nr. 508 izpratnē tiek piešķirta B kategorijas kritiskās infrastruktūras statuss, tas nenozīmē, ka visām sistēmām MK 397 izpratnē arī tiks piešķirta B drošības klase.

3. **Kritiskās infrastruktūras objektā atrodas sistēmas serveris un daļa aprīkojuma, kas ir klasificēti kā B klase. Vai šo sistēmu uzskata kā kritiskās infrastruktūras kopumā esošu sistēmu un jāpārvērtē kā A sistēmu?**

Atbilde: Ja kritiskajā objektā atrodas sistēmas serveris un daļa aprīkojuma, kas ir klasificēti kā B klase, vai šo sistēmu uzskata kā kritiskās infrastruktūras kopumā esošu sistēmu un jāpārvērtē kā A sistēmu, skaidrojam, ka saskaņā ar MK 397 noteikto un augstāk minēto, ja kritiskās infrastruktūras kopumā ir iekļauta visa subjekta IKT infrastruktūra, subjekts informācijas sistēmām nosakāmās drošības klases saskaņo ar SAB. Vienlaikus norādām, ka KI objektā var būt informācijas sistēmas, kas ir zemākas drošības klases par A drošības klasi.

4. **Gadījumā, ja mēs kā iestāde esam noteikti par kritisku infrastruktūru (B kategorijas), tajā esošās informācijas sistēmas, saskaņā ar MK 397 34. punktu, automātiski jāuzskata par A drošības klases sistēmām?**

Atbilde: Ministru kabineta 2021. gada 6. jūlija noteikumi Nr. 508 "Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas, drošības pasākumu un darbības nepārtrauktības plānošanas un īstenošanas kārtība" (turpmāk – MK noteikumi Nr. 508) nosaka, ka valsts drošības iestādes apzina iespējamo A, B un C kategorijas kritisko infrastruktūru un šie noteikumi nenosaka informācijas sistēmas konfidencialitātes, integritātes un pieejamības drošības klases. MK noteikumos Nr. 508 ietvertā kritiskās infrastruktūras klasifikācija izriet no Nacionālās drošības likuma 22.2. panta otrajā daļā ietvertās klasifikācijas. Skaidrojam, ka, piemēram, gadījumā, ja MK noteikumu Nr. 508 izpratnē tiek piešķirta B kategorijas kritiskās infrastruktūras statuss, tas nenozīmē, ka visām sistēmām MK 397 izpratnē arī tiks piešķirta B drošības klase.

5. **Es pareizi saprotu, ka tehniskajiem resursiem nav jānosaka konfidencialitātes, integritātes un pieejamības drošības klase (A, B vai C) atbilstoši MK 397 noteikumu 5. pielikumā ietvertajai metodikai?**

Atbilde: Jā, tehniskajiem resursiem (piemēram, tīkla ierīcēm) nav jāpiešķir A/B/C drošības klase saskaņā ar MK 397 32. punktu, jo klasifikācija attiecas tikai uz informācijas sistēmām un informācijas resursu kategorijām. Tomēr tehniskie resursi manto klasi no tās informācijas sistēmas piederības. Piemēram, tehniskais resurss "Cisco router" pieder pie B drošības klases informācijas sistēmas un ir klasificējams kā B drošības klases tehniskais resurss un uz to attiecas, piemēram, B drošības klases ārpakalpojuma prasības.

6. **Konfidencialitātes, integritātes un pieejamības drošības klasi nosaka katram informācijas resursam / informācijas resursu kategorijai un katrai informācijas sistēmai?**

Atbilde: Pēc MK 397 32. punkta nosacījumiem konfidencialitātes, integritātes un pieejamības klase tiek noteikta katrai informācijas sistēmai un katrai informācijas resursu kategorijai tās sastāvā. Tas nozīmē, ka katrai informācijas sistēmai un katrai kategorijai (piem., personu datu apstrādes serveris, "ierobežota pieejamība" informācija utt.) ir jānosaka atbilstošā A/B/C klase.

7. **Lūdzam paskaidrot noteikumu 32. punktā minēto jēdzienu "informācijas resursu kategorija".**

Atbilde: Tās var būt, piemēram, publiski pieejami dati, personas dati, komerciālas slepenas ziņas, "Ierobežotas pieejamības" informācija utt. MK 397 32. punkts paredz katrai sistēmai un katrai tās apstrādāto informācijas resursu kategorijai piešķirt drošības klasi. Resursu kategoriju piemēri nav tieši definēti MK 397, taču tās saprot kā informācijas veidus vai grupa ar līdzīgu aizsardzības līmeni.

8. **Informācijas sistēmai konfidencialitātes, integritātes un pieejamības drošības klasi nosaka, pamatojoties uz to, kāda (augstākā) klase ir piešķirta šajā sistēmā dzīvojošiem informācijas resursiem? Vai var būt izņēmumi?**

Atbilde: Saskaņā ar MK 397 33. punktu informācijas sistēmas kopējā A/B/C klase tiek noteikta pēc augstākā tās apstrādāto resursu drošības klases (augstākais riska līmeņa kritērijs). Tātad ja kādam informācijas resursam sistēmā klasifikācijā piešķirta A konfidencialitātes (vai integritātes vai pieejamības) klase, visa sistēma ir A klase. Izņēmumu 34. punkts paredz tikai kritiskās infrastruktūras sistēmām (automātiski A klase), citādi sistēmas klase vienmēr balstās uz augstāko resursa klasi.

9. **Veicot IS klasifikāciju identificējam, ka ir arī IS, kuru vērtējums pēc konfidencialitātes, integritātes, pieejamības būtu pat zemāks kā C drošības klases gadījumā un kuras neiespaido organizāciju kā mobilo sakaru pakalpojuma sniedzēja sniegto pakalpojumu (sakarus, SMS, pārraidītos datus). Izrietoši no tā organizācijas juristi un IT departamenta vadība uzskata, ka šādas sistēmas ir ārpus klasifikācijas tvēruma un nav iekļaujamas IS katalogā.**

Atbilde: MK 397 30. punkts prasa uzskaitīt un klasificēt visas IKT resursus un informācijas sistēmas, kas pakļautas kiberriskiem. Nav paredzēts izņēmums sistēmām ar "mazāku par C" vērtējumu. Ja kāda sistēma atrodas pakļauta kiberriskam, tai jāpiešķir klase saskaņā ar 32. un 33. punktu metodiku. Tātad arī organizācijā minētās sistēmas jāiekļauj katalogā un jāklasificē (ja nepieciešams, piešķirot zemāko C klasi).

10. **Vai IS var netikt piešķirta drošības klase (A, B vai C), ja tā neatbilst nevienai no konfidencialitātes, integritātes, pieejamības klasēm? Vai IS, kuras neatbilst nevienai no konfidencialitātes, integritātes, pieejamības klasēm, var neiekļaut IS katalogā?**

Atbilde: MK 397 32. punkts prasa klasificēt katru kiberriskam pakļauto informācijas sistēmu (un resursu kategoriju). Ja kāda sistēma nav nevienas drošības klases kritēriju piemērota, MK 397 neparedz īpašu "nedefinēto" statusu vai izslēgšanu no kataloga. Tādejādi visām sistēmām tomēr tiek piešķirta vismaz C klase (minimālā), un tās jāiekļauj IS katalogā.

11. **Vai rezerves kopijas (69.2., 69.3. punktā minētās) būtu uzskatāmas par informācijas resursu vai tehnisko resursu MK 397 noteikumu izpratnē?**

Atbilde: MK 397 69. punkts skaidro rezerves kopiju prasības, tajā 69.2. punktā piemin rezerves kopijas atvērtā koda bibliotēku pirmkoda (t.i. informācijas sistēmas programmatūras) versijām, bet

69.3. punktā – tehnisko resursu konfigurācijas kopijas. Tāpēc 69.2. attiecināms uz informācijas resursiem (sistēmas kods), savukārt 69.3. attiecināms uz tehniskajiem resursiem (sistēmas darbību nodrošinošo tehnikas uzstādījumi).

12. **Par kritiskās infrastruktūras IS drošības klases iedalījumu, ja KI īpašnieks ir klasificēts kā B drošības klases kritiskā infrastruktūra, vai visas attiecīgās KI informācijas sistēmas automātiski tiek uzskatītas par A drošības klases sistēmām atbilstoši MK 397 prasībām?**

Atbilde: MK 397 34. punkts paredz A klasi tikai IKT kritiskās infrastruktūras kopumā iekļautām sistēmām. Tas neparedz automātiski klasificēt kā A drošības klases visas iestādes sistēmas. Ja kritiskā infrastruktūra kā tāda ir B kategorijas, tas pats princips – tikai sistēmas, kas kvalificētas kā kritiskās infrastruktūras daļa, tiek definētas kā A drošības klases, ja vien SAB nav saskaņojis savādāk, bet pārējās parastajā kārtībā saskaņā ar 32.–33. punktu.

13. **Vai pareizi saprotu, ka tad, ja subjekts ir kritiskā infrastruktūra, bet ne IKT kritiskā infrastruktūra, tad tajā gadījumā visas subjekta valdījumā un īpašumā esošas IS ir A klases IS? Vai arī tikai tās IS, kas ir iekļautas kritiskās infrastruktūras kopumā, tādā gadījumā, kā var izdalīt, kuras sistēmas ir iekļautas kopumā?**

Atbilde: Ja subjekts ir klasificēts kā kritiskā infrastruktūra bet ne IKT kritiskā infrastruktūra, tas pats princips – A drošības klases statuss automātiski pienākas tikai kritiskajai infrastruktūrai iekļautajām IS, ja vien SAB nav saskaņojis savādāk. Tātad netiek automātiski padarītas par A drošības klases vismazākās sistēmas – jāvērtē, kuras sistēmas nodrošina kritiskos pakalpojumus un tiek definētas kā kritiskās infrastruktūras IS. IKT kritiskajā infrastruktūrā drošības klases saskaņo ar SAB.

14. **Vēlētos precizēt, vai grāmatvedības (ERP) sistēma svarīgajiem pakalpojumu sniedzējiem ir A vai B drošības klases drošības klase un vai ir pieejami skaidri nosacījumi, uz kuriem var nošķirt, kura klase būtu jāpiemēro?**

Atbilde: ERP sistēmas klasei nav iepriekš noteikta algoritma. Tā jāklasificē kā jebkura sistēma pēc MK 397 33. punkta kritērijiem. Ja ERP satur "Ierobežotu pieejamību" vai daudz personu sensitīvus datus, tai var būt A klase. Ja tajā apstrādāti, piemēram, personas dati bez papildu augsta līmeņa riskiem, iespējams B klase. Informācijas sistēmas drošības klase seko MK 397 klasifikācijai – A, B vai C sistēmas klasifikācija seko atkarībā no tās augstākā riska līmeņa piešķirtā A/B/C kritērija.

15. MK 397 35. punktā noteikts: "Ja kritiskās infrastruktūras kopumā ir iekļauta visa subjekta IKT infrastruktūra, subjekts informācijas sistēmām nosakāmās drošības klases saskaņo ar Satversmes aizsardzības biroju". **Lūgums skaidrot - Vai klasifikācija veicama subjekta īpašumā un valdījumā esošajām visām IS vai tikai tām IS, kas ietilpst subjekta kritiskajā infrastruktūrā un tiek izmantotas kritisko pakalpojumu nodrošināšanai?**

Atbilde: Ar Satversmes aizsardzības biroju visas drošības klases jāsaskaņo tikai tad, ja visa subjekta IKT infrastruktūra faktiski ir kritiskās infrastruktūras kopumā iekļauta (t.i., piemēro 35. punkta nosacījumu). Tas nozīmē, ka šajā gadījumā visas subjekta IS pakļaujas kritiskās infrastruktūras režīmam. Ja kritiskajā infrastruktūrā iekļautas tikai dažas IS, par kurām noteikta A

klase, tad pārējo riskam pakļauto informācijas sistēmu un resursu drošības klases saskaņojums ar SAB nav nepieciešams.

16. Vai nosakot sistēmas klasi ir jāuzskata, ka starp pazīmēm ir loģiskais "un" vai "vai"? T.i., lai noteiktu, piemēram, A drošības klases konfidencialitāti ir jāizpildās visām trīs pazīmēm, kas minētas 5. pielikumā, vai pietiek ar vienu no šīm pazīmēm?

Atbilde: Saskaņā ar 5. pielikumu katrai drošības klasei ir uzskaitītas vairākas neatkarīgas pazīmes. Lai informācijas sistēma būtu piemērota A drošības klases konfidencialitātei, viena no A drošības klases pazīmēm pietiek. Piemēram, ja sistēmas dati satur vismaz 1 000 000 personas datu, tā jau atbilst A drošības klases konfidencialitātes kritērijiem. Nav vajadzīgs, lai vienlaikus tiktu izpildītas visas tabulā uzskaitītās pazīmes. Šīs pazīmes darbojas kā "vai" nosacījumi. 5. pielikuma tabulā redzams, ka A/B/C klasi piešķir, ja atbilst vismaz vienai no attiecīgajā klasē minētajām pazīmēm (kritērijiem) un klasificē pēc augstākās riska līmeņa dimensijas.

6. IETEIKUMI

6.1. Darbību plāns subjektiem

1. **Apzināt un uzskaitīt visus kiberriskiem pakļautos IKT resursus un informācijas sistēmas**, norādot to īpašniekus, saistītos pakalpojumus, atkarības, atrašanās vietas, piegādātājus un ārpakalpojumus. Katalogu aktualizēt pēc izmaiņām, bet ne vēlāk kā viena mēneša laikā.
2. **Katrai informācijas sistēmai un informācijas resursu kategorijai noteikt konfidencialitātes, integritātes un pieejamības klasi** A, B vai C saskaņā ar MK 397 5. pielikumu.
3. **Dokumentēt** sistēmu arhitektūru, atkarības, datu plūsmas, ārējos savienojumus, mākoņpakalpojumus, ārpakalpojumus, piegāžu ķēdes un uzticamības robežas, lai identificētu apdraudējumus, ievainojamības, kritiskās atkarības un vienas atteices punktus.
4. **Sistemātiski identificēt, analizēt un novērtēt riskus**, ko rada fiziskās infrastruktūras, personāla, tehnoloģiju, informācijas sistēmu, programmatūras un tīklu apdraudējumi, ņemot vērā to iespējamību, potenciālo ietekmi, savstarpējās atkarības un esošo drošības pasākumu efektivitāti.
5. Pamatojoties uz risku novērtējumu un drošības klasēm, **noteikt un ieviest samērīgus aizsardzības pasākumus, tostarp piekļuves kontroli** un MFA, tīkla segmentāciju, žurnālfailu pārvaldību, šifrēšanu, rezerves kopēšanu un atjaunošanas pārbaudes, ievainojamību pārvaldību, kā arī piegādes ķēžu un ārpakalpojumu drošības kontroli.
6. **Pārskatīt dokumentus normatīvajos aktos noteiktajā** regularitātē un pēc būtiskām izmaiņām vai incidentiem.
7. Regulāri **uzraudzīt** cyber.gov.lv, cert.lv un ENISA publicētos brīdinājumus un vadlīnijas, **nosakot atbildīgo personu** un kārtību nepieciešamo drošības pasākumu ieviešanai.

PIELIKUMS – CEĻVEDIS

Solis	Darbība	Ko atbild	Atsauce
1	Identificē sevi kā NKDL subjektu	Būtisko pakalpojumu sniedzējs? Svarīgo pakalpojumu sniedzējs? IKT kritiskā infrastruktūra?	NKDL 20., 21., 24. pants
2	Nosaki kritiskos pakalpojumus, datus un resursus - veic ietekmes un atkarību analīzi.	Cik būtisks ir resurss pakalpojuma sniegšanai un kādus datus tas apstrādā, glabā vai pārsūta? Kādas būs sekas, ja resurss nedarbosies, dati būs neprecīzi vai tiem piekļūs nepiederošas personas? Vai pakalpojums saistīts ar valsts drošības, aizsardzības vai citu kritisku funkciju nodrošināšanu?	MK 397 30. punkts
3	Inventarizē sistēmas un klasificē pēc konfidencialitātes, integritātes un pieejamības	A klase - augstākais riska līmenis. B klase - vidējais riska līmenis. C klase - zemākais riska līmenis.	MK 397 32. punkts un 5. pielikums
4	Atvasini informācijas sistēmas kopējo klasi un laicīgi aktualizē katalogu	Kopējā klase sakrīt ar augstāko no trim dimensiju klasēm. Kritiskās infrastruktūras kopumā iekļauta sistēma ir A klase automātiski.	MK 397 33. un 34. punkts
5	Ievēro attiecīgās prasības un veido kiberdrošības politiku	Daudzfaktoru autentifikācija, žurnālfaili, rezerves kopijas, tīkla segmentācija, ārpakalpojumi un piegādes ķēde - apjomā, kas atbilst piešķirtajai klasei.	MK 397 3.- 8. nodaļa

Identifikācija → ietekme un atkarības → klasifikācija → prasības un kontroles → dokumentēšana → pārskatīšana